**DISQUISITIONES ARITHMETICAE**

CARL F. GAUSS

En 1985 nació la idea, y tendría que pasar una década hasta que esta se llevara a feliz termino. Al igual que habrá sucedido en tantas ocasiones en la comunidad matematica hispanoparlante, nos parecía imperdonable que, ya casi dentro del siglo XXI, no existiera una versián castellana de las Disquisitiones Arithmeticae del gran Gauss.

Iniciamos la tarea de realizar esta traduccion y si bien no sabíamos cuánto tiempo nos iba a tomar su finalizacion, sabíamos que tendríamos la mirada puesta sobre nosotros desde que saliá en Historia Mathematica aquella pequeña notita “A Spanish Edition of Disquisitiones Arithmeticae” en 1987. Tampoco era ajena la interrogation permanente de Víctor Albis, que en cada congreso internacional en el que nos juntíbamos me espetaba su “¿como va la traducciín?”.

El proyecto nacií en la Escuela de Matemítica de la Universidad de Costa Rica y conto con el apoyo durante varios años de la Vicerrectoría de Investigation de esta institution. En el desarrollo de este proyecto participaron muchas personas: el profesor Mark Villarino (en un primer momento), los profesores Michael Josephy y Angel Ruiz (durante todo el tiempo) y el profesor Hugo Barrantes (posteriormente). El entonces estudiante de posgrado Alan Dixon ayudo en el uso de TeX para darle su formato. En diferentes formas de respaldo a la elaboraciín participaron los entonces asistentes Adriín Gonzílez, Luis Gustavo Hernandez, Jesís Peraza y Martin du Saire. Y en la mecanografía nos ayudaron Gaston Guerra, Milton Madriz y Juliín Trejos.

Aunque un primer borrador de la obra completa se terminoí de hacer en 1988, no fue sino hasta 1990 que completamos una version definitiva. Y pasaría aín mas tiempo hasta que se emprendieran las acciones para buscar su publication: burocracias usuales en el medio y hasta licencias sabíticas inaplazables conspiraron para atrasar la salida a la luz píblica.

La idea de hacer esta traduccion no era por supuesto original. Conocemos de otros intentos serios fuera de Costa Rica por hacerla y sabemos tambien que algunos

avanzaron parcialmente en la tarea y otros, simplemente, no lograron pasar de las intenciones. Aunque haya sido la obra que abrió la teoría moderna de números y que ha sido considerada, con toda justicia, una de las joyas de la producción matemútica de todos los tiempos, emprender y completar su traducción no era un objetivo tan facil de asumir: aparte de la traduccion propiamente conceptual, la tarea significaba, inevitablemente, innumerables horas dedicadas a la minuciosa labor de cuidar estilo, simbología usada, representation gráfica, y, ademús, realizar interminables revisiones para minimizar los errores. La materialización de la idea era lo verdaderamente difícil. Era de entrada un gran reto a la constancia y perseverancia personales.

En la realization efectiva de este proyecto en Costa Rica confluyeron varios factores. El apoyo institucional fue importante. Este se dio a pesar de que, en un principio, se dudaba de la conveniencia (“no era de matematicas” ni era un proyecto típico de investigation) o de la factibilidad de un proyecto de este tipo que se debía realizar en un plazo de tiempo relativamente largo. Los directores de la Escuela de Matematica durante estos años en algunos casos apenas toleraron nuestro proyecto (porque, tal vez, no les quedaba mas remedio), aunque en otros sí lo apoyaron sin reservas. En la Vicerrectoría de Investigaciín sucedií un tanto parecido, aunque el apoyo dado globalmente fue siempre, sin duda, mucho mayor. Aparte de este apoyo administrativo, fue muy importante tambien la existencia durante los anos ochenta de un ambiente academico propicio para el desarrollo de este tipo de iniciativas. En 1983 se había fundado la Asociación Costarricense de Historia y Filosofía de la Ciencia que ha buscado desde su nacimiento fomentar proyectos de investigation, publicaciín y de reunion academicas en torno a la historia de las ciencias y de las matematicas en particular. (No sobra indicar que el profesor Michael Josephy ha sido siempre un asociado y colaborador importante de estas iniciativas, que el profesor Hugo Barrantes ha sido durante años el Tesorero de esta Asociacion y quien escribe esta presentation ha permanecido como su Presidente desde su fundacion). Cabe mencionar, ademas, que la accion durante estos anos de la Sociedad Latinoamericana de Historia de las Ciencias y la Tecnología ha permitido importantes intercambios en la comunidad academica latinoamericana preocupada por estos temas, lo que tambien ha nutrido nuestros esfuerzos. Pero lo que mías influencia tuvo fue la persistencia y permanencia de este grupo de matemaíticos dispuestos a no cejar en el empenño de obtener la primera version castellana de las Disquisitiones, a pesar de que, como siempre sucede en proyectos de esta dimension y sobre todo en nuestros países, muchos obstículos humanos y administrativos se sumaron a las dificultades propiamente intelectuales de la tarea.

El proyecto ayudo a fortalecer los trabajos en la historia y la filosofía de las matemáticas en la Universidad de Costa Rica, los que, recientemente, han encon­trado un lugar institucional especial con la creación en 1990 del Programa de In­vestigaciones Meta-Matemáticas (estudios multidisciplinarios sobre las matemáticas y su ensenanza). Varias investigaciones, publicaciones y participaciones en congre­sos acadáemicos dentro y fuera de Costa Rica fueron nutridas con el trabajo de la traducciáon.

Ya en lo que se refiere a la traduccián propiamente, tratamos de hacerla lo mas fiel posible al latín original. Pero consultamos las versiones francesa (trad. A. C. M. Poullet-Delisle, 1807) y alemana (trad. H. Maser, 1889) y sobre todo la version inglesa de A. A. Clarke (tanto la edicion de 1966, como la de 1986 revisada por W. C. Waterhouse). Debe destacarse que en nuestra revisián de la segunda edicion inglesa encontramos una coleccion de erratas que le señalamos directamente a Waterhouse.

Como es loágico suponer, en el desarrollo de nuestra tarea surgieron dificultades filologicas. En cuanto a la semantica, tratamos de hacer una traduccion apropiada palabra por palabra, aprovechando que usualmente la palabra latina corresponde a una ánica palabra castellana, solo en unos casos era necesario modificarla (por ejemplo, el latín “complexus” se traduce como “conjunto” y no como “complejo” aunque el ingles dice “complex”). En cuanto a la sintaxis, la situation era mas problemática: a pesar de la similitud de la estructura latina con la castellana fue necesario reordenar muchas veces las frases para obtener la expresion mas adecuada en espanol. Oraciones muy largas en el original latino las tuvimos que dividir. De la misma manera, expresiones latinas muy compactas (como el ablativo absoluto) fueron expandidas. En general, las cláausulas pasivas se tradujeron con la construcciáon española reflexiva (por ejemplo: “se puede hacer”) y evitamos el uso de la primera persona “podemos hacer”.

Como nuestro propásito fue hacer una traduccion lo mas fiel posible al latán, debemos agradecer muchásimo el haber podido contar con la existencia del sistema TEX (version Macintosh) para el levantamiento del texto y la confeccián de las artes finales. Con TEX pudimos tratar efectivamente la multitud de sámbolos matematicos, la notaciáon complicada y la enorme cantidad de ecuaciones, buscando siempre una representacioán gráafica muy parecida a la del original de 1801.

Nos parecio importante incluir en esta versián de las Disquisitiones una introduccián que permitiera colocar este libro y la obra de Gauss en un contexto apropiado. De igual manera, para beneficio de los lectores, introducimos una lista en lenguaje moderno de los contenidos de cada artáculo de las secciones de la obra.

Para terminar esta presentación, y en nombre del equipo que realizó esta primera versión castellana de las Disquisitiones Artihmeticae, deseo expresar nuestro agradecimiento a varias personas e instituciones. A la Escuela de Matematica y a la Vicerrectoría de Investigation de la Universidad de Costa Rica. A los colegas, asistentes y amigos que mencionamos hace unos cuantos parrafos y que contribuyeron al exito de nuestro proyecto. Y, muy especialmente, a la Academia Colombiana de Ciencias Exactas, Físicas y Naturales que gentilmente decidio publicar este trabajo y, en particular, a nuestro buen amigo y colega Víctor Albis por su aliento y apoyo constantes.

Angel Ruiz Zúñiga Presidente

Asociaciún Costarricense de Historia y Filosofía de la Ciencia Ciudad Universitaria “Rodrigo Facio”

San Jose, Costa Rica 28 de mayo de 1995.

Las ideas que desarrolló Gauss en las Disquisitiones Arithmeticae1 han sido de extraordinaria importancia en la Teoría de Numeros de los siglos XIX y XX. Gauss realizó una magnífica síntesis de los resultados del pasado en la teoría de nómeros, y obtuvo una colección brillante de nuevos resultados, proposiciones y metodos que han servido desde entonces como escuela para una gran cantidad de los matematicos mas importantes.[[1]](#footnote-2) [[2]](#footnote-3) Se dice, por ejemplo, que el gran Dirichlet siempre tenía una copia de las Disquisitiones Arithmeticae en su escritorio, y que estudiaba el libro religiosamente.[[3]](#footnote-4)

Junto con Arquímedes y Newton, Gauss se considera el matematico mas grande de todos los tiempos. Y las Disquisitiones Arithmeticae, una de las joyas del pensamiento humano.[[4]](#footnote-5)

La vida intelectual de Gauss se desarrollo en un “nuevo” contexto historico; se trataba de toda una nueva sociedad que emergía de las entrañas de la sociedad feudal. Aunque Gauss vivií parte de su vida en el feudalismo y el absolutismo germanos,

no puede negarse que la atmósfera de la nueva sociedad afectaba la cultura en su conjunto y, en particular, la producción científica. Esta nueva realidad, que supuso diferentes cosas en la vida de Gauss, y a pesar de que este nunca salió de su país, le generoó interesantes posibilidades para su trabajo y un contacto especial con otros investigadores de las matematicas. Gauss fue un matematico cuyas contribuciones mas que codificar los resultados del pasado abrieron surcos hacia una nueva epoca. Fue un científico moderno en un sentido profundo; su trabajo debe estudiarse por las generaciones de jovenes como un mecanismo de estímulo para la creación intelectual de todos los tiempos.

Vivio en una epoca de cambios historicos importantes: cuando Gauss tenía 12 años empezaba la Revolucion Francesa, y con ella un cortejo de acciones políticas y militares en el suelo europeo, cuya influencia llega hasta nuestros días.

Nacio Johann Friedrich Carl Gauss el 30 de abril de 1777 en la ciudad de Braunschweig (Brunswick).

Ninguno de sus padres poseía una gran cultura y, a lo sumo, sabían leer y escribir.[[5]](#footnote-6) Su familia paterna era de origen campesino.

El talento de Gauss venía de su lado materno. Su madre sostuvo una lucha constante frente a su esposo para que Carl Friedrich pudiera estudiar; tuvo exito afortunadamente.[[6]](#footnote-7)

Un primer estímulo lo recibio de parte de Friedrich Benz, el hermano de su madre y un hombre altamente inteligente que murio prematuramente.[[7]](#footnote-8) Gauss adopto como su segundo nombre el de su tío en reconocimiento a ese primer apoyo familiar.

La circunstancia familiar negativa no fue decisiva porque Gauss pudo estudiar la primaria y la secundaria en condiciones relativamente buenas. Como resultaba comun en ciudades mas o menos importantes de la Alemania de la epoca, Gauss pudo asistir a la escuela. Su primer maestro fue un tal Büttner; el maestro Büttner— segun E. T. Bell[[8]](#footnote-9)—era un bruto al mando de una escuela que esencialmente era una reliquia de la Edad Media.[[9]](#footnote-10) Sabemos que posteriormente Büttner ayudo a Gauss, pero todo pareciera indicar que lo decisivo fue el apoyo del asistente de Buüttner,

Bartels.[[10]](#footnote-11) Johann Martin Bartels (1769-1836), quien también ejerció cierta influencia en Lobachevsky, hizo conocer las hazanas de precocidad de Gauss, que llegaron a los oiídos del Duque de Braunschweig.[[11]](#footnote-12)

Fue en 1791 que Gauss fue presentado al Duque de Brunswick-Wolfenbuttel, quien impresionado por los talentos del joven le concedio un estipendio de diez talentos al ano. Cabe decir, que esto no era algo inusual en lugares en Alemania.

Ingresó Gauss al Collegium Carolinum, una academia recien creada, con una orientacion especial hacia la ciencia; se trataba de una institution publica de muy buena calidad dirigida hacia el personal militar y administrativo del país. Un tipo de institucióon necesariamente elitista, dentro de un róegimen esencialmente absolutista, pero que sirvió para formar a buena parte de los escritores y científicos de la Alemania de la epoca.[[12]](#footnote-13)

Tal vez resulte interesante comentar que estas academias póblicas orientadas a la tecnica y a la ciencia encontraban su lugar en el contexto histórico que vivieron los países protestantes; en su lucha contra la Iglesia Católica, los príncipes, acompanados de la Reforma luterana, se dieron a la importante tarea de asegurarse una nueva intelligentzia, fuera del control de la Iglesia y capaz de administrar la sociedad de acuerdo a la nueva realidad social y política. Eso explica—en parte—la existencia de instituciones educativas secundarias y universitarias con una vocaciín hasta cierto punto fundadas y dirigidas por los gobiernos absolutistas de los principados; así como la vocation laica y progresiva de las mismas. La educaciín y la formation de los cuadros intelectuales fue un componente vital del especial desarrollo de las naciones protestantes en la Europa de la epoca.

En su ingreso, de nuevo Gauss tuvo ayuda: esta vez de parte de Hofrath (consejero) von Zimmermann, quien fuera profesor del Carolinum.

De 1792 a 1795 pasí Gauss en el Carolinum, siendo este el centro de su vida.

Aprovechí la existencia de una excelente biblioteca; lo que le permitií estar al día en la literatura esencial sobre matematicas.

Gauss tuvo un interes muy especial por las lenguas y por los estudios clísicos de literatura; de tal manera que cuando a sus 18 años deja el Colegio Carolinum aín no se había decidido acerca de su carrera: filología o matematicas. El asunto lo

decidlo la construcción del famoso 17-gono el 30 de marzo de 1796: su satisfacción ante el descubrimiento lo convenció de estudiar matemóticas.[[13]](#footnote-14)

Su presencia en la Universidad de Gottingen fue decisiva para su formación intelectual. En esto Gauss no pudo hacer una mejor selección: Gottingen poseía una de las mejores bibliotecas de Alemania y, ademós, había tenido una reforma decisiva que oriento la universidad hacia la ciencia; mas aún, su administracion se encontraba menos influida por la Iglesia y por el gobierno. De esta forma, Gauss completó su formacion en instituciones que le dieron de lo mejor que se podóa conseguir en Europa en cuanto a instrucción, autonomía para el estudio y, ademas, el apoyo de varias personas para dedicarse a cultivar plena y exclusivamente su espóritu cientfico. En esto Gauss tuvo una suerte excepcional.

De su experiencia en Gottingen tal vez debamos subrayar que tuvo pocos amigos, entre ellos Bolyai, con quien sostuvo correspondencia toda su vida. Se dedicóo enteramente a sus estudios, y lo hizo solo. Este es un dato interesante. Tuvo una intensa experiencia intelectual, solo y sin interrupciones, durante estos tres años; generó durante los mismos buena parte de sus principales ideas científicas, que elaboraría con toda minuciosidad durante el resto de su vida. Es decir, en estos años formulo informal e intuitivamente muchas de sus hipotesis, sus ideas. No es que luego no aparecieran otras ideas o que desechara muchas de las que en estos anños formulo, pero que en un tiempo corto genero muchas ideas seminales es un hecho sumamente interesante.[[14]](#footnote-15) Debe recordarse que algo muy similar ocurrio con Newton. En la construccióon del conocimiento, la manera en que se producen o generan las ideas es muy variada; a veces se realiza en momentos cortos de gran intensidad que se repiten pocas veces; a veces, en un proceso lento de maduracióon sistemaótica coronada con síntesis de creatividad; todo depende de las personas, de su contexto existencial, de su capacidad, etc. Pero un hecho muy importante debe senalarse aquó y es la presencia de la intuición y la opinion, la presencia de lo informal, de las hipotesis que nacen de una percepcion intelectual especial, aunque no trascendental o móstica

sino auténticamente humana. Este componente es esencial en la creación intelectual y en la matematica en particular. Despues vendrá la bósqueda de los metodos, las escaleras analíticas, las condiciones formales y las demostraciones precisas, pero esta fase de delinear, de sugerir, de vislumbrar, es esencial en la creación; y, muchas veces, se busca ocultarla por diversas razones, a veces por prejuicio ideológico o por ignorancia. En el caso de Gauss encontramos con precisión un momento de tres años en los que su intuición y creatividad encontraron, como decimos los matemóticos, un punto de acumulación.

El principal resultado de Gottingen fue, sin duda, las Disquisitiones Arith­meticae.

La teoría de numeros constituía, según Gauss, la reina de las matematicas, a la que a su vez consideraba la reina de las ciencias. Y esta no es una mera frase retoórica sin trascendencia sino que revelaba una concepcióon sobre la ciencia y las matemóaticas; Gauss utilizaróa muchos de los recursos, mecanismos y modelos de la teoría de nómeros en los otros trabajos cienríficos que realizaría.

Gauss recibió su doctorado de la Universidad de Helmstedt en 1798. Su tesis fue publicada en 1799 con el rítulo: Demostratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse (Nuevas demostraciones del teorema que toda función entera racional algebraica en una variable puede ser resuelta en factores reales de primero o segundo grado)[[15]](#footnote-16); esto sera conocido como el “teorema fundamental del algebra”. Aunque este resultado ya era conocido[[16]](#footnote-17), incluso con el nombre de Teorema de d’Alembert, Gauss probo que todas las demostraciones anteriores, incluyendo las de d’Alembert (1746), de Euler (1749), de Foncenet (1759) y de Lagrange (1772), eran inadecuadas.[[17]](#footnote-18) En su demostracion Gauss transfería sin probarlo la continuidad geometrica a las cantidades aritmeticas, pero afirmaba que lo podóa demostrar.[[18]](#footnote-19)

La prueba dada por Gauss se basaba en consideraciones de tipo geométrico; sin embargo, en 1816 publicó dos pruebas nuevas, y otra en 1850, buscando una demostración íntegramente algebraica.[[19]](#footnote-20)

Se piensa en nuestros días que este teorema estó basado en consideraciones topológicas.

Antes de entrar en las ideas mismas de Gauss, tal vez resulte interesante recapitular algunos elementos de la teoría de numeros previa a Gauss. Podemos decir que los principales trabajos en la teoría de numeros anteriores a Gauss fueron realizados esencialmente por Fermat, Euler y Legendre.[[20]](#footnote-21)

Empecemos con Fermat. Hay dos conjeturas de Fermat que tuvieron cada una un destino distinto: a) que los nómeros de la forma 22 +1 eran aparentemente siempre primos, y b) que si p es primo y a es un entero no divisible por p, entonces ap — 1 es divisible por p. Euler demostró en 1732 que 22 +1 = 4.294.967.297 = 6.700.417 · 641. Esta conjetura de Fermat parece no ser cierta para ningun primo mayor que n = 4. [[21]](#footnote-22)

Con relacion a la segunda conjetura, que es el llamado “teorema menor” de Fermat, fue Euler el primero en publicar una prueba (aunque Leibniz habóa dejado una demostracion en un manuscrito anterior). La prueba de Euler aparecio en el Commentarii de San Petersburgo en 1736.

En la misma direccion Euler demostró un resultado mas general usando la llamada “funcion de Euler”. Se puede probar que

φ(m) = m(1 )(1 ) ... (1 ) con pi,p2,...pr factores primos distintos de m

p1 p2 pr

Euler probo que a^(m) — 1 es divisible por m si a es primo relativo a m.[[22]](#footnote-23)

Legendre fue un gran matemótico frances que hizo aportes a varias partes de las matematicas y no solo a la teoría de números. En 1797-98 publico su libro Essai sur la théorie des nombres en dos volómenes, que constituye el primer tratado dedicado exclusivamente a esta temótica.

Legendre redescubrió el teorema de la reciprocidad cuadrática que habla sido puesto en terminos menos modernos por Euler (aunque su demostracion no estuviera

completa). Otro asunto interesante de su trabajo fue que conjeturó en la misma obra mencionada que π(η) tiende a n/(ln n — 1, 08366) conforme n crece indefinidamente; no fue sino hasta 1896 que se demostró este resultado: π(η) ^ n/ ln n (en el sentido que su razon tiende a 1). Como afirma Bell, muchos de los resultados contenidos en las Disquisitiones Arithmeticae fueron obtenidos por ilustres matematicos anteriores a Gauss, como Fermat, Euler, Lagrange, Legendre y otros. Pero el tratamiento que realizo Gauss fue diferente: aparte de sus propios aportes originales, adoptó metodos generales que permitían englobar la mayoría de los resultados.[[23]](#footnote-24)

Las Disquisitiones Arithmeticae fueron publicadas en Leipzig en el verano de 1801, casi tres años despues que Gauss había regresado a Brunswick despues de su estancia en Gottingen.[[24]](#footnote-25) Se sabe que las primeras cuatro secciones fueron escritas en borrador en 1796 y escritas en forma definitiva para finales de 1797[[25]](#footnote-26) (en este ano Gauss envio una copia al consejero Zimmermann, y el levantado de texto se inicio en el taller de Kircher); un primer borrador de la Sección Quinta se completó en el verano de 1796, y fue completada a traves de diferentes revisiones en el primer semestre de 1800. [[26]](#footnote-27)

Morris Kline señala que las Disquisitiones Arithmeticae fueron enviadas primeramente a la Academia Francesa en 1800 y el libro fue rechazado, obligando a Gauss a publicarlo el mismo.[[27]](#footnote-28) Sin embargo, aunque ha sido muy extendida la versión de que las Disquisitiones Arithmeticae fueron rechazadas por la Academia Francesa de Ciencias y que ese fue el motivo de que el mismo Gauss asumiera su publicacion, todo parece indicar que fue de otra manera. Segun Bell, la version “romantica” es de W. W. R. Ball en su famoso libro de historia de las matematicas; estudios muy serios en 1935 demuestran que las Disquisitiones Arithmeticae nunca fueron sometidas a la Academia Francesa de Ciencias y mucho menos rechazadas.[[28]](#footnote-29)

Como es bien conocido, las primeras tres secciones son una recopilación introductoria de los principales resultados de la teoría de números en la epoca.29 Las Secciones IV, V y VI son el corazon del trabajo; la Seccion VII se refiere a un tema que aunque esta ligado en si mismo constituye una tematica aparte.

La primera seccion simplemente define la nocion de congruencia entre dos enteros racionales modulo p; solo tiene 5 paginas.

Las Secciones II y III contienen interesantes resultados como la prueba de la unicidad de la factorization de enteros en primos y las definiciones de maximo comun divisor, y de minimo comun multiplo; la investigation de los residuos de una potencia de un numero dado modulo un primo, es decir, partiendo del teorema “pequeño” de Fermat: ap-1 ξ 1 (mod. p), p un primo que no divide a.

El tema central de la Seccion IV es la ley de la reciprocidad cuadrática.30 Aunque ese teorema había sido formulado por Euler, así como discutido por Legendre, Gauss es quien realiza una prueba completa y correcta del teorema.31

La Seccion V investiga la teoría de las formas binarias cuadráticas, es decir del tipo f (x, y) = ax2 + 2bxy + cy2 donde a, b y c son enteros dados. El objetivo central en el estudio de estas formas es el de conocer la manera en que un numero dado m puede ser representado por las binarias ax2 + 2bxy + cy2 y las ternarias ax2 + 2bxy + cy2 + 2dxz + 2eyz + fz2 32; lo cual es esencialmente un resultado aritmetico.

Dickson33 senala correctamente que las binarias así puestas son un caso particular de la formula

ax2 + 2bxy + cy2 = m (\*)

que despues tendría mucha utilidad en el trabajo de Dedekind, que establece una correspondencia entre clases de formas como en (\*) y ciertos conjuntos de numeros [[29]](#footnote-30) [[30]](#footnote-31) [[31]](#footnote-32) [[32]](#footnote-33) [[33]](#footnote-34)

algebraicos determinados por una raíz de αξ2 + + c = 0. 34

La Sección VI es un apendice de la sección anterior; lo que hace Gauss aquí es presentar una coleccion de aplicaciones de los conceptos que desarrolla en la seccion anterior, por ejemplo, para resolver para x e y, la ecuación mx2 + ny2 = A con A, m y n enteros.35

La Sección VII tuvo una gran influencia; uno de los temas centrales es el de la ciclotomía36, 37, es decir de la teoría de la division del círculo, referida a la ecuacion xp — 1 = 0 con p un nómero impar. En esta parte se integra una problematica que involucra geometría, aritmetica y algebra de una manera especial: la construcción del polígono regular de n lados con regla y compós.38 Gauss incluyó su descubrimiento del 17-gono39, pero ademós resolvio el problema de manera general, es decir estableciendo cuóndo el n-gono se puede construir y cuando no.40, 41

Las Disquisitiones Arithmeticae representa tambien un adios a las matema- ticas puras como campo exclusivo en la actividad científica de Gauss.42 Aunque, en realidad, no se puede afirmar tajantemente que Gauss se dedicara exclusivamente a la matematica “pura” durante los años de Gottingen.

Tal vez resulte interesante senalar que Gauss tenía prevista la inclusión de una octava seccion en las Disquisitiones Arithmeticae, pero esta fue eliminada para bajar los costos de publicación.43, 44 [[34]](#footnote-35) [[35]](#footnote-36) [[36]](#footnote-37) [[37]](#footnote-38) [[38]](#footnote-39) [[39]](#footnote-40) [[40]](#footnote-41) [[41]](#footnote-42) [[42]](#footnote-43) [[43]](#footnote-44) [[44]](#footnote-45)

Parece ser que Gauss tenía la intención de escribir una continuación de las Disquisitiones Arithmeticae45, cuyo contenido podría intuirse a partir de un manuscrito encontrado despues de la muerte de Gauss: “Analysis Residuorum”,

así como de los artículos sobre teoría de numeros que escribio despues de las Disquisitiones Arithmeticae. Algunos de los temas habrían sido: el de las sumas, que aparece en el apartado 356 de las Disquisitiones Arithmeticae, la teoría de residuos bicuadraticos y rábicos, y pruebas adicionales de la ley de la reciprocidad cuadrática.

El asunto de las sumas fue desarrollado por Gauss en el artículo “Summatio quarundam serierum singularium” de 1808. Se trata de expresiones de la forma

n-1 v2

W =Σ e 2π ν

ν=0

de importancia en posteriores desarrollos de la teoría de numeros. Los otros resultados de Gauss sobre residuos bicuadraticos aparecieron en los artículos “Theoria residuorum biquadraticorum I & II”, publicados por la Sociedad Real de Gottingen.[[45]](#footnote-46) [[46]](#footnote-47)

Con Morris Kline, podemos decir, en efecto, que las tres principales ideas de las Disquisitiones Arithmeticae y de los trabajos de la teoría de numeros que realizo Gauss son: la teoría de las congruencias, la introduccion de los numeros algebraicos y la teoría de las formas.

La nocioín de congruencia aparece antes de Gauss con Euler, Legendre y Lagrange; sin embargo, Gauss introdujo la notaciín moderna en la primera secciín de las Disquisitiones Arithmeticae:

a es congruente a b mídulo p, a = b (mod. p)

b es un residuo de a modulo p, y viceversa.

En la Secciín III de las Disquisitiones Arithmeticae Gauss analiza los residuos de potencias. En particular, brinda una demostracion del teorema “pequeño” de Fermat. Para demostrarlo debe recurrir al estudio de las congruencias del tipo xn = a (mod. m) ; donde a y m son primos relativos.

Es en la Secciín IV donde trata el asunto de los residuos cuadríticos; dando aquí su primera prueba de la ley de reciprocidad cuadrática. Aunque Gauss reconoce

que Euler había estudiado el asunto en su Opuscula Analytica de 1783, y que Legendre lo había hecho en su trabajo de 1785, Gauss afirma que eran trabajos incompletos y menos simples que el que presenta en las Disquisitiones Arithmeticae.47

Gauss realizó en su vida 8 demostraciones48, y más de cincuenta se han realizado posteriormente.49

Gauss estudió la congruencia de polinomios, usando una idea que luego Cauchy usaría para definir los nómeros complejos en Exercises d’ analyse et de physique mathématique, 4, 1847, 84 ff.50

Las leyes de reciprocidad bicuadratica51 y cubica fueron trabajadas por Gauss entre 1808 y 1817, y el teorema de los residuos bicuadraticos fue dado en artículos de 1828 y 1832.52 Sin embargo, señala Bell que es en 1825 que Gauss encuentra que no son los enteros “corrientes” los que le sirven para este asunto, sino los que hoy llamamos “enteros complejos gaussianos” (es decir, de la forma a + bi, con a, b enteros racionales). Esto hacía referencia a lo que se desarrollaría como “nómeros algebraicos”.53 Segón Kline los enteros complejos ya habían sido introducidos por Euler y Lagrange.54 Lo que Gauss probo fue que se comportaban mas o menos como los enteros racionales ordinarios. En particular, que se cumplía la descomposición ónica en factores primos para cada entero (asumiendo por supuesto que las cuatro unidades complejas no son diferentes factores: i.e.: si a = bc = (ib)(-ic), no estamos [[47]](#footnote-48) [[48]](#footnote-49) [[49]](#footnote-50) [[50]](#footnote-51) [[51]](#footnote-52) [[52]](#footnote-53) [[53]](#footnote-54) [[54]](#footnote-55)

hablando de descomposiciones diferentes).[[55]](#footnote-56) La ley de la reciprocidad cuadrática para enteros complejos fue establecida por Gauss en 1828.[[56]](#footnote-57)

La teoría de los enteros complejos abrió el camino para el desarrollo de una temática apasionante en las matematicas del siglo XIX: los números algebraicos, aunque el mismo Gauss no percibio la riqueza que este campo supondría.[[57]](#footnote-58) Podemos decir que la teoría evoluciono en cuatro momentos: el primero, su origen, se da con el famoso teorema de Fermat acerca de xm + ym = zm. Gauss intento resolver la conjetura para el caso m = 7, pero no tuvo exito.[[58]](#footnote-59) Gauss no quiso involucrarse mucho con el ultimo teorema de Fermat, en parte por considerarlo una proposicion aislada, como muchas otras, que ni puede probarse ni refutarse.[[59]](#footnote-60)

Fue Lame en 1839 quien lo logro hacer para el caso m = 7; y Dirichlet para el caso m = 14.

Otro discípulo de Gauss (y de Dirichlet), Kummer, abordá el asunto utilizando una maquinaria teorica que abrio caminos interesantes, e inicio la segunda fase en la historia de los enteros algebraicos. Se pasa de los números enteros complejos a los algebraicos, en la formulacion de Kummer, los números de la forma

f (a) = ao + aja + ... + ap-2ap 2

donde a es una p-esima raíz imaginaria. Kummer llamo a estos numeros enteros complejos .

Dotados los nuevos numeros de las definiciones naturales de suma y producto, Kummer asumio la factorizacián primaria como única, e incluso hizo de esta

formulación un requerimiento para la resolución de la conjetura de Fermat. (Cauchy y Lame pensaron como Kummer.) Sin embargo, Dirichlet senaló que eso no era cierto; Kummer reconocio el error muy poco tiempo despues. Kummer buscó reconstruir una forma de factorización única a traves de unos numeros que llamó “ideales”, logrando la conjetura de Fermat para una serie de numeros primos: para todos los menores que 100 salvo el 37, 59 y el 67, para los que demostró la conjetura en un artículo de 1857.[[60]](#footnote-61) Posteriormente, Mirimanoff en 1905, perfeccionando el metodo de Kummer, extendio el resultado para todo n hasta 256 si x, y y z son primos al exponente n.[[61]](#footnote-62)

El asunto de la factorizacion unica se volvio el mecanismo teorico para la definición de nuevos nómeros y entidades.

Otro discípulo de Gauss, Dedekind, avanzo extraordinariamente el campo, definiendo una nueva y decisiva etapa. En lugar de trabajar con las raóces de la unidad, Dedekind, en 1871, formulo una definicion mós amplia de los nómeros algebraicos: sea r una raíz de la ecuacion

aoxn + aixn-1 + ... + an-ix + an = 0 ,

con los ai enteros racionales negativos o positivos, y tal que r no es raóz de ninguna ecuacion del mismo tipo y de grado menor a n, se llama a r un nómero algebraico de grado n. Si el coeficiente ao es 1, r se llama un entero algebraico de grado n.

Dedekind introdujo el concepto de campo numerico y mostro que claramente los nuómeros algebraicos forman un campo; introdujo entonces la nocioón de anillo, y proboó que los enteros algebraicos formaban precisamente un anillo. Con las nuevas definiciones de nómeros ya podóa Dedekind buscar una solucion al asunto de la factorizacion ónica, pero ahora en el campo de los nómeros algebraicos. Para esto sólo le faltaba un nuevo concepto que era precisamente el de ideal, en el sentido moderno. La teoría de los ideales constituye entonces una generalizacion de los nómeros enteros ordinarios.[[62]](#footnote-63)

Años mós tarde, en un trabajo de 1887, Kronecker, discópulo de Kummer, demostró que la teoría de los numeros algebraicos es independiente de la teoría de los nómeros reales.[[63]](#footnote-64)

La teoría de las formas fue importante en el siglo XIX. Aunque Euler había obtenido algunos resultados, Lagrange descubrió que existían formas equivalentes para expresar un entero. Como ya lo hemos señalado antes, este es el tema central de la Seccion V de las Disquisitiones Arithmeticae.[[64]](#footnote-65) Gauss probó varios teoremas sobre la equivalencia de las formas. Entre ellos, que dadas tres formas F, Fi y F2, entonces: si F es equivalente a Fi y Fi es equivalente a F2, entonces F es equivalente a F2. Demostró cómo encontrar todas las transformaciones de F en Fi si F y Fi son equivalentes, etc. Y, especialmente, encontró todas las representaciones de un nómero M por una forma F, siempre que x, y sean primos relativos. Gauss probo, ademós, que las formas (con un discriminante igual D) se pueden agrupar en clases.

Uno de los resultados importantes concierne a las formas compuestas: Sea F = AX2 + 2BXY + CY2 una forma que se puede transformar en el producto de dos otras formas f = ax2 + 2bxy + cy2 y f' = a'x02 + 2b'x'y' + Cy'2 por la sustitución

X = pixx' + p2xy' + P3x'y + P4yy',

Y = qixx' + q2xy' + ©x'y + q4yy',

entonces F se dice transformable en ff. Si ademas los números

***p****i****q****2* ***- q****i****p****2****, p****i****q****3* ***- q****i****p****3****, p****i****q****4* ***- q****i****P****4****, P****2****q****3* ***- q****2****P****3****, P****2****q****4* ***- q****2****P****4* y ***P****3****q****4* ***- q****3****P****4*

no poseen un divisor común, F se llama una compuesta de las formas f y f.

Gauss probo que si f y g pertenecen a la misma clase y f y g' pertenecen a la misma clase, entonces la forma compuesta de f y f' pertenece a la misma clase como la forma compuesta de g y g'.[[65]](#footnote-66)

El trabajo de Gauss con las formas pretendóa dotarle de medios para encontrar resultados sobre los nómeros enteros; los mecanismos algebraicos y abstractos le interesaban en función de los resultados concretos en la aritmetica.[[66]](#footnote-67)

Por ultimo, en 1830, en la reseña de un libro llamado Gottingische Gelehrte Anzeigen, escrito por Ludwig Seeber, Gauss dio una representation geometrica de

sus formas y de las clases de formas, comenzando así la llamada teoría geométrica de números, que luego sería desarrollada por Minkowski.[[67]](#footnote-68)

Vamos ahora a completar nuestra introducción mencionando algunos aspectos de la obra no aritmetica de Gauss así como otros de naturaleza personal, que nos permiten una mejor comprension del trabajo de Gauss.

Resulta aquí interesante comparar la personalidad de Gauss con otro gran matematico del siglo XIX: Cauchy. A diferencia de Gauss, Cauchy publicaba rápidamente una vez que hubiera obtenido un resultado. Boyer sugiere que esta fue tal vez la razon por la que en la historia se atribuye mas la introduccion del rigor a Cauchy que a Gauss, a pesar de la extraordinaria precision logica de los trabajos de este.

Por otra parte, Cauchy tenía una vocacion pedagogica y le gustaba enseñar; publicaba continuamente en el Journal de la Ecole Polytechnique así como en las Comptes Rendus de la Academie. Gauss no tenía mucho interes en la docencia.

Los trabajos de Cauchy resultaron muy fructíferos para las matematicas del siglo XIX y, de forma igual que Gauss, Cauchy poseía una percepcion moderna de ellas. A manera de ejemplo: la integracion del siglo XVIII era tratada como la inversa de la derivacion, mientras que en la aproximacion de Cauchy se planteaba como el límite de una suma: esta aproximacion produciría mayor riqueza en la evolucion posterior de la integracion.[[68]](#footnote-69)

Cauchy contribuyo a casi todos los temas de la matematica como Gauss, aunque no tanto en la teoría de numeros. Sin embargo, fue Cauchy quien dio la primera prueba general al teorema de Fermat que establece que todo entero positivo es la suma de a lo sumo tres numeros triangulares o cuatro cuadrados o cinco numeros pentagonales o seis exagonales, y así indefinidamente. Como señala Boyer, de esta forma se daba un clímax al estudio de los numeros figurados que había comenzado con los pitagoricos hace mas de 2000 años.[[69]](#footnote-70) Entre Gauss y Cauchy no existio una relacion muy cordial.

Aunque Gauss no presto mucho interes a la geometría, lo que hizo fue genial: por una parte, en 1827, publico un tratado con el que se inicio la geometría diferencial: Disquisitiones generales circa superficies curvas[[70]](#footnote-71), y, en 1824, establecio

sus conclusiones sobre el postulado de las paralelas. Si hubiera desarrollado y publicado estas ideas habría obtenido el credito como el padre de la geometría no euclidiana.71

La obra matematica y científica de Gauss resulta impresionante.72 Despues de escribir las Disquisitiones Arithmeticae se dedico al calculo astronómico. Gauss creo el metodo y el procedimiento para calcular orbitas celestes con base en ciertos datos observacionales. Esto se codificó en su libro Theoria motus corporum coelestium in sectionibus conicis solem ambientium de 1809. Aquí trato las llamadas “perturbaciones” y brindo las tecnicas que dirigirían la astronomía computacional hasta un tiempo muy reciente. Posteriores observaciones sobre los planetas Ceres, Pallas, Vesta, Juno, etc., confirmaron la precisión de los metodos de Gauss.73 No obstante, dice Bell que—en esencia—ningón descubrimiento matemótico se encuentra en Theoria motus.74

En 1811 Gauss escribía a Bessel un resultado extraordinario en el campo de los nómeros complejos: para que la integral de lónea de una función compleja sea cero es suficiente que la función sea analótica en todo punto de la curva y dentro de la curva. Este resultado no fue publicado por Gauss, como tantos otros resultados. Años despues, Cauchy lo redescubriría y junto con otros resultados empujaría hacia adelante el analisis complejo del siglo XIX.75

En 1812 Gauss publico un trabajo sobre las series hipergeometricas, estable­ciendo las restricciones para definir la convergencia de las mismas. De una manera general, de nuevo, daba tratamiento a las principales series que aparecóan en la física matematica de su tiempo; con su trabajo se pudieron tratar muchas de las ecuaciones diferenciales de la física del siglo pasado.76

Sólo a partir de 1820 Gauss se dedico a la investigación en Geodesia, la base aplicada de lo que sería la geometría diferencial. [[71]](#footnote-72) [[72]](#footnote-73) [[73]](#footnote-74) [[74]](#footnote-75) [[75]](#footnote-76) [[76]](#footnote-77)

Después Gauss hizo descubrimientos en la teoría electromagnética y en la teoría de la atracción newtoniana, creando la llamada teoría del potencial.[[77]](#footnote-78)

Edna Kramer afirma que la contribución de Einstein a la física moderna fue posible sólo gracias a algunos de los grandes avances matemóticos que hizo Gauss.[[78]](#footnote-79) En efecto, la geometría diferencial desarrollada sustancialmente despues de Gauss por Riemann fue esencial para la formulacion de la teoría de la relatividad. Pero ademas: se puede afirmar una conexion teorica interesante entre Gauss y Einstein: la idea de la relatividad nace en Einstein despues de dos años de trabajar con el calculo tensorial realizado por dos matematicos italianos, Ricci y Levi-Civita, ambos discípulos de Riemann y Christoffel, quienes fueron inspirados por el trabajo geometrico de Gauss.[[79]](#footnote-80) [[80]](#footnote-81) [[81]](#footnote-82)

Es interesante señalar tambien que Gauss había anticipado el teorema que el nímero de primos menores que un entero determinado n, tiende a n/ ln n, cuando n tiende a infinito, resultado al que Legendre se acercí mucho; sin embargo, no sabemos si Gauss poseía una prueba cuando escribio el resultado en una tabla de logaritmos que había obtenido a la edad de 14 anos.80, 81

La obra de Gauss y la evolucion de su trabajo se pueden recapitular a partir de un pequenño diario intelectual que se mantuvo escondido en los papeles de la familia hasta 1898; consta de 19 píginas y en el aparecen 146 enunciados de resultados, el ultimo del 9 de julio de 1814.[[82]](#footnote-83) Es este diario la principal fuente documental para demostrar la preeminencia de Gauss en el descubrimiento de tantos resultados

matemáticos que no fueron publicados.[[83]](#footnote-84) [[84]](#footnote-85) [[85]](#footnote-86)

Cuando se estudia la historia de las matemáticas del siglo XIX sucede un asunto curioso: siempre que se analiza un descubrimiento debe cotejarse con el

diario o los papeles no publicados de Gauss para establecer si Gauss no lo había encontrado primeramente.84, 85 Kronecker decía en el siglo pasado: “casi todo lo que las matemáticas de nuestro siglo ha producido en cuanto a ideas científicas originales, esta conectado con el nombre de Gauss”.[[86]](#footnote-87)

¿Por que no publicaba Gauss como otros científicos y se guardaba para sí tantos y formidables resultados matematicos? Si se elimina la interpretación del rechazo de la academia francesa con las Disquisitiones Arithmeticae que se ha dicho doto a Gauss de un celo extralimitado para publicar, pareciera que la clave se encuentra en el lema fundamental de Gauss: “Pauca sed matura” (pocos pero

maduros). La obsesion por la perfection así como un excesivo ensimismamiento pueden dar cuenta de este asunto: de hecho, Gauss nunca tuvo mucho interes en la trasmision del conocimiento y la enseñanza; su investigation era una experiencia individual que le proporcionaba satisfaction a sí mismo y nada mas. Si Gauss hubiera tenido otro tipo de actitud es probable que las matematicas del siglo XIX hubieran avanzado de una forma diferente, permitiendo que otros excelentes cerebros de la epoca no tuvieran que dedicar tantos esfuerzos y tiempo a resultados que ya Gauss había obtenido, ampliando considerablemente los alcances de la production matematica.

La coherencia y la unidad intelectual presentes en las Disquisitiones Arithmeti­cae nos brindan un tema para hacer una reflexion sobre el metodo en la construction matematica. Gauss reconstruye y sistematiza los resultados disponibles, elabora una coleccion de mecanismos y teorías generales, y luego da cuenta de los problemas par­ticulares, llegando a incluir en su trabajo su resultado famoso del 17-gono regular. Se

trata de una exposición intelectualmente serla y profunda, aunque tal vez deba men­cionarse que la emersión de los problemas a los que se enfrentó y resolvió con tanta destreza y generalidad los había estudiado de manera particular; es decir, en nuestra opinion, Gauss abordo los problemas individuales y construyó a partir de ellos el marco teorico que los englobaba y reducía a lo particular precisamente; la exposicion en las Disquisitiones Arithmeticae sigue una línea de lo abstracto y general a lo par­ticular, pero esta logica no debería confundirse con la “logica” heurística e intuitiva de la construccióon intelectual que le permitióo llegar a esos resultados generales y que siempre esta presente en la construcción matematica y científica en general.

Durante los siglos XVII y XVIII la teoría de numeros sumaba una coleccion de resultados particulares y disconexos, sin un marco que les brindara coherencia. Gauss transformo esa situacion convirtiendo la teoría de numeros en una ciencia matematica plena.[[87]](#footnote-88)

Aunque siempre conviene enfatizar la importancia de la relacion entre matematicas y la realidad física, en sus multiples dimensiones, tambien tiene trascendencia entender el papel de los aspectos mas abstractos y “puros” de esta ciencia. La matematica cuenta como una de sus características mas especiales con esa doble naturaleza de abstraccion y empirismo-intuicionismo; es decir, existe un flujo creador y edificante entre las matematicas mas intuitivas físicamente (para no decir el termino muy manido de “aplicadas”) y las puras. En la historia de las matematicas a veces han dominado unas dimensiones, a veces otras; en ocasiones el dominio de una de esas dimensiones ha sido determinante para hacer progresar las matematicas en su conjunto, para ampliar sus horizontes, para solidificar su fisonom ía cognitiva e intelectual, para abrir nuevas vías en la creacion mental, para descubrir nuevos secretos. La relacion con la física jugo un papel singular con Newton y las matematicas del siglo XVIII. Pero tambien la creacion de la Teor ía de Numeros por Gauss, con su tratamiento abstracto y puro[[88]](#footnote-89), contribuyo a abrir camino a la matematica moderna que dominaría el siglo XIX y penetraría en el siglo XX.

Durante casi 20 años Gauss dedico la mayoría de su tiempo a calculos astronomicos.[[89]](#footnote-90) Tal vez se pueda lamentar que su cerebro extraordinariamente dotado no se hubiese dedicado al pensamiento abstracto mas tiempo y menos a este tipo de computos que aunque con mayor dificultad otras personas podrían haber realizado.[[90]](#footnote-91)

Es cierto, pero también debe decirse que su involucramiento en la astronomía y el calculo como una de sus dimensiones le permitió a Gauss una posición de reconocimiento científico e intelectual internacional que le daba medios para vivir e investigar, así como, por otra parte, su interrelation con dimensiones más empíricas de la ciencia le daba elementos teoricos para estimular su creacion matematica y científica de una manera integral. A veces la visián del matematico “purista” de nuestra epoca juzga con su actitud reduccionista la construction matematica del pasado, distorsionando su realidad.

Gauss estaba dotado de una genialidad matematica combinada con una extraordinaria habilidad para la experimentacián empírica. Incluso, creo varios aparatos átiles en el curso de sus investigaciones: el heliotripo, para trasmitir señales luminosas, el magnetámetro, y el famoso telegrafo electrico (en 1833).[[91]](#footnote-92)

Para dar una visián mas completa de Gauss desde un punto de vista humano, vale la pena mencionar los pasatiempos que tema: la literatura europea y clasica antigua, interes en el conocimiento de la política internacional, el dominio de lenguas extranjeras, asá como la incursián en las nuevas ciencias.[[92]](#footnote-93) Gauss era, si se quiere, una persona conservadora que nunca saliá de su paás, aunque seguáa con cierto detenimiento el acontecer europeo a traves de los periodicos y libros; le molestaba cualquier cosa que pudiera obstaculizar o interrumpir su trabajo, que constitma su principal fuente de satisfaccioán. En la dáecada de sus treinta anños Gauss no tuvo muchas fuentes de satisfaction vital y, mas que eso, el infortunio lo rodeo: murio su benefactor, el Duque de Brunswick, Alemania se encontraba hundida bajo la bota napoleánica y, ademas, murio su primera esposa.[[93]](#footnote-94) Pero con el tiempo fue reconstruyendo su vida, estableciendo sus rutinas y sus propoásitos intelectuales de una manera armonica; su madre lo acompañá hasta la muerte de esta, atendida hasta el final por Gauss, quien tal vez agradecía con su actitud la lucha que su madre dio para sacarle del medio social y cultural del que su padre no quería que saliera.

Las matematicas del siglo XIX sufrieron una gran transformation como producto de varios resultados teoricos: entre ellos las geometrías no-euclidianas y los cuaterniones. En realidad, la esencia de este revolucionario proceso fue la ruptura con la matematica “sensible” e intuitiva, euclidiana y física que tenía lugar hasta entonces, y que Kant—por ejemplo—condenso en su filosofía asumiendola como

premisa ontologica. Esto se rompió con una nueva matemática que fundamentaba su validez en el discurso lógico, combinando rigor y abstraction, aunque sufriera un “distanciamiento” de lo real intuitivo. Aquí nace la matematica moderna: con sus virtudes y sus vicios.[[94]](#footnote-95)

Se debe enfatizar el carócter revolucionario[[95]](#footnote-96) de la perspectiva de Gauss en su trabajo matemótico; no se trataba de la ampliation de resultados de una manera lineal y acumulativa, era mós que eso. El trabajo de Gauss representaba una nueva actitud que reformaba la praóctica matemaótica en dimensiones muy importantes, que recolocaba los resultados obtenidos en una nueva direccióon, transformando cualitativamente lo que existía antes y permitiendo nuevos derroteros.[[96]](#footnote-97)

Esto hizo de Gauss el dueño de la perspectiva intelectual e histórica mas avanzada en los matemóticos de su tiempo. Gauss llego a resultados que definían un nuevo camino y una nueva estructuración de las matematicas; sin duda, esta perspectiva y su gran talento matemaótico creaban las condiciones para hacer la nueva matematica con mayor propiedad que muchos otros: Gauss sabóa hacia dónde apuntar y dirigir sus esfuerzos. No es extrano que encontrara tantos resultados en tantos campos antecediendo durante muchos años al resto de los matemóticos.

Aunque su preocupacióon por el rigor desde un principio fue decisiva para cristalizar su vision intelectual de las matematicas, tambien participo su madurez para captar lo extrano y lo nuevo.

La “ruptura” con las matemóticas post-newtonianas del siglo XVIII no fue asumida por otros grandes matematicos como Laplace o Legendre en el mismo

siglo XIX; muchos siguieron siendo matemáticos “del siglo XVIII”[[97]](#footnote-98). Gauss fue el primer matemático de las nuevas matemáticas que nacen el siglo pasado. Sin embargo, a pesar del sentido de apuntalamiento de lo general y abstracto que Gauss imprimió a sus trabajos, nunca dejo de tener una vision de las matematicas asida a la realidad y al mundo; para Gauss las matematicas nacían de problemas específicos que podían ser tratados de manera general; encontraba motivacion en ellos. Su trabajo en varias partes de la física-matematica no puede verse simplemente como una necesidad pecuniaria, sino mas bien en la visián y la actitud que este tenía frente a las matematicas. En este sentido, Gauss podría considerarse menos moderno que Galois, Hamilton o Grassmann.[[98]](#footnote-99) Podríamos decir que Gauss se quedaba en un termino medio entre la matematica empírica del siglo XVIII y la matematica “libre y pura” de los ultimos 150 años. En nuestro tiempo, despues de tantos años recorridos de la matematica moderna, tal vez podamos reevaluar intelectualmente aquel término “medio” de Gauss, extraer un nuevo sentido en la naturaleza de las matematicas[[99]](#footnote-100) y vislumbrar mejor las matematicas del futuro.

CONTENIDOS POR ARTICULO.

***En la siguiente tabla los traductores indicamos los contenidos de cada artículo de las*** Disquisitiones Arithmeticae. ***Para ayudar al lector, nos permitimos utilizar lenguaje moderno, es decir, se usan términos introducidos después del tiempo de Gauss.***

SECCION PRIMERA. DE LA CONGRUENCIA DE LOS NUMEROS EN GENERAL.

Artículo 1. Definición de congruente, modulo y residuo.

1. Clases módulo m; notación para congruencias.
2. Las clases modulo m forman una particion de los enteros.
3. Residuos mínimos.
4. Congruencias segón modulos compuestos; transitividad de congruencias.
5. Sumas de nómeros congruentes.
6. Multiplos de nómeros congruentes.
7. Productos de numeros congruentes.
8. Polinomios de nómeros congruentes.
9. Período de un polinomio módulo m.
10. Criterio necesario para resolver polinomios racionales.
11. Aplicaciones de la teoría a las reglas de aritmetica elemental.

SECCION SEGUNDA. SOBRE LAS CONGRUENCIAS DEL PRIMER GRADO

1. Lema para §14.
2. Si p\ab entonces p\a o p\b.
3. Extensión de §14 a productos de varios factores.
4. Teorema fundamental de aritmetica.
5. Fórmula para τ(A), el nómero de factores de un entero compuesto A.
6. Cólculo del maximo común divisor y mínimo comón multiplo.
7. Proposiciones elementales acerca de enteros relativamente primos.
8. Factorizacion primaria de una n-esima potencia.
9. Factores de una n-esima potencia.
10. División de una congruencia por un factor relativamente primo al módulo.
11. Si a y m son relativamente primos, a genera los enteros módulo m aditivamente.
12. Solubilidad de una congruencia lineal modulo m.
13. Congruencias trascendentales y algebraicas.
14. La solución de una congruencia consiste de varias clases de congruencia.
15. Algoritmo para resolver una congruencia lineal módulo un primo.
16. Metodo de Euler y Lagrange usando fracciones continuas.
17. Reduccion del caso de un módulo compuesto.
18. Otro metodo para el caso de un modulo compuesto.
19. Cocientes modulo c.
20. Teorema chino del residuo.
21. Caso de §32 cuando los módulos son primos entre sí.
22. Posibilidad de que una congruencia sea superflua o inconsistente.
23. Ejemplo numerico del Teorema chino del residuo.
24. Otro algoritmo si los modulos son relativamente primos.
25. Sistemas de congruencias lineales.
26. Cólculo de la función φ(Α) de Euler.
27. Inversion de Mobius de la función de Euler.
28. El móximo común divisor como combinacion lineal.
29. Divisibilidad de un coeficiente multinomial por un primo.
30. El lema de Gauss para un producto de polinomios con coeficientes racionales.
31. Una congruencia de grado m tiene a lo sumo m raíces.
32. Comentarios sobre el teorema de §43.

SECCION TERCERA. SOBRE RESIDUOS DE LAS POTENCIAS.

1. En el grupo multiplicativo U(p) de enteros relativamente primos al modulo p, todo elemento es de orden finito menor que p.
2. Subgrupo generado por un elemento a E U(p).
3. Calculo de potencias modulo p.
4. Si |a| = t y ak ξ 1 (mod. p), entonces t|k.
5. Si p es primo, a E U(p) y |a| = t, entonces t|p — 1.
6. El pequeño teorema de Fermat: ap-1 ξ 1 (mod. p), un primo que no divide a a.
7. La p-esima potencia de una suma es la suma de las pAsimas potencias mod. p.
8. Si d|p, ¿cual es el numero φ(ά) de elementos de U(p) de orden d?
9. La prueba de que φ(ά) = ^>(d) o φ(ά) = 0.
10. En efecto ψ^) = <^(d).
11. Existencia de raíces primitivas modulo p; una segunda prueba de esto.
12. Historia de pruebas anteriores de la existencia de raíces primitivas.
13. El índice de un elemento b respecto a una raíz primitiva a modulo p.
14. Indice de un producto y de una potencia.
15. Indice de un cociente.
16. Calculo de raíces modulo p.
17. Calculo directo de raíces de la unidad modulo p: primera reducción.
18. Raíces cuadradas de la unidad.
19. Calculo directo de raíces de la unidad: segunda reduccion.
20. ¿Cuando es —1 un residuo cuadratico?
21. Calculo de n-esimas raíces cuando n|p — 1.
22. ¿Cuando existen n-esimas raíces de A modulo p?
23. Calculo del orden t de A modulo p.
24. Calculo de las demas raíces a partir de una.
25. Cambio de raíz primitiva como base.
26. Invariancia del m. c. d. del índice y p — 1.
27. Eleccion de la base para que un entero tenga un índice determinado.
28. Escogencia conveniente de la raíz primitiva como base.
29. Algoritmo para encontrar raíces primitivas.
30. Ejemplo de encontrar una raíz primitiva modulo 73.
31. Producto de los elementos de un subgrupo c íclico de U(p).
32. El Teorema de Wilson: (p — 1)! ξ —1 (mod. p).
33. Segunda prueba del Teorema de Wilson.
34. Generalizacion del Teorema de Wilson a bases compuestas.
35. Suma de los elementos de un subgrupo cíclico de U(p).
36. Producto de todas las raíces primitivas.
37. Suma de todas las raíces primitivas.
38. Caso de módulos compuestos.
39. Orden de a £ U(m) divide a φ(Μ).
40. No hay mós que t raíces tAsimas de 1 modulo pn.
41. Nómero exacto de raíces t-esimas de 1 módulo pn.
42. Prueba de §85: primera parte.
43. Prueba de §85: segunda parte.
44. Prueba de §85: tercera parte.
45. Cólculos con raíces primitivas módulo pn.
46. Móximo orden en U (2n).
47. Cólculos con óndices módulo 2n.
48. Cólculos modulo un entero compuesto.
49. Trabajos de Euler sobre estos temas.

SECCION CUARTA. SOBRE LAS CONGRUENCIAS DE SEGUNDO GRADO.

1. Numero maximo posible de residuos cuadraticos modulo m.
2. Definición de residuo y no residuo.
3. Numero de residuos cuadraticos modulo p primo.
4. Segunda prueba de §96; ejemplos con p < 17.
5. AB es un residuo sii A y B son ambos residuos o ambos no residuos.
6. ¿Cuando un producto de varios factores es un residuo?; uso de tablas.
7. Numero de residuos cuadraticos modulo pn.
8. Si a no es divisible por p, es un residuo de p sii es un residuo de pn.
9. ¿Cuando un entero divisible por p es un residuo modulo pn?
10. Residuos cuadraticos modulo 2n.
11. Numero de raíces λ/Α si A es un residuo modulo pn.
12. Numero de raíces \/A si A es un residuo modulo m cualquiera.
13. Criterio de Euler para residuos cuadraticos.
14. Problema fundamental: dado a, encontrar todo p del cual a es un residuo.
15. —1 es un residuo de p primo sii p = 4n +1.
16. Otra prueba de §108.
17. Referencia al trabajo de Euler; relacion al Teorema de Wilson.
18. Caracterizacion de los enteros para los cuales —1 es un residuo.

Estudio de §107 cuando a = ±2 y p ξ 3 o 5 (mod. 8).

Estudio de §107 cuando a = ±2 y p ξ 7 (mod. 8).

112.

113.

114.

115.

116.

117.

118.

119.

1. 121. 122.

123.

124.

125.

126.

127.

128.

129.

130.

131.

132.

133.

134.

135.

136.

137.

138.

139.

140.

141.

142.

143.

144.

145.

146.

Estudio de §107 cuando a = ±2 y p ξ 1 (mod. 8).

Otra prueba de §114.

Caracterización de los enteros para los cuales ±2 es un residuo; historia. Estudio de §107 cuando a = ±3 y p ξ 5 u 11 (mod. 12).

Estudio de §107 cuando a = ±3 y p ξ 7 (mod. 12).

Estudio de §107 cuando a = ±3 y p ξ 1 (mod. 12).

Caracterizacioón de los enteros para los cuales ±3 es un residuo; historia. Estudio de §107 cuando a = ±5 y p ξ 2 o 3 (mod. 5).

Estudio de §107 cuando a = ±5 y p Ξ 1 ni 9 (mod. 20).

Ley de Reciprocidad Cuadrática para a = ±5.

Discusión de §107 cuando a = ±7.

Todo p ξ 1 (mod. 4) es un no residuo de algun primo q < p; prueba si p ξ 5 (mod. 8).

Primer lema para probar el caso p ξ 1 (mod. 8) de §125.

Segundo lema para probar el caso p ξ 1 (mod. 8) de §125.

Tercer lema para probar el caso p ξ 1 (mod. 8) de §125.

Prueba de §125.

Evidencia numerica para la Ley de Reciprocidad Cuadrática.

Enunciado de la Ley de Reciprocidad Cuadróatica; notacióon. Consecuencias de §131 con numeros compuestos.

Reciprocidad cuadrática generalizada a enteros compuestos.

Prueba de §133, suponiendo §131.

Ley de Reciprocidad Cuadrática (L. R. C.): hipótesis inductiva.

comienzo de la induccióon; divisioón en casos. caso 1, a ξ p ξ 1 (mod. 4), ±pRa. caso 2, a ξ 1, p ξ 3, ±pRa. caso 3, a ξ p ξ 1, ±pNa. caso 4, a ξ 1, p ξ 3, ±pNa. caso 5, a ξ p ξ 3, pRb. caso 6, a ξ 3, p ξ 1, pRb. caso 7, a ξ p ξ 3, pNb. caso 8, a ξ 3, p ξ 1, pNb.

Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C. Prueba de L. R. C.

Otra prueba de §114.

Resumen del metodo para determinar si Q es un residuo de P; ejemplo.

1. Formas de los divisores de x2 — A: enunciado.
2. Prueba de §147 cuando A ξ 1 (mod. 4).
3. Prueba de §147 cuando A ξ 2 o 3 (mod. 4).
4. Corolario de §147 con B compuesto.
5. Historia de la Ley de Reciprocidad Cuadrática.
6. Resolucián de congruencias ax2 + bx + c ξ 0.

SECCION QUINTA. SOBRE LAS FORMAS Y LAS ECUACIONES INDETERMINADAS DE SEGUNDO GRADO.

1. Definición de formas cuadráticas; notación.
2. Representacion de un námero M; el determinante.
3. La raíz cuadrada \/D del determinante es una clase mádulo M.
4. Representaciones que corresponden a valores iguales u opuestos de \/~D.
5. Transformaciones lineales de formas; formas equivalentes; transformaciones propias e impropias.
6. Equivalencia propia e impropia; ejemplo; problemas a ver.
7. Transitividad de implicacián de formas; formas opuestas.
8. Formas contiguas.
9. Divisores comunes de los coeficientes de formas.
10. Encontrar todas las transformaciones de una forma a otra que la contiene.
11. Formas ambiguas.
12. Condiciáon necesaria y suficiente para que una forma implique a otra propia e impropiamente.
13. Ejemplo de §164; existencia de una forma ambigua en una clase.
14. Representaciáon de nuámeros por formas transformadas.
15. Determinantes de formas equivalentes.
16. Toda representaciáon de un entero M conduce a una forma propiamente equivalente con primer coeficiente M.
17. Aplicacion de la teoría de transformaciones a la de representaciones.
18. Caso de §168 con una forma ambigua.
19. Formas con determinante negativo: reduccioán a forma reducida.
20. Condiciones para que dos formas reducidas de determinante — D sean propiamente equivalentes.
21. Condiciones para que dos formas reducidas de determinante — D sean equivalentes.
22. El námero de formas reducidas de determinante —D.
23. Clases de formas de determinante — D.
24. Tabla de clases de formas de determinante —D, D < 12.
25. Transformaciones propias entre formas contiguas.
26. Calculo de una transformación propia entre formas propiamente equivalentes.
27. Calculo de todas las transformaciones entre formas equivalentes.
28. Algoritmo para encontrar todas las representaciones de M por una forma de determinante — D.
29. Caso de §180 con coeficientes no relativamente primos.
30. Aplicacion a la representation de M como x2 + ny2, n = 1, 2, 3.
31. Formas con determinante positivo no cuadrado: reducción a forma reducida.
32. Propiedades de formas reducidas con determinante positivo no cuadrado.
33. Algoritmos para encontrar todas las formas reducidas de determinante D.
34. Período de una forma F.
35. Propiedades de períodos; formas asociadas.
36. Sustitucion α,β,γ,δ; ejemplo de período de una forma reducida.
37. Signos y otras propiedades de las formas en un período.
38. Lema para §191.
39. Aproximacion racional a \[D.
40. Convergentes de la fracción continuada de \[D.
41. Formas reducidas propiamente equivalentes estan en el mismo período.
42. Otra prueba del Teorema de §165.
43. Algoritmo que determina si formas del mismo determinante son equivalentes.
44. Algoritmo para encontrar una transformación propia entre formas propiamente equivalentes.
45. Relevancia de la ecuación de Pell al estudio de formas.
46. Solucion fundamental de la ecuacion de Pell.
47. Aplicación de fracciones continuadas a §198.
48. Solucion general de la ecuación de Pell.
49. Comentarios sobre la solucion de la ecuación de Pell.
50. Historia de la ecuacion de Pell.
51. Algoritmo para encontrar todas las transformaciones entre formas equivalentes.
52. Observaciones sobre §203.
53. Algoritmo para encontrar todas las representaciones de un entero por una forma dada.
54. Formas reducidas con determinante h2.
55. Toda clase contiene una sola forma reducida.
56. Encontrar una transformation entre formas equivalentes con determinante h2.
57. Encontrar las demás transformaciones de §208.
58. Criterio para equivalencia impropia de formas reducidas (a, h, 0).
59. Numero de clases de formas de determinante h2.
60. Algoritmo de §205 para el caso de formas de determinante h2.
61. Criterio para que una forma de determinante D implique una de determinante De2.
62. Encontrar todas las transformaciones correspondientes a §213.
63. Formas de determinante igual a cero.
64. Resolución de la ecuación cuadrática general de dos incógnitas.
65. Continuation de §216.
66. Caso de §216 con determinante cuadrado y M = 0.
67. Caso general de §216 con determinante cero.
68. Caso especial de §216 con determinante cero.
69. Ejemplo del metodo de §217.
70. Notas historicas acerca de formas cuadráticas.
71. Division de las formas de determinante D en clases.
72. Usos de las clases; clases opuestas; clases ambiguas.
73. Clases positivas y negativas.
74. Formas primitivas; division de clases en ordenes; ejemplos.
75. Uso de clases propiamente primitivas.
76. Una forma primitiva representa un námero infinito de enteros no divisibles por p.
77. Una forma primitiva representa solo residuos o sólo no residuos modulo p.
78. Caracteres de una forma primitiva.
79. Division de ordenes en generos; forma principal.
80. Ejemplos con clases positivas y negativas.
81. Raíz cuadrada de una forma; námeros característicos de una forma.
82. Lema para §239 y §240.
83. Forma compuesta; seis propiedades.
84. Construction de una forma compuesta.
85. Forma compuesta de formas transformadas.
86. Forma compuesta de formas equivalentes.
87. Equivalencia de las compuestas de formas equivalentes.
88. Asociatividad de composition.
89. Asociatividad generalizada de composition.
90. Propiedades de la composition de formas.
91. Clases de formas tienen la estructura de un grupo.
92. Representación de un producto por una forma compuesta.
93. Composicion de ordenes.
94. Composicion de generos.
95. Producto de generos esta bien definido para formas primitivas.
96. Producto de generos esta bien definido en general.
97. Composicion de clases.
98. Forma mas simple de un orden.
99. Una forma primitiva que transforma formas del mismo orden.
100. Existe el mismo número de clases en cada genero del mismo orden.
101. Discusion del número de clases en ordenes distintos.
102. Composiciúon de la forma maús simple de un orden con una primitiva.
103. Clases propiamente primitivas que representan un entero cuadrado.
104. Comparacion del número de clases primitivas de úrdenes distintos.
105. Numero de formas ambiguas primitivas (A, 0,C) y (A, A/2,C).
106. Conteo del número de clases ambiguas propiamente primitivas.
107. Conteo del número de clases ambiguas impropiamente primitivas.
108. Numero de clases propiamente primitivas k con k2 = K.
109. La mitad de los caracteres no pertenece a un genero propiamente primitivo.
110. Otra prueba de la L. R. C. para ciertos residuos.
111. Los caracteres que corresponden a generos.
112. Caracteres para gúeneros negativos y gúeneros impropiamente primitivos.
113. Metodo para descomponer un primo como suma de dos cuadrados.

***Una digresión conteniendo un estudio de formas ternarias.***

1. Introducción al estudio de formas ternarias.
2. Formas ternarias: notacion, adjunta y determinante.
3. Transformacion de formas ternarias.
4. Formas ternarias equivalentes.
5. Transitividad de equivalencia.
6. Clases de formas ternarias; formas positivas, negativas e indefinidas.
7. Reducciúon de formas ternarias.
8. Ejemplos numericos de la reducciún de formas ternarias.
9. Segunda reducciún de formas ternarias.
10. Ejemplos de la composicion de transformaciones de formas ternarias.
11. El número de clases de formas ternarias de determinante D es finito.
12. Ejemplos de formas ternarias reducidas de determinante pequeño.
13. Problemas para considerarse acerca de formas ternarias.
14. Lema para §280.
15. Algoritmo para encontrar las representaciones propias de un entero por una forma ternaria.
16. Representaciones impropias por una forma ternaria.
17. Observaciones acerca de la representación de una forma binaria por una forma ternaria.
18. Algoritmo para encontrar todas las representaciones de una forma binaria por una forma ternaria.
19. Representaciones impropias de una forma binaria por una forma ternaria.
20. Equivalencia de formas ternarias.

***Algunas aplicaciones a la teoría de las formas binarias.***

1. Toda forma del genero principal es el cuadrado de alguna forma.
2. Exactamente la mitad de los caracteres corresponden a géneros propiamente primitivos.
3. Existencia de formas primitivas negativas de determinante — M y numero característico —1.
4. Representaciones de formas binarias por x2 + y2 + z2.
5. Estudio de §289 para formas binarias de determinante —1o —2.
6. Las representaciones de un entero positivo por x2 + y2 + z2.
7. Numero de representaciones por x2 + y2 + z2.
8. Todo entero positivo es la suma de tres números triangulares.
9. Condicion necesaria y suficiente para resolver ax2 + by2 + cz2 = 0.
10. Método alternativo para §294.
11. Trabajo de Legendre acerca de §294.
12. Incompletitud del argumento de Legendre en §296.
13. Caso general de §294.
14. Representaciúon de cero por formas ternarias.
15. Solucion racional de una ecuacion cuadrática con dos incognitas.
16. Comportamiento asintotico del numero de generos.
17. Comportamiento asintotico del numero de clases: determinante negativo.
18. Tablas acerca de §302; conjetura sobre el numero de clase.
19. Nuúmero de clases: determinante negativo.
20. Toda clase es de orden que divide al número de clases.
21. Las clases forman un grupo.
22. Algoritmo para calcular gúeneros y clases; ejemplos.

SECCION SEXTA. APLICACIONES VARIAS DE LAS INVESTIGACIONES PRECEDENTES.

1. Introducción y resumen de la sección.
2. Descomposición de una fracción con denominador ab.
3. Descomposición de una fraccion con denominador abc · · · .
4. Unicidad de la descomposicion de §310.
5. Mantisa decimal de una fraccion.
6. Calculo del numerador a partir de la mantisa y del denominador.
7. Período de una fracción α/ρμ.
8. Cólculo del período de b/pA a partir del período de α/ρμ.
9. Comentarios sobre las tablas de los períodos de fracciones.
10. Metodo de calculo de expansiones decimales en general.
11. Mantisa de una fraccion en el caso general.
12. Metodos para resolver una congruencia x2 ξ A (mod. m).
13. Metodo de exclusion para la congruencia x2 ξ A (mod. m).
14. Numeros excluyentes que conviene escoger en el metodo de exclusion.
15. Atajos que se pueden usar en el metodo de exclusión.
16. Otro metodo para resolver mx2 + ny2 = A.
17. Uso de numeros excluyentes en §323.
18. Un ejemplo del metodo de §323 y §324.
19. Observaciones para acortar el cóalculo en §323.
20. Otro metodo para resolver x2 ξ A (mod. M) cuando A < 0.
21. Ejemplos numericos del metodo de §327.
22. Metodos de factorización de enteros: observaciones elementales.
23. Primer metodo de factorizacion: residuos cuadraticos de M.
24. Tecnicas para la aplicacion de §330.
25. Tres metodos para encontrar los residuos cuadraticos de M.
26. Segundo metodo de factorizacion: valor de V—D (mod. M).
27. Aplicaciones de §333.

SECCION SETIMA. ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

1. Introduccion a la ciclotomía; generalizaciones futuras posibles.
2. Reduccion al caso de la division del córculo en p (primo) partes.
3. Las raóces de xn — 1 son exp(2nk/n) = cos(2nk/n) + i sen(2nk/n).
4. La fórmula de Newton para la suma de las AAsimas potencias de las raóces.
5. La estructura cíclica de las raíces Ω de un polinomio ciclotomico X.
6. Sustitución de raíces de un polinomio ciclotomico en un polinomio.
7. Irreducibilidad de polinomios ciclotomicos sobre los racionales.
8. Factorización del polinomio ciclotomico depende de p — 1.
9. Subgrupos y clases laterales de las raíces de un polinomio ciclotomico.
10. Clases laterales de Ω forman una partición.
11. Productos de períodos en Ω.
12. Grado de subextensiones del campo ciclotómico.
13. Sustitucion de un período en un polinomio simetrico.
14. Coeficientes de un polinomio son funciones simetricas de las raíces.
15. Aplicacion del Teorema de Newton al calculo de los coeficientes.
16. Generalizacion de §347 con subperíodos.
17. Calculo de polinomio mínimo de un período; ejemplo n = 19.
18. Algoritmo para encontrar las raíces de un polinomio ciclotomico.
19. Cílculo completo de §352 cuando n = 19.
20. Cílculo completo de §352 cuando n = 17.
21. Uso de numeros complejos en §352.
22. Calculo de sumas gaussianas.

***η,ο o-,***

1. El polinomio ciclotómico se descompone como g(y ^ pz2).
2. Distribucion de las raíces Ω en tres períodos.
3. Conjetura de la imposibilidad de resolver polinomios de grado > 5 por radicales.
4. Uso de resolventes de Lagrange para resolver el polinomio ciclotómico.
5. Calculo de sen ω y cos ω donde ω = 2'nk/n.
6. Cílculo de las otras funciones trigonometricas de ω.
7. Factorizacion del polinomio con raíces sen kω, etc.
8. Observaciones sobre §363; automorfimos de una extension; ejemplos.
9. Se construye un p-gono sii p es un primo de Fermat.
10. Caracterizacion de los n para los cuales el n-gono es construible.

AL SERENISIMO

PRINCIPE Y SEÑOR  
CARLOS GUILLERMO FERNANDO  
DUQUE DE BRUNSWICK Y LUNEBURG

SERENISIMO PRINCIPE

Considero como mi mayor fortuna que VOS me permitáis adornar este trabajo con VUESTRO honorabilísimo nombre. Estoy obligado por un sagrado deber a ofreceroslo a VOS. Si no fuera por vuestro favor, Serenísimo Príncipe, no habría realizado mi primer acercamiento a las ciencias. Si no fuera por VUESTROS beneficios incesantes en apoyo de mis estudios, no habría estado en capacidad de dedicarme completamente a mi apasionado amor, el estudio de las matemaíticas. Ha sido exclusivamente VUESTRA generosidad la que me ha permitido liberarme de otras preocupaciones, dedicarme muchos años a la contemplación y estudio fructíferos, y finalmente darme la oportunidad de anotar en este volumen algunos de los resultados de mis investigaciones. Cuando al fin estuve preparado para presentar mi trabajo al mundo, fue exclusivamente VUESTRA munificencia la que removio todos los obstaculos que retardaron continuamente su publicación. Tanta ha sido VUESTRA generosidad hacia mí y mis esfuerzos que mías bien puedo admirarla con espíritu agradecidísimo y admiración silenciosa que celebrarla con los encomios justamente merecidos. Porque no sílo me siento difícilmente a la altura de este oficio, sino tambien todos conocen VUESTRA extraordinaria liberalidad hacia todo

aquel que se dedica a las disciplinas superiores. Todos saben que VOS nunca habéis excluido de VUESTRO patrocinio a aquellas ciencias que comúnmente son vistas como demasiado recúnditas y demasiado alejadas de la vida ordinaria. VOS MISMO en VUESTRA suprema sabiduría estais bien enterado del íntimo y necesario lazo que une a todas las ciencias entre sí y con cualquier cosa que atañe a la prosperidad de la sociedad humana. Por ende, presento este libro como un testimonio de mi profundo respeto hacia VOS y de mi dedicación a la mas noble de las ciencias. Serenísimo Príncipe, si VOS juzgais merecedor del extraordinario favor que siempre me habeis prodigado, me congratulare de que mi trabajo no haya sido en vano y de que haya sido favorecido con un honor que aprecio por encima de todos los demas.

SERENISIMO PRINCIPE

Brunswick, en el mes de julio de 1801

De Vuestra Alteza, el mas dedicado servidor

C.F. GAUSS

PREFACIO.

Las investigaciones contenidas en este volumen pertenecen a la parte de la Matemática que trata de los números enteros, y a veces de las fracciones pero nunca de los irracionales. El analisis llamado indeterminado o Diofúntico que muestra la forma de seleccionar de entre las infinitas soluciones de un problema indeterminado aquellas que son enteras o al menos racionales (usualmente con la condiciún adicional que deben ser positivas) no es la disciplina a la cual nos referimos, sino mús bien a una parte verdaderamente especial, relacionada con ella en túerminos generales como se relaciona el arte de reducir y resolver ecuaciones (Algebra) con el Anúlisis general. Tal como incluimos bajo el título Análisis todas las discusiones que involucran cantidades, asú los enteros (y las fracciones en tanto que estan determinadas por enteros) constituyen el objeto propio de la ARITMETICA. Sin embargo, lo que comúnmente es llamado Aritmetica, escasamente se extiende mas alla del arte de enumerar y calcular (i.e., expresar los numeros mediante súmbolos idúneos, por ejemplo, por una representaciún decimal, y llevar a cabo operaciones aritmeticas). A menudo incluye algunos temas que realmente no pertenecen a la Aritmetica (como la teoría de logaritmos) y otros que no son propios de los enteros sino comunes a todas las cantidades. Se ve como resultado que se debe dividir la Aritmetica en dos partes: la Aritmetica Elemental y la Aritmetica Superior. La segunda incluye todas las investigaciones generales acerca de las propiedades especiales de los enteros, y es la única que tratamos en este volumen.

Incluidos bajo el tútulo Aritmetica Superior estan aquellos tópicos que Euclides trato en Libros VII y siguientes de los Elementos con la elegancia y el rigor habitual entre los antiguos, pero estan limitados a los rudimentos de la ciencia. La celebre obra de Diofanto, dedicada totalmente a problemas indeterminados contiene muchos resultados que provocan una apreciacion mas alla de lo ordinario por la ingeniosidad y habilidad del autor, a causa de las dificultades que enfrento y los sutiles artificios que uso, especialmente si consideramos las pocas herramientas que pudo usar. Sin embargo, demandan una cierta destreza y una manipulation habil mas que principios profundos, y dado que las cuestiones son muy especializadas y rara vez conducen

a conclusiones más generales, se ve que el libro de Diofanto marca una época en la historia de las Matematicas, más debido a que presenta los primeros trazos del arte característico del Algebra que a causa de que haya enriquecido la Aritmetica Superior con nuevos descubrimientos. Se debe mucho mas a los autores modernos, de los cuales aquellos pocos hombres de gloria inmortal, P. DE FERMAT, L. EULER, L. LAGRANGE, A. M. LEGENDRE (y otros pocos) abrieron la entrada al santuario de esta ciencia divina y revelaron abundantes riquezas dentro de el. No haremos aquá un recuento de los descubrimientos individuales de estos geoámetras puesto que se pueden encontrar en el Prefacio del Apendice que Lagrange agregá al Algebra de Euler y en el reciente volumen de Legendre (que citaremos luego). Tambien citaremos muchos de ellos en el lugar apropiado dentro de estas Disquisiciones.

El proposito de este volumen, cuya publicación prometí hace cinco anos, es divulgar mis investigaciones en la Aritmáetica Superior, tanto las iniciadas por aquellos días como las posteriores. Para que nadie se sorprenda porque comienzo casi desde el principio y trato nuevamente muchos resultados que ya han sido estudiados activamente por otros, debo explicar que cuando primero me encamine a este tipo de investigaciones, a principios de 1795, no estaba al tanto de los modernos descubrimientos en el campo y no tenía los medios para descubrirlos. En efecto, ocupado en otro trabajo, me encontré con un extraordinario resultado aritmetico (si no me equivoco, fue el teorema del artículo 108); puesto que lo considere bellísimo en sí mismo y en vista de que sospeche su conexion con resultados aín mas profundos, concentre en el todos mis esfuerzos, con el fin de entender los principios de los que dependía y para obtener una prueba rigurosa. Cuando tuve exito en esto, me atrajeron tanto estos asuntos que no pude dejarlos. Así, mientras un resultado conducía a otro, había completado la mayor parte de lo que se presenta en las cuatro primeras secciones de esta obra antes que entrara en contacto con trabajos similares de otros geometras. Una vez que estuve en capacidad de estudiar los escritos de estos hombres de genio, reconocí que la mayor parte de mis meditaciones habían sido agotadas en materias ya bien desarrolladas. Pero esto solo me estimulí un mayor interes, y caminando sobre sus pasos intente extender la Aritmetica mas alla, logrando resultados que estan incorporados en las secciones V, VI y VII. Despues comence a considerar la publicaciín de los frutos de mis investigaciones y me deje persuadir de no omitir ninguno de los primeros resultados, porque en ese momento no había ningín libro que pusiera juntos los trabajos de otros geometras, dispersos como estaban dentro de los Comentarios de las Academias eruditas. Por otra parte, muchos de los resultados eran nuevos, la mayoría fueron tratados por nuevos metodos y los ultimos resultados estaban tan ligados con los viejos que no podían explicarse sin repetir desde el inicio.

En el ínterin apareció un trabajo sobresaliente de un hombre a quien la Aritmética Superior ya debe mucho, “Essai d’une theorie des nombres” (Paris, año VI) de Legendre, donde el reune y sistematiza no solamente todo lo que habla sido descubierto hasta esa fecha sino tambien muchos nuevos resultados propios. Ya que ese libro llego a mis manos despues de que gran parte de mi trabajo estaba levantado, no pude referirme a el en secciones analogas de mi libro. Sin embargo, me sentí obligado a agregar Notas Adicionales en algunos pasajes y confío que este comprensivo e ilustre hombre no se ofendera.

La publicacion de mi trabajo se vio estorbada por muchos obstaculos a lo largo de un período de cuatro años. Durante este tiempo no solo continue investigaciones que ya había emprendido y aplazado para una fecha posterior de modo que el libro no fuera demasiado extenso, sino tambien acometí nuevas investigaciones. De modo semejante, muchos asuntos que asumí solo a la ligera, porque un tratamiento mas detallado parecía menos necesario (e.g., los contenidos de los artículos 37, 82 y siguientes, y otros), han sido desarrollados en mayor grado y han conducido a resultados mas generales que parecen dignos de publicacion (vease la Nota Adicional en artículo 306). Finalmente, ya que el libro se hizo mucho mas extenso de lo que yo esperaba, debido al tamanño de la Seccion V, acorte mucho de lo que primeramente intente hacer y, en particular, omití toda la Seccion ocho (aun cuando en ocasiones me refiero a ella en el presente trabajo; iba a contener un tratamiento general de las congruencias algebraicas de rango arbitrario). Todas estas cosas, que llenarían facilmente un libro del tamanño de este, se publicaran en la primera oportunidad.

En varias cuestiones difíciles he usado pruebas sinteticas y he suprimido el analisis que conduce a los resultados. Esto fue necesario por brevedad, una consideracion que hubo que tener en cuenta tanto como fuera posible.

La teor ía de la division de un c írculo o de polígonos regulares, tratada en la Seccion VII, en sí misma no pertenece a la Aritmetica, pero los principios involucrados dependen exclusivamente de la Aritmetica Superior. Los geometras pueden sorprenderse de este hecho en s í, tanto como espero que estarán complacidos con los nuevos resultados que se derivan de este tratamiento.

Estas son las cosas acerca de las cuales quería prevenir al lector. No me corresponde a mí juzgar el trabajo mismo. Mi mayor esperanza es que el complazca a aquellos que se interesan en el desarrollo de las ciencias, ya sea suministrando soluciones que ellos buscaban o abriendo el camino para nuevas investigaciones.

DISQUISITIONES ARITHMETICAE.

Sección Primera

DE

LA CONGRUENCIA DE LOS NUMEROS EN GENERAL

***Números congruentes, módulos, residuos y no residuos.***

1.

Si un número a divide la diferencia de los números b y c, se dice que b y c son congruentes según el modulo a; si no lo son, se dice que son incongruentes; el número a se llama módulo. Ambos números b y c, en el primer caso, son llamados uno residuo del otro y, en el segundo caso, no residuos.

Tales nociones valen para todos los enteros, tanto positivos como negativos[[100]](#footnote-101)), y no para las fracciones. Por ejemplo, —9 y +16 son congruentes según el modulo 5; —7 es un residuo de +15 segun el modulo 11; pero no es un residuo segun el modulo

1. Dado que cada número divide a cero, todo número puede considerarse congruente consigo mismo, según cualquier modulo.

2.

Todos los residuos de un número dado, a, según el modulo m están comprendidos en la formula a + km, donde k es un numero entero indeterminado. Las proposiciones mús fúciles, a las cuales haremos referencia mas adelante, pueden demostrarse aquí sin dificultad alguna, y quienquiera podrú comprobar su veracidad con igual facilidad.

Señalaré la congruencia de los números mediante este símbolo ‘=’ y, cuando sea necesario, pondré el múdulo entre paréntesis; por ejemplo, -16 = 9 (mod. 5), -7 = 15 (mod. 11)[[101]](#footnote-102)).

3.

TEOREMA. ***Dados m números enteros sucesivos a, a*** +1, ***a*** + 2, ...a + m — 1,

***y dado otro entero A, uno y solo uno de estos enteros será congruente a A según el modulo m.***

Si a—A es un entero, entonces a = A; si a—A es una fracciún, sea k el prúximo mayor entero positivo (y si es negativo, el proximo menor, sin considerar el signo). A + km, que estaré entre a y a + m, serú el numero buscado. Es evidente que todos los cocientes —A, a+1-A, y a+2~A, etc. estún ubicados entre k — 1 y k + 1; por lo

r r r

que solo uno de ellos puede ser entero.

***Residuos mánimos.***

4.

Así, pues, cada numero tendré un residuo, tanto en la sucesiún 0, 1, 2, ...m— 1, como en 0, —1, —2, ... —(m — 1) a los que llamamos residuos mánimos. Es evidente que, a no ser que 0 sea un residuo, siempre se presentan en pares: uno positivo y el otro negativo. Si son diferentes en magnitud, uno serú < y; de otro modo, cada uno sera = y sin considerar signos. De donde es evidente que cada numero tiene un residuo no mayor que la mitad del modulo, al que se llamara residuo absolutamente mínimo.

Por ejemplo: —13 tiene, según el múdulo 5, un residuo múnimo positivo que es un residuo absolutamente múnimo; —3 es el residuo minimo negativo; +5 es residuo mínimo positivo de sú mismo, según el múdulo 7; —2 es el residuo múnimo negativo, y a la vez, absolutamente múnimo.

***Proposiciones elementales sobre congruencias.***

5.

Establecidos estos conceptos, reflexionemos sobre las propiedades de los números congruentes que son inmediatamente obvias.

***Los números congruentes, según un módulo compuesto, también serán con­gruentes segUn cualquier factor de este modulo.***

***Si varios números son congruentes a un mismo número según un mismo módulo, seran congruentes entre sé*** (según el mismo modulo).

Esta identidad de modulos se debe sobreentender, tambien, en lo siguiente:

***Los numeros congruentes poseen los mismos residuos ménimos; los números no congruentes poseen diferentes residuos ménimos.***

6.

***Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., que son respectivamente congruentes a ellos según un múdulo cualquiera, es decir,*** A ξ ***a, B*** *ξ* ***b, etc. entonces, A*** + B + C + etc. ξ ***a*** + b + c + etc.

***Si A*** *ξ* ***a, B*** *ξ* ***b, entonces A — B*** *ξ* ***a — b.***

7.

***Si A*** *ξ* ***a, entonces, tambiún kA*** *ξ* ***ka.***

Si k es un numero positivo, entonces este es un caso particular del artículo anterior (art. 6), suponiendo que A = B = C etc., y a = b = c etc. Si k es negativo, entonces, —k sera positivo, de donde —kA ξ —ka, de tal modo que kA ξ ka.

***Si A*** *ξ* ***a, B*** *ξ* ***b, entonces AB*** *ξ* ***ab, pues AB*** *ξ* ***Ab*** *ξ* ***ab.***

8.

***Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., respectivamente congruentes a aquellos, esto es si A*** *ξ* ***a, B*** *ξ* ***b, etc., los productos de cada uno de ellos serún congruentes, ABC*** etc. ξ ***abc*** etc.

Del artículo anterior, se tiene AB ξ ab, y, por la misma razón, ABC ξ abc, así para cualquier número de factores.

Si todos los números A, B, C, etc. se suponen iguales, y también los correspondientes a, b, c, etc., se tiene este teorema: Si A ξ a y k es un entero positivo, entonces Ak ξ ak.

9.

***Sea X una función algebraica de la indeterminada x, de la forma***

Axa + Bxb + Cxc + etc.

***donde A, B, C, etc., son nómeros enteros cualesquiera, y donde a, b, c, etc. son enteros no negativos. Entonces, si se dan valores congruentes a la indeterminada x, según cualquier modulo entero, los valores correspondientes de la función X serán congruentes.***

Sean f y g valores congruentes de x. Luego, por el artículo anterior, fa ξ ga y Afa ξ Aga, y del mismo modo Bfb ξ Bgb, etc. Entonces,

Afa + Bfb + Cfc + etc. ξ Aga + Bgb + Cgc + etc. Q. E. D.

Facilmente se infiere como puede ser extendido el teorema a las funciones de varias indeterminadas.

10.

Si se sustituye x por todos los nuúmeros enteros, consecutivamente, y si se reducen los valores de la función X a los residuos mínimos, entonces estos formarún una sucesion en la que despues de un intervalo de m terminos (tomando a m como el modulo) los mismos terminos se repetirán de nuevo. Entonces, la serie estarú formada por un período de m terminos repetido infinitamente. Por ejemplo, sea X = x3—8x+6 y m = 5; entonces para x = 0, 1, 2, 3, etc. los valores de X producen estos residuos mínimos positivos: 1, 4, 3, 4, 3, 1, 4, etc. donde los primeros cinco numeros 1, 4, 3, 4, 3 se repiten indefinidamente y, si la sucesiún se continúa en el sentido contrario, esto es, si se dan valores negativos a x, el mismo período aparece con los terminos en el orden inverso. De donde, resulta evidente que no pueden tener lugar otros terminos en cualquier sucesion, excepto aquellos que constituyen este período.

11.

Por lo tanto, en este ejemplo, X no puede ser ni ξ 0, ni ξ 2 (mod. 5), ni mucho menos = 0 ni = 2. De donde, se deduce que las ecuaciones x3 — 8x + 6 = 0, y x3 — 8x + 4 = 0 no pueden resolverse con numeros enteros, y, como se sabe, tampoco con racionales. Mas generalmente, es evidente que, cuando X es una función de la incognita x, de la forma

xn + Axn 1 + Bxn 2 + etc. + N

donde A, B, C, etc. son enteros y n es un entero positivo (en realidad todas las ecuaciones algebraicas pueden reducirse a esta forma), la ecuación X = 0 no tiene ninguna raíz racional, si la congruencia X ξ 0 no puede satisfacerse para ningun modulo. Aunque este criterio se nos presento espontaneamente, sera tratado mas ampliamente en la Sección VIII. A partir de este ejemplo se puede formar alguna idea sobre la utilidad de estas investigaciones.

***Algunas aplicaciones.***

12.

Muchas cosas que suelen ensenarse en aritmetica dependen de los teoremas expuestos en esta sección, e.g., las reglas para averiguar la divisibilidad de un nómero dado por 9, 11 u otro. Según el modulo 9 todas las potencias del nómero 10 son congruentes con la unidad: por eso, si un nómero dado tiene la forma

a + 10b + 100c + etc., entonces dará, segón el módulo 9, el mismo residuo mínimo que a + b + c + etc. Así, es evidente que, si los dígitos de un nómero expresado en decimales se suman uno a uno sin tener en cuenta el lugar que ocupan, esta suma y el numero dado presentan los mismos residuos mínimos, de tal modo que este ultimo puede dividirse entre 9, si aquel es divisible entre 9 y viceversa. Lo mismo es cierto para el divisor 3. Puesto que según el módulo 11, 100 ξ 1 sera, en general 102k ξ 1,

102k+1 ξ 10 ξ — 1,

y un numero de la forma a + 10b + 100c + etc. dará, segun el modulo 11, el mismo residuo mínimo que a — b + c etc.; de donde de inmediato se deriva la regla conocida. De este mismo principio, se deducen todas las reglas similares.

De lo anterior se puede inferir el principio de las reglas dadas para la verificacion de las operaciones aritmeticas. Desde luego, si de los números dados, se derivan otros ya sea por suma, resta, multiplicacióon o elevacióon a potencia, se

sustituyen los residuos mínimos en lugar de los números dados, según un módulo arbitrario (por lo general se usan 9 u 11, porque como lo presentamos en nuestro sistema decimal, según estos, los residuos pueden hallarse con facilidad). Por esto, los resultados deben ser congruentes con los que se derivaron de otros dados; porque si no sucediera así, se concluiría que se ha cometido un error en el calculo.

Pero, puesto que estos resultados son bastante conocidos y semejantes con los anteriores, sería innecesario detenerse en ellos.

Sección Segunda

SOBRE

LAS CONGRUENCIAS DEL PRIMER GRADO

***Teoremas preparatorios sobre los números primos, factores, etc.***

13.

TEOREMA. ***El producto de dos números positivos, mas pequeños que un número primo dado, no puede dividirse por este numero primo.***

Sea p primo, y a positivo < p: entonces no puede encontrarse ningún número positivo b menor que p tal que ab = 0 (mod. p).

Demostración. Si se niega el teorema, tendremos números b, c, d, etc., todos < p, tales que ab = 0, ac = 0, ad = 0, etc., (mod. p). Sea b el menor de todos estos, tal que ningún numero menor que b tenga esta propiedad. Es evidente que b > 1: pues si b =1, entonces ab = a < p (por hipútesis) y por lo tanto no es divisible por p. Ahora, como p es primo, no puede dividirse por b pero estú comprendido entre dos multiplos sucesivos de b, mb y (m + 1)b. Sea p — mb = b0; así b0 serú un numero positivo y < b. Ahora, como suponemos que ab = 0 (mod. p), tambien tenemos mab = 0 (por art. 7), y restando este de ap = 0 resulta a(p — mb) = ab0 = 0; esto es: b0 tiene que ser uno de los nuúmeros b, c, d, etc., aunque resulta menor que el menor de tales números, b. Q. E. A.

14.

***Si ni a ni b pueden dividirse por un numero primo p, tampoco el producto ab puede dividirse por p.***

Sean α y β los menores residuos positivos de los números a y b, respectiva­mente, según el múdulo p. Ninguno de ellos es cero (por hipútesis). Ahora, si ab = 0 (mod. p), entonces αβ = 0, puesto que ab = αβ. Pero esto contradice el teorema anterior.

Euclides ya había demostrado este teorema en sus Elementos (libro VII, No. 32). No obstante deseabamos no omitirlo puesto que muchos autores modernos han usado razonamientos inciertos en vez de demostraciones, o bien han despreciado el teorema completamente. Ademas, mediante este uso muy sencillo, podemos con mas facilidad comprender la naturaleza del metodo que se usara mús adelante para resolver problemas mucho mas difíciles.

15.

***Si ninguno de los números a, b, c, d, etc., puede dividirse por un número primo p, tampoco puede dividirse por p el producto abcd etc.***

Según el artículo anterior, ab no puede dividirse por p; por lo tanto, tampoco abc, ni tampoco abcd, etc.

16.

TEOREMA. ***Cualquier numero compuesto puede resolverse en factores primos de una manera única.***

Demostración. Que cualquier número compuesto pueda resolverse en factores primos, resulta de consideraciones elementales, pero estú supuesto tacitamente, y en general sin demostraciúon, que no puede hacerse de muchas maneras diferentes. Supongamos que algun número compuesto A, que es = aabβC etc., donde a, b, c, etc. denotan números primos diferentes, es resoluble en factores primos de otra manera.

Primero, es claro que no puede aparecer en este segundo sistema de factores ninguún otro primo mas que a, b, c, etc. puesto que ninguún otro primo puede dividir a A, el cual esta compuesto de estos primos. De forma semejante, ninguno de los primos a, b, c, etc. puede estar ausente del segundo sistema de primos, puesto que si no, no podría dividir a A (artúculo anterior). Asú, estas dos resoluciones en factores pueden ser diferentes solamente si un primo aparece múas veces en una resoluciúon que en la otra. Sea p un tal primo que aparece m veces en una resolución, y n veces en la otra, y tal que m > n. Al disminuir en n el número de factores p en cada sistema,

quedarán m — n factores p en un sistema mientras que no quedará ninguno en el otro. Esto es, tenemos dos resoluciones en factores del námero pn. El que una de ellas no contenga al factor p mientras que la otra lo contenga m — n veces contradice lo que acabamos de demostrar.

17.

Si un námero compuesto A es el producto de B, C, D, etc., entonces entre los factores primos de B, C, D, etc., no puede aparecer ninguno que no sea factor de A. Ademas cada uno de estos factores debe aparecer en la resolución de A tantas veces como aparece en B, C, D, etc., en total. Por lo tanto tenemos un criterio para determinar si un námero B divide a un námero A o no. B dividirá a A siempre que contenga solo factores primos de A mismo, y siempre que no los contenga mas veces que A. Si alguna condiciáon no se cumple, B no divide a A.

Es facil ver por el cálculo de las combinaciones que si, como arriba, a, b, c, etc., son numeros primos diferentes y si A = aabβC etc., entonces A tendrá

(α + 1)(β + 1)(γ + 1) etc. divisores diferentes, incluyendo a 1 y a A mismo.

18.

Por lo tanto si A = aabβ(A etc., K = kKl^mA etc., y si los primos a, b, c, etc., k, l, m, etc., son todos diferentes, entonces es claro que A y K no tienen un factor comán aparte de 1, o sea: son primos relativos.

Dados varios numeros A, B, C, etc., el máximo común divisor se determina de la manera siguiente. Supáongase que todos los nuámeros estáan resueltos en sus factores primos, y de estos ultimos se extraen aquellos que sean comunes a A, B, C, etc., (si no hay ninguno, no habrá un divisor comán de todos ellos). Luego, se nota el námero de veces que aparece cada factor primo en A, en B, en C, etc., o sea se nota cuál exponente tiene cada uno de ellos en A, en B, en C, etc. Finalmente asignamos a cada factor el más pequeño de los exponentes que tenga en A, en B, en C, etc. Al formar el producto de estos obtendremos el comán divisor buscado.

Cuando deseamos el mínimo común múltiplo, seguimos el siguiente proced­imiento: se reunen todos los nuámeros primos que dividen a alguno de los nuámeros A,

B, C, etc., y se asigna a cada uno el mayor exponente que tiene en A, B, C, etc. Al formar el producto de estos, tendremos el multiplo que buscamos.

Ejemplo. Sea A = 504 = 23327, B = 2880 = 26325, C = 864 = 2533. Para el maximo común divisor tenemos los factores primos 2 y 3 con los exponentes 3 y 2 respectivamente; esto será 2332 = 72, y el menor número divisible por ellos en común será 26355 · 7 = 60480.

Omitimos las demostraciones debido a su facilidad. Además, sabemos por consideraciones elementales coámo resolver estos problemas cuando la resolucioán de los números A, B, C, etc., no viene dada.

19.

***Si los números a, b, c, etc., son todos primos relativos a k, también su producto será primo relativo a k.***

Como ninguno de los numeros a, b, c, etc., tiene un factor primo común con k, y como el producto abc etc., no tiene factores primos diferentes de los factores primos de uno de los números a, b, c, etc., el producto abc etc., tampoco tendrá ningún factor primo común con k. Por lo tanto se sigue del artículo anterior que k y abc etc. son primos relativos.

***Si los números a, b, c, etc., son primos entre sé, y si cada uno de ellos divide a algún k, entonces su producto divide a k.***

Esto se sigue fúcilmente de los artículos 17 y 18. Sea p un divisor primo del producto abc etc. que lo contiene π veces. Es claro que alguno de los numeros a, b, c, etc., tiene que contener este mismo divisor π veces. Luego tambien k, al cual este número divide, contiene π veces a p. De manera semejante sucede con los restantes divisores del producto abc etc.

Asú, ***si dos números m y n son congruentes segun varios médulos a, b, c, etc., que son primos entre sé, entonces semn congruentes según el producto de ellos.***

Como m — n es divisible por cada uno de los numeros a, b, c, etc., sera divisible por su producto tambien.

Finalmente, ***si a es primo a b y ak es divisible por b, entonces k también es divisible por b. Porque ak es divisible por ambos a y b, es divisible por ab también; es decir*** ab = k ***es un entero.***

20.

***Cuando A = aab***c7 ***etc., donde a, b, c, etc., son números primos distintos, es alguna potencia, digamos kn, todos los exponentes a, β, γ, etc., serán divisibles por n.***

Puesto que el número k no involucra factores primos diferentes de a, b, c, etc., supóngase que k contiene el factor a, a' veces. kn, o A, contendrá este factor na' veces. Por lo tanto na' = a y a es un numero entero. De igual manera se demuestra que n, etc., son numeros enteros.

21.

***Cuando a, b, c, etc., son primos entre sú y el producto abc etc. es alguna potencia, por ejemplo kn, entonces cada uno de los numeros a, b, c, etc., sera una potencia semejante.***

Sea a = l^múpn etc. con l, m, p, etc., numeros primos diferentes. Por hipútesis, ninguno de ellos es factor de los números b, c, etc. Así, el producto abc etc. contendrú λ veces el factor l, μ veces el factor m, etc. Así que (por el artículo anterior) λ, μ, π, etc., son divisibles por n y resulta que

***/— λ μ π***

y a = ln mnpn etc.

es un entero. De manera semejante para los restantes b, c, etc.

Estos teoremas sobre los numeros primos tenían que presentarse primero; ahora nos dedicaremos a las proposiciones propias de nuestros fines.

22.

***Si los números a y b son divisibles por otro numero k, y si son congruentes segun un modulo m que es primo a k, entonces*** | ***y*** | ***serún congruentes según el mismo modulo.***

Es claro que a — b es divisible por k y ademas por m (por hipotesis); así que (art. 19) atT es divisible por m, o sea, | ξ | (mod. m).

Manteniendo iguales las otras cosas, si m y k tienen un maximo comun divisor e, entonces | ξ k (mod. m), puesto que k y m son primos entre sí. Pero a — b es divisible por k y por m, así que es divisible por k y por ™, entonces es divisible por kip; esto es es divisible por m, lo cual implica que | ξ | (mod. m).

23.

***Si a es primo a m, y e y f, no son congruentes según el módulo m, entonces ae y af, tampoco serón congruentes según el módulo m.***

Esto es simplemente el recíproco del teorema anterior.

Después de esto, es evidente que si se multiplica a por todos los números enteros de 0 hasta m — 1, y se reduce cada producto a su menor resto según el modulo m, entonces todos serún diferentes. Como hay m de estos restos, ninguno de los cuales es > m, se encuentran entre ellos todos los números de 0 hasta m — 1.

24.

***La expresión ax*** + ***b, donde a y b*** son numeros dados y x denota un número indeterminado o variable, ***puede hacerse congruente segun el módulo m a cualquier nómero, siempre que m sea primo a a.***

Sea c el número al cual se hará congruente, y sea e el menor resto positivo de c — b según el modulo m. Por el artúculo anterior necesariamente se da un valor de x < m tal que el menor resto del producto ax según el modulo m será e. Si este valor es v, av = e = c — b; por lo tanto av + b = c (mod. m). Q. E. F.

25.

Llamamos congruencia a cualquier expresión que contiene dos cantidades congruentes como en una ecuaciún. Si involucra una incúgnita, se dice que se resuelve cuando se encuentra un valor (raíz) que satisface la congruencia. Asú es claro lo que significan una congruencia resoluble y congruencia no resoluble. Obviamente se pueden usar aquú las distinciones parecidas a las usadas al hablar de las ecuaciones. Ejemplos de congruencias trascendentales se darún mas adelante. Las congruencias algebraicas se distribuyen seguún la mayor potencia de la incúognita en congruencias de primero, de segundo, y de maús altos grados. De manera semejante se pueden proponer varias congruencias involucrando varias incognitas, y podemos hablar de su eliminacióon.

***La resolution de las congruencias del primer grado.***

26.

La congruencia del primer grado ax + b = c, segun el artúculo 24, siempre es

resoluble cuando el módulo es primo relativo a a. Ahora, si v es un valor conveniente de x, o sea, es una raíz de la congruencia, resulta claro que todo nómero congruente a v segun el módulo involucrado tambien es raíz (art. 9). Con igual facilidad se ve que todas las raíces tienen que ser congruentes a v. De hecho si t es otra raíz, entonces av + b = at + b, entonces av = at, v = t (art. 22). Se concluye que la congruencia x = v (mod. m) representa la solución completa de la congruencia.

Como todos los valores de x que son valores de la congruencia son congruentes entre sí, y como así los nómeros congruentes pueden considerarse equivalentes, se puede considerar tales soluciones como una sola. Por lo cual, como nuestra congruencia ax + b = c no admite otras soluciones, diremos que tiene una, y ínicamente una solucion, o bien que tiene una, y ínicamente una raíz. Así, por ejemplo, la congruencia 6x + 5 = 13 (mod. 11) no admite mís raíces que las que son = 5 (mod. 11). Esto no es cierto en las congruencias de otros grados ni en las congruencias del primer grado en las cuales se multiplica la incígnita por un nímero que no es primo relativo al modulo.

27.

Quedan por añadir algunos detalles sobre el calculo de la solucion de alguna congruencia. Primero notamos que una congruencia de la forma ax + t = u, donde suponemos que el mídulo es primo a a, depende de ax = ±1. Porque si x = r satisface esta íltima, x = ±(u — t)r satisfará la penultima. Pero la congruencia ax = ±1, cuyo modulo se denota por b, es equivalente a la ecuaciín indeterminada ax = by ± 1. Como hoy en día es conocida la resoluciín de ella, basta presentar el algoritmo para su caílculo.

Si las cantidades A, B, C, D, E, etc., dependen de α, β, γ, δ, etc., de tal manera que

A = α, B = βΑ +1, C = γΒ + A, D = δC + B, E = eD + C, etc. por brevedad las escribimos así:

A = bL B = ^^ C = ^^^^ D etc.[[102]](#footnote-103))

Ahora consideramos la ecuación indeterminada ax = by+1, donde a y b, son positivos. Podemos suponer sin perdida de generalidad que a no es < b. Ahora, mediante el algoritmo conocido para calcular el maximo comón divisor de dos numeros, formamos a traves de la division ordinaria las ecuaciones

a = ab + c, b = ^c + d, c = γά + e, etc.,

así que α, β, γ, etc., c, d, e, etc., son enteros siempre positivos, y b, c, d, e, decrecen hasta que encontramos m = μη + 1, algo que eventualmente debe ocurrir. Así resulta

a = [n^...^,e,aL b = [n^ ...,γ,β] .

Si tomamos x = [μ, ...,γ,β] , y = [μ, ...,γ,β,α]

tendremos ax = by + 1 cuando el nómero de terminos α, β, γ, ...μ, es par, o bien ax = by — 1 cuando es impar.

28.

El ilustre Euler fue el primero en dar la resolución general para las ecuaciones indeterminadas de este tipo (Comment. Petrop. T. VII. p. 46). El metodo que el uso consistía en sustituir x e y por otras incognitas, y hoy es bien conocido. El ilustre Lagrange trató el problema de una manera un tanto diferente. Como el mismo observo, es claro a partir de la teoría de las fracciones continuas que si la fracción se convierte en la fraccióon continua

1

1

1

α+

β+

γ + etc.

1

μ+

1

n

y si de la última parte se borra n y se reconvierte en una fracción x, entonces ax = by ± 1, siempre que a sea primo a b. Ademas, se obtiene el mismo algoritmo de los dos metodos. Las investigaciones del ilustre Lagrange aparecen en Hist. de l’Ac. de Berlin, 1767, p. 173, y con otros en los apendices de la version francesa del Algebra de Euler.

29.

La congruencia ax +1 = u, cuyo múdulo no es primo a a, se reduce facilmente al caso anterior. Sea m el modulo y sea δ el maximo común divisor de a y m. Es claro que cualquier valor de x que satisface la congruencia según el modulo m tambien la satisface segun el múdulo δ (art. 5). Pero ax = 0 (mod. δ) puesto que δ divide a a. Por tanto la congruencia no tiene solucion a menos que t = u (mod. δ), esto es t — u es divisible por δ.

Ahora, sean a = δe, m = δf, t — u = δ&; e serú primo a f. Entonces ex + k = 0 (mod. f) sera equivalente a la congruencia propuesta ax + t = u; esto es, cualquier valor de x que cumple la una tambien satisfará la otra y viceversa. Porque claramente ex + k es divisible por f cuando δex + δk es divisible por δf, y viceversa. Pero vimos antes cúmo resolver la congruencia ex + k = 0 (mod. f); así es claro que si v es uno de los valores de x, x = v (mod. f) nos da la soluciún completa de la congruencia propuesta.

30.

Cuando el múdulo es compuesto, a veces es ventajoso usar el siguiente metodo.

Sea el múdulo = mn, y la congruencia propuesta ax = b. Primero, se resuelve la congruencia según el múdulo m, y se supone que resulta x = v (mod. ψ) donde δ es el múaximo comuún divisor de los nuúmeros m y a. Es claro que cualquier valor de x que satisface la congruencia ax = b según el modulo mn tambien la satisface segun el módulo m, y sera expresable en la forma v + ψ x' donde x' es algún número indeterminado. El recíproco, sin embargo, no es cierto puesto que no todos los números de la forma v+ψx' satisfacen la congruencia según el múdulo mn. La manera de determinar x' tal que v + ψx' es una raíz de la congruencia ax = b (mod. mn) puede deducirse de la soluciún de la congruencia apx' + av = b (mod. mn) o de la congruencia equivalente a x' = ψυ (mod. n). Por tanto la resoluciún de

cualquier congruencia seguún el moúdulo mn puede reducirse a la resoluciúon de dos

congruencias según los módulos m y n. Y es evidente que si n es otra vez el producto de dos factores, la resoluciún de la congruencia, relativa al modulo n depende de la resoluciún de las congruencias cuyos modulos son estos factores. En general la resoluciúon de una congruencia seguún el moúdulo compuesto depende de la resoluciúon de otras congruencias cuyos modulos son factores del modulo compuesto. Estos factores pueden tomarse como numeros primos si esto es conveniente.

Ejemplo. Si se propone la congruencia 19x ξ 1 (mod. 140), se resuelve primero según el múdulo 2, y resulta x ξ 1 (mod. 2). Sea x = 1 + 2x'; se convierte en 38x' ξ —18 (mod. 140), o lo que es equivalente, 19x' ξ — 9 (mod. 70). Si se resuelve esta otra vez según el modulo 2, resulta x' ξ 1 (mod. 2), y al colocar x' = 1 + 2x" se convierte en 38x'' ξ—28 (mod. 70) o 19x'' ξ—14 (mod. 35). Según el múdulo 5 nos da la solución x'' ξ 4 (mod. 5), y sustituyendo x'' = 4 + 5x''' se convierte en 95x''' ξ —90 (mod. 35) o 19x''' ξ—18 (mod. 7). De esto resulta x''' ξ 2 (mod. 7), y al colocar x''' = 2 + 7x'''' resulta x = 59 + 140x''''; por lo tanto x ξ 59 (mod. 140) es la soluciúon completa de la congruencia propuesta.

31.

De la misma manera que se expresa la raíz de la ecuacion ax = b por a, designamos por a la raíz de la congruencia ax ξ b, y adjuntamos el múdulo de la congruencia para distinguirla. Así por ejemplo, (mod. 12) significa cualquier

número que es ξ 11 (mod. 12)\*). Es claro de esto en general que a (mod. c) no significa nada real (o si se quiere, es imaginario) cuando a y c tienen un comuún divisor que no divide a b. Aparte de este caso excepcional, la expresion a (mod. c) siempre tendrá valores reales, de hecho, un número infinito de ellos. Todos ellos serán congruentes según c cuando a es primo a c, o primo a | cuando δ es el maximo comun divisor de c y a.

Estas expresiones tienen un algoritmo muy parecido al empleado para las fracciones ordinarias. Indicamos unas propiedades que pueden deducirse facilmente de la discusiúon anterior.

1. Si según el modulo c, a ξ α, b ξ β, entonces las expresiones a (mod. c) y ^ (mod. c) son equivalentes.
2. af (mod. cδ) y a (mod. c) son equivalentes.
3. ail (mod. c) y a (mod. c) son equivalentes cuando k es primo a c.

Podríamos citar muchas otras proposiciones parecidas, pero, como no presen­tan ninguna dificultad ni son necesarias para lo siguiente, procedemos a otros temas.

***La búsqueda de un número congruente a un número dado según un módulo dado.***

32.

Se puede fácilmente, por medio de lo que precede, hallar todos los números que tienen residuos dados, según cualquier modulo, esto nos servirá mucho en lo que sigue.

Sean, en primer lugar, A y B, dos modulos segán los cuales el námero buscado z tiene que ser congruente a los námeros a y b. Todos los valores de z están necesariamente contenidos en la formula Ax + a, donde x es indeterminado, pero tal que Ax + a = b (mod. B). De manera que si δ es el maximo comán divisor de A y de B, la resolución completa de esta congruencia tomará la forma x = v (mod. B), o sea, lo que es igual, x = v + ^, siendo k un número entero indeterminado. Por lo tanto, la fármula Av + a + contiene todos los valores de z, lo que se reduce a z = Av + a (mod. ). Si hay un tercer mádulo C segán el cual el námero buscado

tiene que ser congruente a c, se sigue el mismo procedimiento, segun el cual se debe reunir las dos primeras condiciones en una sola. Así, sea e el máximo comán divisor de los námeros y C, entonces se obtendrá la congruencia x+Av+a = c (mod. C),

que será resuelta por una congruencia de la forma x = w (mod. C) y la propuesta sera resuelta completamente por la congruencia z = + Av + a (mod. ).

Se procede de la misma manera sea cual sea el námero de mádulos. Es conveniente observar que y son los menores námeros divisibles a la vez por A y B, o por

1. B y C y se puede concluir fáacilmente que sea cual sea la cantidad de máodulos A,
2. C, etc., si se representa por M el menor námero divisible por cada uno de ellos, se tendrá la resolucion completa al tomar z = r (mod. M). Pero cuando alguna de las congruencias auxiliares es irresoluble, concluimos que el problema involucra una imposibilidad. Pero obviamente esto no puede ocurrir cuando todos los nuámeros A, B, C, etc., son primos entre sí.

Ejemplo. Sean los námeros A, B, C, a, b, c, iguales a 504, 35, 16, 17, -4, 33. Aquá las dos condiciones z = 17 (mod. 504) y z = —4 (mod. 35) son equivalentes a la unica condicián z = 521 (mod. 2520). Al adjuntar la condicián z = 33 (mod. 16), nos dará finalmente z = 3041 (mod. 5040).

33.

Si todos los números A, B, C, etc., son primos entre sí, es claro que el producto de ellos es igual a su mínimo común multiplo. En tal caso, todas las congruencias z ξ a (mod. A), z ξ b (mod. B), etc., son equivalentes a la única congruencia z ξ r (mod. R), donde R denota el producto de los números A, B, C, etc. Resulta en seguida que la sola condición z ξ r (mod. R), puede descomponerse en varias; de hecho, si R se resuelve en factores A, B, C, etc., que son primos entre sí, entonces las condiciones z ξ r (mod. A), z ξ r (mod. B), z ξ r (mod. C) etc., agotan la condicion original. Esta observaciún nos abre no solamente un metodo de descubrimiento de la imposibilidad cuando existe, sino tambien un metodo mas comodo y mús elegante para calcular las raíces.

34.

Sean, como arriba, z ξ a (mod. A), z ξ b (mod. B), z ξ c (mod. C). Se resuelven todos los modulos en factores que son primos entre sú A en A0, A", A000, etc., B en B0, B00, B000, etc., y de tal manera que los números A0, A00, etc., B0, B00, etc., etc., o bien son primos o bien son potencias de primos. Si cualquiera de los números A, B, C, etc., ya es primo o la potencia de un primo, no hay que resolverlo en factores. Entonces, de lo anterior es claro que en vez de las condiciones propuestas podemos poner las siguientes: z ξ a (mod. A0), z ξ a (mod. A00), z ξ a (mod. A000), etc., z ξ b (mod. B0), z ξ b (mod. B00), etc., etc. Ahora, si no todos los números A, B, C, son primos entre sú (por ejemplo si A no es primo a B), es obvio que no pueden ser diferentes todos los factores primos de A y B. Tiene que ser uno u otro de ellos entre los factores A0, A00, A000, etc., que tiene entre los factores B0, B00, B000, etc., uno que es igual, o bien un multiplo, o bien un divisor propio. Primero, supóngase que A0 = B0. Entonces las condiciones z ξ a (mod. A0), z ξ b (mod. B0), tienen que ser identicas; a ξ b (mod. A0 o B0), y asú se puede ignorar una. Sin embargo, si no se da que a ξ b (mod. A), el problema es imposible de resolver. Si, en segundo lugar, B0 es multiplo de A0, la condiciún z ξ a (mod. A0) tiene que ser inclmda en la condiciún z ξ b (mod. B0); o sea la congruencia z ξ b (mod. A0) que se deduce de la posterior tiene que ser identica a la primera. De esto se sigue que la condiciún z ξ a (mod. A) puede rechazarse a menos que sea inconsistente con alguna otra condiciún (en cuyo caso el problema es imposible). Cuando todas las condiciones superfluas han sido rechazadas, todos los modulos que queden de los factores A0, A00, A000, etc., B0, B00, B000, etc., etc. serán primos entre sú Entonces podemos estar seguros de la

posibilidad del problema y proceder como antes.

35.

Ejemplo. Si, como arriba (art. 32), z = 17 (mod. 504), z = —4 (mod. 35) y z = 33 (mod. 16), entonces estas condiciones pueden reducirse a las siguientes: z = 17 (mod. 8), = 17 (mod. 9), = 17 (mod. 7), = —4 (mod. 5), = —4 (mod. 7), = 33 (mod. 16). De estas condiciones z = 17 (mod. 8), z = 17 (mod. 7), pueden omitirse puesto que la primera esta contenida en la condición z = 33 (mod. 16) y la segunda es identica a z = —4 (mod. 7). Permanecen:

17 (mod. 9) —4 (mod. 5) —4 (mod. 7) 33 (mod. 16)

y así: z = 3041 (mod. 5040)

Es cierto que a veces es más conveniente reunir las congruencias que se derivan de una misma condition separadamente de las condiciones restantes, puesto que es fácil hacerlo; e.g., cuando se eliminan unas de las condiciones z = a (mod. A!), z = a (mod. A00), etc., se reemplazan las restantes por z = a segán el mádulo que es el producto de todos los mádulos que se quedan del conjunto A0, A00, A000, etc. Así que, en nuestro ejemplo, las condiciones z = —4 (mod. 5), z = —4 (mod. 7) se reemplazan por z = —4 (mod. 35). Ademas resulta que no es indiferente para abreviar los calculos cuales condiciones superfluas se rechazan. Pero no es nuestro proposito tratar estos detalles ni otros artificios prácticos que pueden aprenderse mas facilmente por practica que por preceptos.

36.

***Cuando todos los modulos A, B,*** C, ***D, etc., son primos entre si, muchas veces es mejor usar el siguiente método.***

Se determina un numero congruente a la unidad segun el modulo A, y congruente a 0 segun el producto de los modulos restantes; o sea, sera un valor (preferiblemente el menor) de la expresion bcd etc (mod. A) multiplicado por BCD etc. (vease art. 32). De manera semejante, sea β = 1 (mod. B) y = 0 (mod. ACD etc.), γ = 1 (mod. C) y = 0 (mod. ABD etc.), etc. Entonces si sedesea un número z que según los módulos A, B, C, D, etc., sea congruente a a, b, c, d, etc., respectivamente, podemos colocar:

z = aa + βb + γc + úd etc. (mod. ABCD etc.)

Es obvio que aa = a (mod. A) y que todos los restantes números β^ jc, etc. son todos = 0 (mod. A), así que z = a (mod. A). Una demostraciún semejante vale para los otros múdulos. Esta solution es preferible a la primera cuando tenemos que resolver mas problemas del mismo tipo para los cuales los múdulos A, B, C, etc., mantienen sus valores, puesto que así α, β, γ, etc., tienen valores constantes. Esto ocurre en el problema de la cronología donde se intenta determinar el ano juliano dados su número dorado y su ciclo solar. Aquú A = 15, B = 19, C = 28, asú que el valor de la expresion ^g^g (mod. 15), o —(mod. 15) es 13, luego a = 6916. De manera que β es 4200 y γ es 4845, asú que el número que deseamos es el menor residuo del número 6916a + 4200b + 4845c, donde a es la indicción, b el número dorado, c el ciclo solar.

***Congruencias lineales con varias incógnitas.***

37.

Esto basta para las congruencias del primer grado con una incognita. Se procede a las congruencias que contienen varias incognitas. Si expusieramos el asunto con todo rigor, esta secciún nunca terminaría. Por tanto, se propone tratar solamente lo que parezca merecer atenciún, restringir nuestra investigation a unas observaciones, y dejar una exposiciúon completa para otra ocasioún.

1. Al igual que en las ecuaciones, vemos que se debe tener tantas congruencias como incúognitas por determinar.
2. Se proponen, entonces, las congruencias

|  |  |  |
| --- | --- | --- |
| ax + by + cz + · · | ■ · = f (mod. m) | (A) |
| a0x + b0y + c0z + · · | ■· = f' | (A0) |
| a00x + b00y + c00z + · · | ■ · = f" | (A00) |

etc.

de las cuales hay tantas como incúgnitas x, y, z, etc.

Ahora, se determinan los números ξ, ξ0, ξ00, etc., tales que

+ b'^ + ϋ"ξ" + etc. = 0 cξ + ο0ξ0 + ο00ξ00 + etc. = 0 etc.

y tales que todos los numeros sean enteros sin común divisor, lo cual es siempre posible por la teoría de las ecuaciones lineales. De modo semejante ν, ν0, ν00, etc., ζ, ζ0, ζ00, etc., etc., tales que

αν + a'ν' + α00ν00 + etc. = 0  
cv + ο0ν0 + ο00ν00 + etc. = 0  
etc.

αζ + α0ζ0 + α00ζ00 + etc. = 0  
bZ + b0Z0 + b00Z00 + etc. = 0  
etc. etc.

1. Es claro que si se multiplican las congruencias A, A0, A00, etc., por ξ, ξ0, ξ00, etc., luego por ν, ν0, ν00, etc., etc., y luego se suman, resultarún las siguientes congruencias:

(αξ + α'ξ' + α00ξ00 + etc.)x = /ξ + f0ξ0 + /00ξ00 + etc.

(bv + b0v0 + b0V00 + etc.)y = /ν + /0ν0 + /00ν00 + etc.

(οζ + ο0ζ0 + °00ζ00 + etc.)z = /ζ + /0ζ0 + / 00 ζ00 + etc.

etc.

las cuales escribimos por brevedad de la manera siguiente:

Σ(αξ)x = Σ(/ξ)> Σ(bv)y = Σ(/ν)> Χ(οζ)z = Σ(/ζ), etc.

1. Ahora se distinguen varios casos.

Primero, cuando todos los coeficientes ^(αξ), Σ^ν), etc. son primos a m, el modulo de las congruencias, ellas se resuelven según los preceptos ya tratados, y se

encuentra la solución completa por congruencias de la forma x = p (mod. m), y = q (mod. m), etc.[[103]](#footnote-104)) E.g., si se proponen las congruencias

x + 3y + z = 1, 4x + y + 5z = 7, 2x + 2y + z = 3 (mod. 8)

se encuentra que ξ = 9, ξ' = 1, ξ'' = -14, luego — 15x = — 26 luego x = 6 (mod. 8). De igual manera se encuentra que 15y = —4, 15z = 1, y así que y = 4, z = 7 (mod. 8).

1. Segundo, cuando no todos los coeficientes Σ(«ξ), ΣΧ^ν), etc., son primos al modulo, sean α, β, γ, etc., los maximos comunes divisores del modulo m con Σ(«ξ), ΣΧ^ν)^ü(cC), etc. respectivamente. Es claro que el problema es imposible a menos que ellos dividan los nómeros ΣΧ/ξ), ΣΧ/ν), ΣΧ/Ζ), etc., respectivamente. Sin embargo, cuando se cumplan estas condiciones, es claro que las congruencias en (3) se resolverón completamente por congruencias de la forma x = p (mod. ψ), y = q (mod. ψ), z = r (mod. m), etc., o si se quiere hay α valores diferentes

de x (o sea, no congruentes segón m), digamos p, p + ψ,...p + (α q1)to, β valores diferentes de y, etc., que satisfacen las congruencias. Es evidente que todas las soluciones de las congruencias propuestas (si hay) se encuentran entre estas. Pero esta solución no puede invertirse puesto que en general no todas las combinaciones de todos los valores de x, al combinarlos con todos los de y y z etc., satisfacen el problema, sino ónicamente aquellas cuya interrelacion puede mostrarse por una o varias de las congruencias condicionales. Sin embargo, como la solucion completa de este problema no es necesaria para lo que sigue, no desarrollaremos el argumento mas sino que ilustraremos la idea por medio de un ejemplo.

Sean las congruencias propuestas:

3x + 5y + z = 4, 2x + 3y + 2z = 7, 5x + y + 3z = 6 (mod. 12)

Entonces, ξ, ξ', ξ''; ν, ν', ν''; Ζ, Z', Ζ'' serán respectivamente iguales a 1, —2, 1;

1, 1, —1; —13, 22, —1, y de esto 4x = —4, 7y = 5, 28z = 96. A partir de esto

se crean cuatro valores de x, digamos = 2, 5, 8, 11; un valor de y, digamos = 11,

y cuatro valores de z, digamos = 0, 3, 6, 9 (mod. 12). Ahora, para saber cuales

combinaciones de los valores de x pueden usarse con los valores de z, se sustituyen en las congruencias propuestas para x, y, z, respectivamente, 2 + 3t, 11, 3u. Esto convierte las congruencias en

57 + 9t + 3u ξ 0, 30 + 6t + 6u ξ 0, 15 + 15t + 9u ξ 0 (mod. 12),

y facilmente se ven equivalentes a

19 + 3t + u ξ 0, 10 + 2t + 2u ξ 0, 5 + 5t + 3u ξ 0 (mod. 4).

La primera claramente requiere que u ξ t + 1 (mod. 4); al sustituir este valor en las restantes congruencias, tambien las satisface. Se concluye que los valores 2, 5, 8, 11 de x, que resultan al poner t ξ 0, 1, 2, 3, estan necesariamente combinados con los valores de z ξ 3, 6, 9, 0, respectivamente. En total tenemos cuatro soluciones:

x ξ 2, 5, 8, 11 (mod. 12) y ξ 11, 11, 11, 11

z ξ 3, 6, 9, 0

A estas investigaciones, las cuales completan la finalidad que habíamos propuesto para esta sección, adjuntamos unas cuantas proposiciones que dependen de los mismos principios y que serán ótiles frecuentemente en lo que sigue.

***Varios Teoremas.***

38.

PROBLEMA. ***Hallar cuantos números positivos hay menores que un número positivo dado A, y a la vez primos a él.***

Por brevedad simbolizamos el numero de enteros positivos que son primos a A y menores que el por el prefijo <£>. Por lo tanto se busca a <^>A.

1. Cuando A es primo, es claro que todos los nómeros desde 1 hasta A — 1 son primos a A; y así en este caso resultara

<£>A = A — 1

1. Cuando A es la potencia de un primo, digamos = pm, ninguno de los nómeros divisibles por p sera primo a A, pero los demas sí. Entonces, de los pm — 1

números, tienen que rechazarse: p, 2p, 3p, ... , (pm 1 — 1 )p. Por lo tanto sobran pm — 1 — (pm 1 — 1) o sea pm-1(p — 1) de ellos. Así

vpm = pm-1(p \_ !)

1. Los casos restantes se reducen facilmente a estos mediante la siguiente proposición: Si A se resuelve en factores M, N, P, etc., que son primos entre si, será

***φΑ*** = ***φΜ · φΝ · φΡ*** etc.

Esto se demuestra como sigue. Sean m, m', m", etc., los números primos a M y menores que M, y sea el número de ellos = φΜ. De manera semejante, sean n, n', n", etc., p, p', p'', etc., los números primos a N ya P, respectivamente y menores que ellos, y sean φΝ, φΡ, etc., los numeros de ellos. Es evidente que todos los números que son primos al producto A, tambien serán primos a los factores individuales M, N, P, etc., y viceversa (art. 19); y además que todos los numeros congruentes a cualquiera de m, m , m , etc., serúan primos a M y viceversa. De modo semejante para N, P, etc. Así el problema se reduce a este: determinar cuúntos números hay menores que A y tambien congruentes según el modulo M a los números m, m', m'', etc., y que son congruentes según el modulo N a los numeros n, n', n'', etc. Pero del artúculo 32 se sigue que todos los nuúmeros que tienen residuos dados seguún cada uno de los modulos M, N, P, etc., serún congruentes según su producto A. Asú habrá únicamente uno que es menor que A y congruente a los residuos dados según M, N, P, etc. Por lo tanto, el nuúmero que buscamos es igual al nuúmero de combinaciones de cada uno de los numeros m, m', m'', etc., con cada uno de los n, n', n'', etc., y p, p', p'', etc., etc. Es evidente que por la teoría de las combinaciones esto sera = <^>M · <^>N · <^>P etc. Q. E. D.

1. Ahora es facil ver cúmo aplicar esto al caso considerado. Sea A resuelto en sus factores primos; esto es, reducido a la forma aabβc7 etc., donde a, b, c, etc., son nuúmeros primos diferentes. Entonces se tendrúa

φΆ = φαα · · φύ7 etc. = aa-1(a — 1)b^\_1(b — 1)c7\_1(c — 1) etc.

o, con múas elegancia,

a— 1 b— 1 c— 1

<r>A = A · · · etc.

b

a

c

Ejemplo. Sea A = 60 = 2§ · 3 · 5; entonces φΆ = § · § · | · 60 = 16. Los números que son primos a 60 son 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

La primera resolución de este problema aparece en la memoria del ilustre Euler titulada Theoremata arithmetica nova methodo demostrata (Comm. nov. Ac. Petrop. VIII p. 74). La demostraciún se repitio en otra disertaciún titulada Speculationes circa quasdam insignes propietates numerorum (Acta Petrop. VIII, p. 17).

39.

Si determinamos el significado del símbolo φ de tal manera que φΆ exprese el número de enteros que son primos a A y no mayores que A, es evidente que ya no vale φ1 = 0 sino = 1. No se cambia nada en ningún otro caso. Tomando esta definicion, tendremos el teorema siguiente:

***Si a, a, a", etc. son todos los divisores de*** A ***(incluyendo a 1 y a*** A ***mismo), se tendrá***

φα + φα + φα" + etc. = A

Ejemplo. Si A = 30, entonces φ1 + φ2 + φ3 + φ5 + φ6 + φ10 + φ15 + φ30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30

Demostración. Se multiplican por Al todos los números que sean primos a a y no mayores que a, por todos los números primos a a' y no mayores que a', etc., y se tendrán φa + <^>a' + <^>a'' + etc. números, ninguno mayor que A mismo. Pero:

1. Todos estos números serán diferentes. De hecho, es evidente que todos aquellos engendrados por un mismo divisor de A serán diferentes. Ahora, si dos números diferentes fueran engendrados por dos divisores diferentes M y N, y por dos números μ y v que fueran primos respectivamente a M y N, esto es, si (M)μ = (N)v, resultaría que μΝ = vM. Supúngase que M > N (lo cual se puede). Como M es primo a μ , y como divide al número μΝ, tiene que dividir a N. Por lo tanto, un número mayor divide a un número menor. Q. E. A.
2. Se incluyen todos los números 1, 2, 3, ...A, entre estos números. Sea t un número cualquiera no mayor que A, y sea δ el múximo común divisor de A y t. A sera el divisor de A que es primo a |. Es evidente que este numero se encuentra entre los engendrados por el divisor ^ .
3. Resulta de esto que el número de estos enteros será A y por lo tanto

φα + φα0 + φα00 + etc. = A. Q. E. D.

40.

***Si el máximo común divisor de los números A, B, C, D, etc.*** = ***μ, siempre pueden determinarse números a, b, c, d, etc., tal que***

aA + bB + cC + etc. = μ.

Demostración. Consideramos primero dos de tales números A y B, y sea su máximo común divisor = λ. Entonces, la congruencia Ax = λ (mod. B) sera resoluble (art. 30). Sea la raíz = α, y se pone λ—Αα = β. Entonces se obtendrú aA + ^B = λ como deseamos.

Si hay un tercer número C, sea λ0 el múximo común divisor de los números λ y C, el cual será tambien el maximo común divisor de los números A, B y C[[104]](#footnote-105)). Determúnense números k y γ tales que ^λ + qC = λ0, entonces kaA + keB + qC = λ0.

Si hay un cuarto número D, sea λ00 el maximo común divisor de los números λ0 y D (es fúcil ver que serú tambien el maximo común divisor de A, B, C y D), y sea krX + ÓD = λ00. Entonces tenemos kk'aA + kk0eB + k0qC + ÓD = λ00.

De manera semejante se procede si todavía hay mas números.

Y si los números A, B, C, D, etc., no tienen divisor común, claramente se

tiene

aA + bB + cC + etc. = 1

41.

Si p ***es nUmero primo y se tienen p objetos, entre los que cualquier número de ellos pueden ser iguales, pero no todos, el número de permutaciones de estos objetos sera divisible por p.***

Ejemplo. Cinco objetos A, A, A, B, B pueden disponerse de diez maneras diferentes.

La demostración de este teorema puede derivarse fácilmente de la conocida teoría de permutaciones. Supóngase que entre estos objetos hay a iguales a A, B iguales a B, c iguales a C, etc. (cualesquiera de a, b, c, etc. pueden ser iguales a la unidad), entonces se tiene

a + b + c + etc. = p y el numero de permutaciones sera

1· 2 · 3 •••p

1 · 2 · 3 •••a · 1 · 2 · ·· b · 1 · 2 · ·· c etc.

Ahora, es claro que el numerador tiene que ser divisible por el denominador, puesto que el nómero de permutaciones debe ser un entero. Pero el numerador es divisible por p, mientras que el denominador, el cual esta compuesto de factores menores que p, no es divisible por p (art. 15). Así el nómero de permutaciones sera divisible por p (art. 19).

Esperamos que la siguiente demostración complacera al lector.

Cuando en dos permutaciones de los mismos objetos el orden de ellas no difiere salvo que el primero en una ocupa una posición diferente en la otra mientras que los restantes siguen el mismo orden, de manera que, en el segundo orden, el primer objeto del primer orden sigue al óltimo de el, las llamamos: permutaciones semejantes[[105]](#footnote-106)). Así, en nuestro ejemplo, las permutaciones ABAAB y ABABA serán semejante puesto que los objetos que ocupan los lugares primero, segundo, etc., segun la primera, ocuparóan los lugares tercero, cuarto, etc., en la uóltima, siguiendo la misma sucesioón.

Ahora, como cualquier permutación esta compuesta de p objetos, es evidente que se pueden encontrar p — 1 permutaciones que sean semejantes a ella avanzando el objeto del primer lugar al segundo, al tercero, etc. Es evidente que el nuómero de todas las permutaciones no idóenticas es divisible por p puesto que este nuómero es p veces mayor que el numero de todas las permutaciones no semejantes.

Supongamos, pues, que dos permutaciones

***PQ...TV ...YZ; V...YZPQ*** ...T,

donde se engendra una a partir de la otra avanzando sus términos, sean idénticas, o sea P = V, etc. Sea el termino P, que es el primero en la primera, el (n + 1)-esimo en la siguiente. Entonces, en la sucesión siguiente el (n + 1)-simo termino sera igual al primero, el (n + 2)-esimo al segundo, etc., y el (2n + 1)-esimo vuelve a ser igual al primero, como el (3n + 1)-esimo, etc.; y , en general, el (kn + m)-esimo termino igual al m-esimo (donde, cuando kn + m supera a p mismo, es necesario concebir la sucesión V ...Y ZPQ ...T como repetida continuamente desde el comienzo, o se resta de kn + m el móltiplo de p menor que kn + m y mas proximo en magnitud). Asó pues, si se determina k tal que kn ξ 1 (mod. p), lo cual siempre puede hacerse, pues p es primo, resulta en general que el m-esimo termino es igual al (m +1)-^simo, o que cada termino es igual a su sucesor, i.e., todos los terminos son iguales, contrariamente a la hipotesis.

42.

***Si los coeficientes A, B, C, ..., N; a, b, c, ..., n de dos funciones de la***

***forma***

xm + Axm-1 + Bxm-2 + Cxm-3 + ■■■ + N (P)

χμ + αχμ-1 + bxμ-2 + cx^-3 + ■■■ + n (Q)

***son todos racionales, y no todos enteros, y si el producto de (P***) ***y*** (Q)

= xm+^ + Αχτη+μ-1 + Bxm+^-2 + etc. + 3

***entonces no todos los coeficientes A,*** B, ... 3 ***pueden ser enteros.***

Demostración. Se expresan todos las fracciones entre los coeficientes A, B, etc., a, b, etc., en su forma reducida, y se elige libremente un primo p que divida uno o varios de los denominadores de estas fracciones. Supongamos que p divide al denominador de uno de los coeficientes en (P). Es claro que si se divide (Q) por p, por lo menos uno de los coeficientes fraccionales en tendrá a p como factor de su denominador (por ejemplo, el primer coeficiente, 1). Ahora, es facil ver en (P) que siempre habrá un termino, una fraccion, cuyo denominador involucra potencias mós altas de p que los denominadores de todos los coeficientes fraccionales que lo preceden y ninguna potencia menor que los denominadores de todos los coeficientes fraccionales subsiguientes. Sea este termino = Gxg, y sea la potencia de p en el denominador

de G, = t. Un término semejante puede encontrarse en . Sea = Γχγ, y sea la potencia de p en el denominador de Γ, = τ. Es evidente que t + τ sera = 2 por lo menos. Ahora se demostrara que el termino x9+7 en el producto de (P) y (Q) tendrá un coeficiente fraccional cuyo denominador involucrará t + τ — 1 potencias de p.

Sean 'Gx9+1, "Gx9+2, etc., los terminos en (P) que preceden a Gx9, y G0x9-1, G0/x9-2, los que le siguen; de manera semejante sean 0rxY+1, /0rxY+2, etc., los terminos que preceden a TxY, y los terminos que lo siguen serán Ux7-1, r0/x7-2, etc. Es claro que en el producto de (P) y el coeficiente del termino x9+7 sera

= Gr + 0GU + "GU" + etc.

+ TG + "rG" + etc.

La parte Gr sera una fracción, y si se expresa en forma reducida, se involucraran t + τ potencias de p en el denominador; las partes restantes, si son fracciones, contendráan en sus denominadores menos potencias de p puesto que todos son productos de dos factores de los cuales uno no contiene mas que t potencias de p, el otro menos que τ potencias de p; o el otro no tiene más que τ, y el primero menos que t. Así Gr sera de la forma jp+pe, mientras que la suma de las restantes de la forma f ,pte+T, donde δ es positivo y e, f, f' esrán libres del factor p: por lo cual la suma de todos sera

= ef0 + ***e'fpS ff'pt+τ***

cuyo numerador no es divisible por p. De tal manera el denominador no puede obtener potencias menores que t + τ por ninguna reduccián. Por lo tanto, el coeficiente del termino x9+Y en el producto de (P) y (Q) sera

= ef0 + efp¿

ffV+r-1 ’

i.e., una fraccián cuyo denominador contiene t + τ — 1 potencias de p. Q. E. D.

43.

***Las congruencias del m-esimo grado***

Axm + Bxm-1 + Cxm-2 + etc. + Mx + N = 0

***cuyo modulo es el número primo p que no divide a A, no pueden resolverse más que de m maneras diferentes, o sea, no pueden tener más que m raíces no congruentes segun p.*** (Vea artículos 25 y 26).

Si se asume falso, tendremos congruencias de grados diferentes m, n, etc., con mas de m, n, etc. raíces, y si el menor grado es m, todas las congruencias semejantes de menor grado se encuentran en concordancia con nuestro teorema. Como ya hemos demostrado esto para el primer grado (art. 26), es claro que m es = 2 o mayor. Por eso la congruencia

Axm + Bxm-1 + etc. + Mx + N = 0

admite por lo menos m +1 raíces, x = a, x = β, x = γ, etc., y suponemos (lo que es válido) que α, β, γ, etc., son positivos y menores que p, y que a es el menor de todos. Ahora, en la congruencia propuesta se sustituye x por y + a. La congruencia se transforma en

A'ym + B'ym-1 + C'ym-2 + ··· + M0y + N = 0

Entonces es evidente que se satisface esta congruencia si se pone y = 0, o = β — a, o = γ — a, etc. Todas estas raíces serán diferentes, y el numero de ellas = m +1. Pero como y = 0 es raíz, N0 es divisible por p. Así que tambien la expresión

y(A0ym-1 + B0ym-2 + etc. + M0) sera = 0 (mod. p)

si se reemplaza y por uno de los m valores β — a, γ — a, etc., todos los cuales son > 0 y < p. Así, en todos estos casos, tambien

A0ym-1 + B0ym-2 + etc. + M0 serí = 0 (mod. p)

i.e., la congruencia

A0ym-1 + B0ym-2 + etc. + M0 = 0 (art. 22)

que es de grado m — 1, tiene m raíces, contrariamente a nuestro teorema (es evidente que A0 sera = A y así no divisible por p, como se requiere), pero hemos supuesto que nuestro teorema vale para toda congruencia de grado inferior a m. Q. E. A.

44.

Aunque hemos supuesto que el módulo p no divide al coeficiente del término más alto, el teorema no se restringe sólo a este caso. Porque, si el primer coeficiente o cualquiera de los otros, es divisible por p, puede rechazarse sin riesgo, por eso se reduce la congruencia a un grado inferior, para el cual el primer coeficiente ya no sería divisible por p, a menos que todos los coeficientes sean divisibles por p, en cuyo caso la congruencia sería una identidad y la incognita completamente indeterminada.

Este teorema primero fue propuesto y demostrado por Lagrange (Mem. de l’Ac. de Berlin, 1768 p. 192). Tambien se encuentra en la memoria de Legendre, Recherches d’Analyse indéterminée, Hist. de l’Acad. de Paris 1785 p. 466. El gran Euler en Nov. Comm. Ac. Petr. XVIII, p. 93 demostró que la congruencia xn — 1 ξ 0 no puede tener mós que n raíces diferentes. A pesar de que era un caso particular, el metodo que uso este gran senor puede adaptarse facilmente a todas las congruencias. Anteriormente el había resuelto un caso aun mós limitado, Comm. nov. Ac. Petr. V p. 6 , pero este metodo no puede generalizarse. En la sección VIII demostraremos este teorema por un metodo todavía diferente; aunque a primera vista parecen diferentes estos metodos, los expertos que quieran compararlos llegarón fócilmente a ver que todos estan construidos sobre el mismo principio. Sin embargo, como el teorema considerado aquó no es móas que un lema, y como la exposicióon completa no pertenece a este lugar, no pararemos aquó para tratar los modulos compuestos por separado.

Sección Tercera

SOBRE

RESIDUOS DE LAS POTENCIAS

***Los residuos de los términos de una progresión geométrica  
que comienza desde la unidad constituyen una serie periódica.***

45.

TEOREMA. ***En toda progresión geométrica 1, a, a2, a3, etc., aparte del primer término, se da ademós otro término at, congruente a la unidad, segun el módulo p, que es primo a a, cuyo exponente es t < p.***

Demostración. Puesto que el modulo p es primo a a, y por lo tanto es primo a cualquier potencia de a, ningUn termino de la progresión será ξ 0 (mod. p), sino que cada uno será congruente a uno de los nómeros 1, 2, 3, ...p — 1. De estos, hay p — 1, pues, es evidente que si se considerasen mas que p — 1 terminos de la progresión, no todos pueden tener diferentes residuos mínimos. Entonces, entre los terminos 1, a, a2, a3, ...ap—1, se encontraran al menos dos congruentes a un residuo mínimo. Sea pues, am ξ an y m > n, y al dividir por an, resultara am—n ξ 1 (art. 22), donde m — n < p, y > 0. Q. E. D.

Ejemplo. En la progresion 2, 4, 8, etc., el primer termino que es congruente a la unidad, segun el modulo 13, resulta ser 212 = 4096. Pero, segun el modulo 23, en esta progresion es 211 = 2048 ξ 1. Igualmente, 15625, la sexta potencia del numero 5, es congruente a la unidad, segun el modulo 7, la quinta de ella, 3125, segun el modulo

1. Por tanto, en unos casos la potencia congruente a la unidad resulta menor que p — 1. Pero, en otros, es necesario ascender hasta la (p — 1)-esima potencia.

46.

Cuando se continúa una progresión más allá de un término que es congruente a la unidad, se producen nuevamente los mismos residuos que se tienen al principio. Es claro que si at = 1, se tendrá at+1 = a, at+2 = a2, etc., hasta que se encuentre

C\ -L

el termino a cuyo residuo menor otra vez sera = 1, y el período de los residuos comenzara de nuevo. Se tiene, pues, un período que comprende t residuos, que en cuanto finaliza se vuelve a repetir desde el comienzo; y ningun otro residuo, salvo aquellos contenidos en este período, puede aparecer en toda la progresion.

En general, será amt = 1, y amt+n = an, lo cual en nuestra notacion se presenta

así:

***Si r = ρ*** (mod. ***t), será ar = ap*** (mod. p).

47.

De este teorema, se gana un metodo para encontrar muy fácilmente los residuos de potencias, tan grandes como sean sus exponentes, una vez que se encuentra una potencia congruente a la unidad. Si, por ejemplo, se busca el residuo resultante de la division de la potencia 31000 por 13, será 33 = 1 (mod. 13), t = 3; como 1000 = 1 (mod. 3), será 31000 = 3 (mod. 13).

48.

Cuando at es la menor potencia congruente a la unidad (excepto a0 = 1, tal caso no sera tratado aquá), los t terminos que constituyen un período de residuos serán todos diferentes, como se puede ver con facilidad de la demostracián del art. 45. Entonces, tambien la proposicián del art. 46 puede invertirse; esto es, si am = an (mod. p), será m = n (mod. t). Pues, si m y n fueran incongruentes segán el modulo t, sus residuos mánimos μ, ν serían diferentes. Pero, ap‘ = am y av = an, asá pues aμ = av, i.e., no todas las potencias menores que d son incongruentes, contra la hipáotesis.

Si ak = 1 (mod. p), entonces sera k = 0 (mod. t), i.e., k sera divisible por t.

Hasta aquá hemos hablado de modulos cualesquiera, primos a a. Ahora, trataremos por aparte los modulos que son námeros absolutamente primos y luego desarrollaremos una investigacián mas general con esta base.

***Se consideran primero los módulos que son numeros primos.***

49.

TEOREMA. ***Si p es un número primo que no divide a a, y si at es la menor potencia de a congruente a la unidad, según el múdulo p, el exponente t serú = p — 1, o sera un factor de este número.***

Consúltese los ejemplos del art. 45.

Demostracion. Puesto que ya hemos demostrado que t es= p — lo <p — 1, falta

que, en el segundo caso, se demuestre que t siempre es un factor de p — 1.

.0

1. Reúnanse los menores residuos positivos de todos estos terminos 1, a, a2,

. ..at-1, que se denotaran por α, α', α'', etc., de modo que sea α = 1, α' = a, α'' = a2, etc. Se ha visto que todos son diferentes; pues, si dos terminos am y an tuvieran el mismo residuo, (al suponer m > n) sería am-n = 1, no obstante que m — n < t. Q.E.A., puesto que ninguna potencia inferior a af es congruente a la unidad (por hipútesis). Ademas, todos los α, α', α'', etc. estan contenidos en la sucesión de números 1, 2, 3, ...p — 1 que, sin embargo, no se agotan pues t < p — 1. Denotaremos el conjunto de todos α, α', α'', etc. con (A). Por tanto, (A) contiene t terminos.

1. Túmese un numero cualquiera β entre 1, 2, 3, ...p — 1 que falte en (A) . Multipliquese β por todos los α, α', α'', etc. Sean β, β', β'', etc. los residuos menores originados de allí cuyo numero sera t. Pero estos residuos serán diferentes entre si y ademas diferentes de α, α', α'', etc. Si la primera asercion fuera falsa, se tendría βαm = βan, dividiendo por β, am = an, contra lo que hemos demostrado. Si la segunda fuera falsa, se tendría βαm = an. Por tanto, cuando m < n, β = an-m, i.e., β ser ía congruente con uno de estos α, α', α'', etc. contra la hipotesis; cuando vale m > n, al multiplicar por at-m, βat = at+n-m, o por medio de at = 1, β = at+n-m, lo cual es un absurdo. Denotese el conjunto de todos los β, β', β'', etc., cuyo numero = t con (B) y se tiene ya 2t números de 1, 2, 3, ...p — 1. Por tanto, y si (A) y (B) comprenden todos estos numeros, se tiene = t. As í el teorema se ha demostrado.
2. Si todavía quedan algunos, sea γ uno de ellos. Multiplíquense por el todos α, α', α'', etc. y sean γ, γ', γ'', etc. los residuos mínimos de los productos y denotese el conjunto de todos ellos con (C). Por tanto, (C) comprende t números de 1, 2, 3, ...p — 1, que son todos diferentes entre s í, y diferentes de los contenidos en (A) y (B). Las primeras aserciones se demuestran de igual modo como en el II, la tercera como sigue: si fuera γαm = βan, sería γ = βαn-m, o = βat+n-m segun que m<n o > n, y en cualquier caso γ ser ía congruente a un numero de (B) contra

la hipótesis. Por tanto, se tienen 31 números de 1, 2, 3, ...p — 1 y si no faltan más resulta t = 2—1 y así el teorema quedarú demostrado.

1. Si faltan todavía otros, del mismo se habrú de proceder a un cuarto conjunto (D) de números, etc. Pero, es evidente, puesto que el número de enteros 1, 2, 3, ...p — 1 es finito, que al fin se habrán de agotar todos ellos, y que sera un múltiplo de t: por eso t serú algun factor del numero p — 1. Q. E. D.

***El teorema de Fermat.***

50.

Asú, puesto que 2—1 es un entero, resulta al elevarse ambas partes de la congruencia al· = 1 a la potencia 2—1, ap\_1 = 1o sea ap\_1 — 1 siempre es divisible por p, cuando p es un primo que no divide a a.

Este teorema, el cual ya sea por su elegancia o por su gran utilidad es digno de toda atención, suele llamarse el teorema de Fermat, por su inventor. (Vease Fermat, Opera Matem., Toulouse 1679, p. 163). El inventor no presento una demostracion, sin embargo afirmo tener una en su poder. El gran Euler fue el primero que publico una demostracion, en su disertacion titulada Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T. VIII.[[106]](#footnote-107)) Se basa esta en el desarrollo de la potencia (a + 1)p, donde se deduce facilmente de la forma de los coeficientes, que (a + 1)p — ap — 1 siempre sera divisible por p cuando ap — a es divisible por p. Ahora, como 1p — 1 siempre es divisible por p, tambien 2p — 2 lo sera siempre, por tanto tambien 3p — 3, y en general ap — a. Y si p no divide a a, tampoco ap\_1 — 1 sera divisible por p. Esto basta para aclarar la idea del metodo. El gran Lambert presento una demostracion parecida en Actis Erudit, 1769, p. 109. Porque se veía que el desarrollo de una potencia binomia era bastante ajeno de la teoría de los numeros, el gran Euler busco otra demostracion que aparece en Comment. nov. Petr. T. VII p. 70, y que esta en armonía con lo que expusimos en el artículo anterior. Ademas, en lo siguiente, se nos ofrecerán otras demostraciones. En este lugar, se permite añadir otra mas, la cual se basa en principios semejantes a los de la primera del gran Euler.

La siguiente proposición, de la cual un caso especial es nuestro teorema, también será útil para otras investigaciones.

51.

***La p-ésima potencia del polinomio a*** + b + c + etc. ***es***

= aP + bp + cP + etc.

***según el módulo p siempre que p sea un número primo.***

Demostración. Es evidente que la p-esima potencia del polinomio a + b + c + etc. esta compuesta de terminos de la forma χααόβC etc., donde α + β + γ + etc. = p, y χ denota en cuantas maneras p objetos pueden permutarse cuando α, β, γ, etc. de ellas son respectivamente iguales a a, b, c, etc. Pero, antes, en el artículo 41, mostramos que este numero siempre es divisible por p, si todos los objetos no son iguales, i.e., si no es que uno de los numeros α, β, γ, etc. = p y los demas = 0. De esto se sigue que todos los terminos de (a + b + c + etc.)p, excepto ap, bp, cp, etc., son divisibles por p; por tanto, cuando se trata la congruencia segun el modulo p, pueden omitirse todos ellos, y sera

(a + b + c + etc.)p = ap + bP + cp + etc. Q.E.D

Ahora si se ponen todas las cantidades a, b, c, etc. = 1 y el numero de ellas es = k, tendremos kp = k, como en el artículo anterior.

***Cuantos números corresponden a un período,  
en el cual el número de terminos es un divisor dado del número p — 1.***

52.

Dado que otros numeros, que no sean divisores del numero p — 1, no pueden ser los exponentes de las potencias menores congruentes a la unidad, se plantea el problema de si todos los divisores de p — 1 disfrutan de esta propiedad, y cuando se clasifican todos estos numeros no divisibles por p, segun el exponente de su potencia menor congruente a la unidad, ¿cuantos de ellos se encuentran para cada uno de los exponentes? Primero conviene observar que basta considerar todos los numeros positivos de 1 hasta p — 1; pues, es evidente que los numeros congruentes deben

elevarse a una misma potencia para que sean congruentes a la unidad, y por tanto, un numero cualquiera debe referirse al mismo exponente al que su residuo menor se refiere. Por consiguiente, tenemos que dedicarnos a hallar como, con respecto a esto, se han distribuido los numeros 1, 2, 3, ...p — 1 entre los factores individuales del número p — 1. Por brevedad, si d es uno de los divisores del número p — 1 (entre los que tambien se incluyen 1 y p — 1) por medio de ψd denotaremos el numero de enteros positivos menores que p mismo, cuya d-esima potencia es la menor congruente a la unidad.

53.

Para que esta investigaciún pueda entenderse facilmente, agregamos un ejemplo. Para p = 19, los numeros 1, 2, 3, ... 18 se distribuirán entre los divisores del número 18, de este modo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 |  |  |  |  |  |
| 2 | 18 |  |  |  |  |  |
| 3 | 7, | 11 |  |  |  |  |
| 6 | 8, | 12 |  |  |  |  |
| 9 | 4, | 5, | 6, | 9, | 16, | 17 |
| 18 | 2, | 3, | 10 | 13, | 14, | 15 |
| = 1, Ψ | | = | 1, | ψ3 | = 2 | , ψ6 |

Un poco de atención enseña que tantos números pertenecen a cualquier exponente como tantos se dan no mayores que el y primos a el, o que en este caso particular, usando la notacion del art. 39, ψd = <pd. Ahora demostraremos que esta observaciún es verdadera en general.

I. Si se tiene algún número a perteneciente al exponente d (i.e., cuya d-esima potencia es congruente a la unidad y todas sus potencias inferiores son incongruentes), todas sus potencias a2, a3, a4, ...ad, o los menores restos de ellas, poseerán tambien la primera propiedad (la d-esima potencia de ellas es congruente a la unidad) y puesto que esto puede expresarse diciendo que todos los residuos mínimos de los numeros a,

a3, ...ad (que son todos diferentes) son raíces de la congruencia xd = 1 y como esta no puede tener mas que d raíces diferentes, es evidente que, excepto los residuos mínimos de los numeros a, a2, a3, ...ad, no se presenta ningun otro entre los numeros de 1 a p — 1 inclusive, cuya d-esima potencia sea congruente a la unidad. De donde,

a

2 „3

es claro que todos los números pertenecientes al exponente d se encuentran entre los residuos mínimos de los números a, a2, a3, . ..ad. Cuales son y cuantos son ellos, se encontrarú como sigue. Si k es un número primo a d, todas las potencias de ak, cuyos exponentes son < d, no serún congruentes a la unidad; pues, sea k (mod. d) ξ m (ver art. 31), sera akm ξ a, por tanto, si la e-esima potencia de ak fuera congruente a la unidad y e < d, entonces, resultaría akme ξ 1, y de aquí ae ξ 1, contrario a la hipútesis. Por eso, es claro que el residuo múnimo de ak pertenece al exponente d. Si k tiene algún divisor δ común con d, el residuo múnimo de ak no pertenecerá al exponente d, pues, ademas la |rásima potencia es congruente a la unidad (pues, kd

54.

***kS***

kd sería divisible por d, o sea ξ 0 (mod. d) y por ende a~ ξ 1). Por consiguiente, se reunen tantos numeros pertenecientes al exponente d como numeros de 1, 2, 3, ...d que sean primos a d. Pero, debe recordarse que esta conclusion esta basada en la suposición de que ya se tiene un numero a perteneciente al exponente d. Por lo cual queda la duda de si es posible que ningun numero pertenezca del todo a algun exponente y la conclusion se limita a que ’d sea = 0 o = φd.

II. Ahora sean d, d', d", etc. todos los divisores del numero p — 1: como todos los numeros 1, 2, 3, ...p — 1 esrán distribuidos entre estos,

ψ’d + ψd' + ’d'' + etc. = p — 1

Pero, en el art. 40, hemos demostrado que

φ^ + φδΐ! + φ^'' + etc. = p — 1

y del artículo anterior, se sigue que ’d es igual o menor que <^>d, pero no puede ser mayor; de modo semejante para ’d' y <^>d', etc., por lo tanto, si algun termino (o varios) de ’d, ’d', ’d'', etc., fuera menor que el termino correspondiente de <^>d, <^>d', <^>d'', la suma de aquellos no podría ser igual a la suma de estos. De esto concluimos que ’d siempre es igual a <^>d, y por eso no depende de la magnitud de p — 1.

55.

Un caso particular del artículo anterior merece muchísima atencion, a saber, siempre se presentan números de los cuales ninguna potencia menor que la (p — 1)- ésima es congruente a la unidad, y hay tantos de ellos entre 1 y p — 1 como numeros

menores que p — 1 y primos a p — 1. Puesto que la demostración de este teorema no es tan obvia como puede parecer a primera vista, y por la importancia del propio teorema, se puede añadir aquí otra bastante diferente de la anterior; ya que una diversidad de metodos suele ayudar mucho a esclarecer asuntos bastante dudosos. Resuelvase p — 1 en sus factores primos, de modo que p — 1 = aab3c7 etc., donde a, b, c, etc. denotan numeros primos diferentes. Entonces, complementaremos la demostración de este teorema por medio de lo siguiente:

1. Siempre puede encontrarse un numero A (o varios) pertenecientes al exponente aa, e igualmente nómeros B, C, etc., pertenecientes respectivamente a los exponentes b3, c7, etc.
2. El producto de todos los nuómeros A, B, C, etc. (o el producto de sus residuos mínimos) pertenece al exponente p — 1. Esto lo demostramos así:
3. Sea g algun nómero de 1, 2, 3, ...p — 1 que no satisface la congruencia

p — 1

x~a = 1 (mod. p). Como es de grado < p — 1, todos estos nómeros no pueden satisfacerla. Entonces, digo que si se pone = h la p-. -esima potencia de g, este nómero o su residuo mínimo perteneceró al exponente aa.

Pues, es evidente que la potencia aa-esima de h será congruente a la (p — 1)- esima de g, i.e., a la unidad. Pero, la aa-1-esima potencia de h sera congruente a la p-1 -esima potencia de g, i.e., sera no congruente a la unidad, y mucho menos las aa-2, aa-3, etc. potencias de h pueden ser congruentes a la unidad. Pero, el exponente de la potencia menor de h congruente a la unidad, o el exponente al cual pertenece h debe dividir al numero aa (art. 48). Por lo tanto, puesto que aa no es divisible por ningun otro numero mas que por sí mismo y por las potencias menores de a, necesariamente aa sera el exponente al cual pertenece h. Q. E. D. Con un metodo similar se demuestra que existen numeros que pertenecen a los exponentes b3, c7, etc.

1. Si suponemos que el producto de todos los A, B, C, etc. no pertenece al exponente p — 1, sino a uno menor t , p — 1 se dividirá por t (artículo 48), es decir,

sera un entero mayor que la unidad. Sin embargo, con facilidad se ve que este coeficiente o es uno de los numeros primos a, b, c, etc., o al menos es divisible por uno de ellos (artículo 17), e.g., por a. Con respecto a los otros, la demostracion es igual. Así, t dividira a p-1; por tanto, el producto ABC etc., elevado a la -esima potencia seró congruente a la unidad (artículo 46). Pero, es claro que cada uno de los B, C, etc. (excepto A) elevados a la p-1 -esima potencia serán congruentes a la unidad, cuando los exponentes b3, c7, etc. a los cuales pertenecen dividan a p-1. Por

De donde sigue que el exponente, ál cual pertenece A, debe dividir á p-1 (art. 48), p—! es entero; pero p+\_\ = ^Caetc· no puede ser un número entero (art. 15).

i.e.

eso se tendrá

A

*E-!*

*a*

***B***

*E*-1

*a*

C

*E*-1

*a*

etc.

p — 1

ΞΞ AV

1

Finalmente, hay que concluir que nuestra suposición no puede afirmarse, i.e., el producto ABC etc., en realidad, pertenece al exponente p — 1. Q. E. D.

La segunda demostracion parece algo mas larga que la primera, pero la primera resulta menos directa que esta.

56.

Este teorema suministra un ejemplo notable sobre cuanta circunspecciún se requiere siempre en la teoría de los numeros, para que no supongamos como cierto lo que no es. El celebre Lambert en su disertacion citada arriba, Acta Erudit. 1769, p. 127, hace mencion a esta proposition, pero no atestigua necesidad alguna de una demostracion. Nadie ha intentado una demostraciún excepto Euler, Comment. nov. Ac. Petrop. T. XVIII, 1773, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia p. 85 y siguientes. Vease en particular su artículo 37 donde hablo bastante sobre la necesidad de una demostraciún. Pero, la demostracion que el docto hombre presento tiene dos defectos. Uno: en su art. 31, tácitamente supone que la congruencia xn = 1 (traducidos sus argumentos usando nuestra notation) en realidad tiene n raíces diferentes, aunque, solo había demostrado anteriormente que no puede tener mas que n raíces. Otro: dedujo la fórmula de su artículo 34 solo por induction.

***Raíces primitivas, bases e índices.***

57.

Como el ilustre Euler, llamaremos raíces primitivas a los numeros pertene­cientes al exponente p — 1. Por lo tanto, si a es una raíz primitiva, los residuos mínimos de las potencias a, a2, a3, ...ap-1 serán todos diferentes, de donde se deduce fácilmente que entre estos deben aparecer todos los nímeros 1, 2, 3, ...p — 1, ya que el numero de estos es igual al numero de residuos mínimos, i.e., cualquier numero no divisible por p es congruente a alguna potencia de a. Esta propiedad notable es de gran utilidad y puede simplificar bastante las operaciones aritmíeticas respecto a las

congruencias, casi de igual modo como la introducción de los logaritmos simplifica las operaciones de la aritmética comón. Elegiremos libremente alguna raíz primitiva como base, a la cual referiremos todos los nómeros no divisibles por p, y si ae ξ b (mod. p), llamaremos a e el índice de b. Por ejemplo, si para el módulo 19 se toma la raíz primitiva 2 como base, corresponderón

nómeros 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. índices 0. 1. 13. 2. 16. 14. 6. 3. 8. 17. 12. 15. 5. 7. 11. 4. 10. 9.

Es claro, ademas, al mantener la base constante, que a cada nómero corresponden varios óndices, pero todos ellos serán congruentes segun el módulo p — 1. Por lo que, cuando hay una discusión sobre los mdices, aquellos que son congruentes segón el modulo p — 1 se consideraran equivalentes de la misma manera como los numeros se consideran equivalentes cuando son congruentes segun el modulo p.

***Algoritmos de los índices.***

58.

Los teoremas que tratan sobre los índices son completamente analogos a los que se refieren a los logaritmos.

***El índice del producto compuesto de cualquier número de factores es con­gruente, según el modulo p — 1, a la suma de los índices de los factores individuales.***

***El índice de la potencia de un numero cualquiera es congruente, segun el modulo p — 1, al producto del índice del numero dado por el exponente de la potencia.***

Hemos omitido las demostraciones por su facilidad.

De esto se percibe que si deseamos construir una tabla de la cual se puedan sacar los índices de todos los numeros segun modulos diferentes, de esta se pueden omitir tanto todos los numeros mayores al modulo como todos los compuestos. Se ha agregado un ejemplo de este tipo de tabla al final de esta obra, Tab. I, donde en la primera columna vertical se colocan los numeros primos y las potencias de numeros primos de 3 hasta 97, los cuales se deben considerar como modulos. A la par de estos estan los numeros tomados como base. Luego siguen los índices de los numeros primos sucesivos que siempre estan arreglados en pequeños bloques de cinco. Arriba los numeros primos estan dispuestos en el mismo orden; de modo que un índice que corresponda a un numero primo dado, segun un modulo dado, pueda encontrarse facilmente.

Así por ejemplo si p = 67; el índice del número 60, tomado 12 como base, será ξ 2Ind. 2 + Ind. 3 + Ind. 5 (mod. 66) ξ 58 + 9 + 39 ξ 40.

59.

***El indice de un valor cualquiera de la expresión*** | (mod. p), ***(art. 31) es congruente, según el modulo p — 1, a la diferencia de los indices del numerador a y del denominador b, si es que a y b no son divisibles por p.***

Sea c, pues, un valor cualquiera; tenemos bc ξ a (mod. p) y por lo tanto

Ind. b + Ind. c ξ Ind. a (mod. p — 1) y así Ind. c ξ Ind. a — Ind. b

Entonces, si se tiene una tabla con el índice que corresponde a cualquier número, según cualquier modulo primo, y otra de la cual pueda derivarse el número que corresponda a un índice dado, todas las congruencias de primer grado podran resolverse muy facilmente; puesto que todas pueden reducirse a aquellas cuyo modulo es un primo (art. 30). E.g., la congruenca propuesta

7

29x + 7 ξ 0 (mod. 47) será x ξ — (mod. 47)

29

De donde Ind. x ξ Ind. —7 — Ind. 29 ξ Ind. 40 — Ind. 29 ξ 15 — 43 ξ 18 (mod. 46)

Pero, se encuentra el número 3 cuyo índice es 18. Así, x ξ 3 (mod. 47). No hemos adjuntado la segunda tabla; pero, a cambio de esto, podrí servir otra en su lugar, como mostraremos en la Secciún VI.

***Sobre las raíces de la congruencia xn=A.***

60.

De una manera semejante a como hemos designado en el art. 31 las raíces de las congruencias del primer grado, así, en lo siguiente, presentaremos las raíces de las congruencias puras de grados mayores con un símbolo. Como ^A no puede significar mús que una raíz de la ecuación xn = A, así al adjuntarse el modulo con el símbolo (mod. p) se denotarú cualquier raíz B de la congruencia xn ξ A

(mod. p). Decimos que esta expresion tyA (mod. p) tiene tantos valores comoraíces incongruentes mod. p, puesto que todos los que son congruentes según el modulo p se consideran como equivalentes (art. 26). Además, es claro que si A y B son congruentes, segán el mádulo p las expresiones nA y nB (mod. p) serán equivalentes.

Ahora, si se pone tyA = x (mod. p), será n Ind. x = Ind. A (mod. p — 1). De esta congruencia, se deducen, segán las reglas de la sección anterior, los valores de Ind. x, y de estos, los valores correspondientes de x. Facilmente, se percibe que x tiene tantos valores como raíces de la congruencia n Ind. x = Ind. A (mod. p — 1). Es claro, pues, que nA tendrá un ánico valor, cuando n es primo a p — 1; sin embargo, cuando los námeros n y p — 1 tienen un máximo comun divisor δ, Ind. x tendrá δ valores incongruentes segun el modulo p — 1, y nA tantos valores incongrentes, segun p, siempre que Ind. A sea divisible por δ. Al faltar esta condicion, PA no tendrá ningán valor real.

Ejemplo. Búsquense los valores de la expresión ν'ΓΪ (mod. 19). Asá, debe resolverse la congruencia 15 Ind. x = Ind. 11 = 6 (mod. 18) y se encontraran tres valores de Ind. x = 4, 10, 16 (mod. 18). Los valores correspondientes de x son 6, 9 y 4.

61.

Por mas facil que este metodo sea, cuando esrán adjuntadas las tablas necesarias, no debemos olvidarnos de que este es indirecto. Por lo tanto, vale la pena investigar cuan poderosos son los metodos directos; trataremos aquá lo que pueda resultar de lo anterior; otros que requieren consideraciones máas profundas esrán reservados para la seccián VIII. Iniciamos con el caso mas sencillo, donde A = 1, es decir, donde se buscan las raíces de la congruencia xn = 1 (mod. p). Aquí, por tanto, tomando cualquier raíz primitiva como base, debe resultar n Ind. x = 0 (mod. p — 1). Esta congruencia, cuando n es primo a p — 1, tendrá una sola raíz; es decir, Ind. x = 0 (mod. p — 1). En este caso -^T (mod. p) tendrá un unico valor, o sea = 1. Sin embargo, cuando los numeros n y p — 1 tengan maximo comun divisor δ, la solucion completa de la congruencia n Ind. x = 0 (mod. p — 1) sera Ind. x = 0 (mod. p-1) (ver art. 29): i.e., Ind. x, segun el modulo p — 1, deberá ser congruente a alguno de estos numeros

p — 1 2(p — 1) 3(p — 1) (δ — 1)(p — 1)

δ

δ

δ

δ

o tendrá δ valores incongruentes según el módulo p — 1, por tanto, también en este caso, x tendrá δ valores diferentes (incongruentes según el modulo p). De donde se percibe que la expresión p1 tambien tiene δ valores diferentes, cuyos índices coinciden completamente con los anteriores. Por eso, la expresión p1 (mod. p) equivale totalmente a p1 (mod. p); i.e., la congruencia χδ ξ 1 (mod. p) tiene las mismas raíces que esta, xn ξ 1 (mod. p). La anterior, sin embargo, seró de grado inferior, si δ y n no son iguales.

Ejemplo. v'T (mod. 19) tiene tres valores, pues 3 es el maximo divisor comun de los numeros 15 y 18 y, a la vez, estos serán valores de la expresión p1 (mod. 19). Estos son 1, 7 y 11.

62.

Por medio de esta reduccion, no logramos resolver ninguna otra congruencia sino las de la forma xn ξ 1, donde n es un divisor del numero p — 1. Mas adelante, mostraremos que las congruencias de esta forma siempre pueden reducirse, pero lo anterior no basta. Podemos aquí tratar un solo caso, o sea, donde n = 2. Es claro que los valores de la expresion p1 serán +1 y —1, pues, no puede tener mas que dos y +1 y —1 siempre son incongruentes a menos que el modulo sea = 2, en cuyo caso p1 puede tener un solo valor, como se puede ver. De donde, por consiguiente, sigue que +1 y —1 serán tambien los valores de la expresion 2^Ι cuando m es primo a Pp. Esto siempre sucede cuando el modulo es de esta clase, con tal que sea un numero absolutamente primo (a menos que p — 1 = 2m, en tal caso todos los numeros 1, 2, 3, ...p— 1 son raíces), e.g., cuando p = 3, 5, 7, 11, 23, 47, 59, 83, 107 etc. Se adjuntara aquí como corolario que el índice de —1 siempre es ξ P-1 (mod. p — 1) cualquiera que sea la raíz primitiva tomada como base. Pues, 2Ind. (—1) ξ 0 (mod. p — 1). Así, Ind. (—1) sera ξ 0, o ξ P-1 (mod. p — 1). Pero, 0 siempre es el índice de +1, y +1 y —1 siempre deben tener diferentes índices (excepto el caso p = 2, al que no vale la pena referirse aquí).

63.

Hemos mostrado, en el art. 60, que la expresion pA (mod. p) tiene δ valores diferentes, o no tiene ninguno, si δ es el maximo comun divisor de los numeros n y p — 1. Ahora, del mismo modo como mostramos que pA y pA son equivalentes si A ξ 1, demostramos mas generalmente que la expresion pA siempre puede reducirse

a la otra v'B, a la cual equivalga. Pues, denotado un valor cualquiera de éstos por x, sera xn = A; ahora, sea t un valor cualquiera de la expresión n (mod. p — 1), la cual tiene valores reales como se percibe en el art. 31, sera xtn = A^, pero xtn = χδ, puesto que tn = δ (mod. p — 1). Por tanto, x^ = At y cualquier valor de v^A sera tambien un valor de ^A3. Por lo tanto, cuando vA tiene valores reales, sera totalmente equivalente a la expresion νΆ^, puesto que aquella ni tiene otros valores diferentes a la anterior, ni tiene menos. Es posible que vA no tenga ningun valor real aun cuando νΆ\* tenga valores reales.

Ejemplo. Si se buscan los valores de la expresion 2^2 (mod. 31), el maximo comun divisor de los numeros 21 y 30 sera 3, y este es un valor de la expresion (mod. 30); por tanto, si v^2 tiene valores reales, equivaldrá a la expresion o sea ^8, se encontrara en verdad que los valores de la expresion posterior, que son 2, 10, 19, tambien satisfacen la anterior.

64.

Para no intentar realizar en vano esta operacion, conviene investigar una regla por medio de la cual pueda deducirse de inmediato si vA admite valores reales o no. Si se tiene una tabla de índices, el asunto es claro, pues, es claro, en el art. 60, que se tendrán valores reales si el índice de A, tomando cualquier raíz primitiva como base, es divisible por δ; pero si no lo es, no se tendrán. No obstante, esto puede hallarse sin esa tabla. Pues, al poner el índice de A = k, si es divisible por δ, sera divisible

por p — 1 y vice-versa. Pero, el índice del numero A~— sera . Por lo cual, si vA

(mod. p) tiene valores reales, Asera congruente a la unidad; en caso contrario, sera incongruente. Así, en el ejemplo del artículo anterior, se tiene 2j0 = 1024 = 1 (mod. 31), de donde se concluye que 2^2 (mod. 31) tiene valores reales. De modo semejante, resulta cierto que ^ — 1 (mod. p) siempre tiene dos valores reales cuando p es de la forma 4m + 1, pero ninguno cuando p es de la forma 4m + 3, puesto que (—1)2m = 1 y (—1)2m+j = —1. Este elegante teorema se enuncia ordinariamente así: si p es número primo de la forma 4m + 1, se puede encontrar un cuadrado a?, de modo que a2 + 1 sea divisible por p, pero si al contrario, p es de la forma 4m — 1, no se puede encontrar tal cuadrado. De esta forma fue demostrado por el ilustre Euler, en Comm. nov. Acad. Petrop. XVIII, p. 112 del año 1773. El ya había presentado otra demostracion mucho antes en 1760, Comm. nov. V, p. 5. En una disertacion anterior, Comm. nov. IV, p. 25, todavía no la había perfeccionado. Luego, el ilustre Lagrange

presentó una demostración del teorema, Nouveaux Mém. de l’Ac. de Berlín, 1775, p. 342. Presentaremos otra demostración, en la siguiente sección, específicamente dedicada a este argumento.

65.

Despues de que hemos hablado de reducir todas las expresiones ^~A (mod. p) a otras, donde n es divisor del nómero p — 1, y hemos encontrado un criterio de si admite o no valores reales, consideraremos mós precisamente tales expresiones tfA (mod. p), donde n es divisor de p — 1. Primero mostraremos que relacion tienen los valores individuales de la expresion entre sí; luego indicaremos unos artificios, con cuya ayuda muchas veces puede encontrarse un valor de la expresióon.

Primero. Cuando A ξ 1 y r es alguno de los n valores de la expresión (mod. p), ó rn ξ 1 (mod. p), tambien todas las potencias de este r serán valores de esta expresión; pero de ellos, tantos serón diferentes como unidades tenga el exponente al cual r pertenece (art. 48). Si, por lo tanto, r es el valor que pertenece al exponente n, estas potencias r, r2, r3, ...rn de este mismo r (donde en el lugar de la última puede sustituirse la unidad) involucrarón todos los valores de la expresion (mod. p). En la seccion VIII explicaremos bastante cuales metodos existen para encontrar aquellos valores que pertenecen al exponente n.

Segundo. Cuando A es incongruente a la unidad, y conocemos un valor de la expresión nA (mod. p), digamos z, los restantes pueden deducirse del siguiente modo. Sean los valores de la expresión

1. r, r2,

rn-1

(como mostramos arriba). Entonces todos los valores de la expresión ^A serón

2 n 1

z, zr, zr2, ...zrn 1.

Esta claro, pues, que todos estos satisfacen la congruencia xn ξ A: pongamos cualquiera de ellos ξ zrk, la n-esima potencia de ella, znrnk, por ser rn ξ 1 y zn ξ A, sera congruente a A. Todos son diferentes como se deduce facilmente del art. 23; pero la expresión ^A no puede tener mas que estos n valores. Asó, por ejemplo, si un valor de una expresion ^A es z, el otro seró —z. Finalmente, de esto se debe concluir que no se pueden encontrar todos los valores de la expresión ^A si no se conocen igualmente todos los valores de la expresión ^1.

66.

Lo segundo que nos habíamos propuesto mostrar era en cuál caso un valor de la expresión PA (mod. p) puede encontrarse directamente (donde se supone que n es un divisor de p — 1). Esto resulta cuando algán valor es congruente a alguna potencia de A, lo cual no es tan raro, y no sera superfluo detenernos en ello. Sea tal valor z, si existe, o sea z ξ Ak y A ξ zn (mod. p). De esto se deduce que A ξ Akn; por lo tanto, si se tiene un námero k, de modo que A ξ Akn, Ak será el valor buscado. Pero esto equivaldrá aquí a la condicián siguiente, 1 ξ kn (mod. t), denotando a t el exponente al cual pertenece A (art. 46, 48). Para que esta congruencia sea posible, se requiere que n sea primo a t. En este caso sera k ξ n (mod. t), pero si t y n tienen un divisor comán, ningun valor z puede ser congruente a alguna potencia de

A.

67.

No obstante, como conviene conocer a t para esta solucián, veamos como podemos proceder si desconocemos este número. Primero, se percibe fácilmente que t debe dividir a p-1, si es que pA (mod. p) tiene valores reales, como siempre lo hemos supuesto aquí. Sea pues y una solucion cualquiera, entonces tendremos yp\_1 ξ 1 y yn ξ A (mod. p); por lo cual elevando las partes de la ultima congruencia a la p-1 -esima potencia resultará AE— ξ 1; de tal modo p-1 es divisible por t (art. 48). Ahora, si p-1 es primo a n, la congruencia del artículo anterior, kn ξ 1, no sálo podrá resolverse segán el modulo p-1, sino claramente el valor de k que satisface a esta congruencia segán este modulo tambien la satisfará segán el mádulo t, el cual divide a p-1 (art. 5). Por tanto, se ha encontrado lo buscado. Sin embargo, si p-1 no es primo a n, se eliminaran todos los factores primos de p-1, que a la vez dividen a n. Por eso, encontraremos un námero p-1, primo a n, donde q denota el producto de todos los factores primos que hemos eliminado. Ahora, si la condicioán que logramos en el artáculo anterior, que t sea primo a n, tiene lugar, t no sáolo seraá primo a q sino tambien dividirá a p-1. Por eso, si se resuelve la congruencia kn ξ 1 (mod. p-1) (lo que puede ser, puesto que n es primo a p-1), el valor k tambien satisfará la congruencia, segun el mádulo t; lo cual se buscaba. Todo este artificio consiste en hallar un námero que pueda funcionar en vez de t, el cual no conocemos. Aunque siempre conviene recordar: hemos supuesto que, cuando p-1 no es primo a n, cabe la condicion del artículo anterior, pero si no es cierta, todas las conclusiones seráan erráoneas. Sin embargo, si auán siguiendo las reglas dadas, se encuentra un valor

para z, cuya n-ésima potencia es incongruente a A, esto sería una muestra de que la condición no puede satisfacerse y que el metodo no puede emplearse del todo.

68.

Pero, en este caso tambien puede ser ventajoso haber realizado este trabajo y vale la pena investigar como este valor falso se relaciona con los verdaderos. Así, supongamos que los numeros k y z estan bien determinados, pero que zn no es = A (mod. p). Entonces, si solo pueden determinarse valores de la expresion ^ZV (mod. p), multiplicando cada uno de estos valores por z, obtendremos los valores de V/A. Pues si v es algun valor de ^ZV: sera (vz)n = A. Pero la expresion ^ZV es mas simple que v^A, puesto que ZV (mod. p) con frecuencia pertenece a un exponente menor que A. Es decir, si d es el maximo comun divisor de los numeros t y q, ZV (mod. p) pertenecerá al exponente d, como se demostrara ahora. Sustituyendo por

(mod. p). Pero, kn — 1 es divisible por p-1 (artículo

el valor z sera ZV = jkV-T

p-1 sera divisible por -j o bien pnq1 por d. Tambien kn — 1 sera divisible por d y (kn — 1)d por t. Por lo tanto, A(kn-1)d = 1 (mod. p). De donde se deduce facilmente que ZV, elevada a la drásima potencia, sera congruente a la unidad. El que Zñ no pueda pertenecer a un exponente menor que d, puede demostrarse facilmente; pero, ya que no se requiere para nuestros fines, no nos detendremos en esto. Podemos estar seguros que ZV (mod. p) siempre pertenecerá a un exponente menor que A, excepto en un caso unico, cuando t divide a q; de donde d = t.

anterior), p—1 por t (ibid.) o sea 2—1 por d. Ahora bien d es primo a d (hip.), así

***nd***

p—1

***tq***

Pero, ¿de que sirve que ZV pertenezca a un exponente menor que A? Se presenta mayor cantidad de numeros que pueden ser A que los que pueden ser ZV, y cuando haya ocasion de desarrollar varias expresiones ^A segun un mismo modulo, tendremos la ventaja de derivar varios resultados de una misma fuente. Así, por ejemplo, siempre sera posible determinar al menos un valor de la expresion tyA (mod. 29), si solo se conocen los valores de la expresion ^ —1 (que son ±12). Del artículo anterior se conoce facilmente que un valor de esta expresion siempre puede determinarse directamente, ya sea cuando t es impar y d = 2 o cuando t es par. Excepto para —1, ningun otro numero pertenece al exponente 2.

Ejemplos. Búsquese (mod. 37). Aquí, p — 1 = 36, n = 3, 2—1 = 12,

y así q = 3. Por lo tanto, debe ser 3k = 1 (mod. 4), lo cual se obtiene poniendo k = 3. Aquí z = 313 (mod. 37) = 6, se halla realmente 63 = 31 (mod. 37). Si losvalores de la expresión (mod. 37) son conocidos, también los restantes valores de la expresión pueden determinarse. Los valores de pT (mod. 37) son 1, 10 y 26. Al multiplicarlos por 6, se producen los restantes ξ 23 y 8.

Sin embargo, si se busca el valor de la expresión (mod. 37), seró n = 2,

p-1 = 18, y de aquí q = 2. Por tanto, debe ser 2k ξ 1 (mod. 9), de donde resulta k ξ 5 (mod. 9). Por consiguiente, z ξ 35 ξ 21 (mod. 37); pero 212 no es ξ 3, sino ξ 34. Así, 34 (mod. 37) ξ—1, y — 1 (mod. 37) ξ ±6; de donde se obtendrán los valores verdaderos ±6 · 21 ξ ±15.

Esto es casi todo lo que se puede decir acerca del desarrollo de tales expresiones. Es evidente que los metodos directos con frecuencia resultan bastante largos; pero esto es cierto para casi todos los metodos directos en la teoría de los números; por esto, consideramos que debemos demostrarlo. Tambien, conviene observar que no es de nuestro interes explicar los artificios particulares que se presentan aquó.

***La conexión entre los indices en sistemas diferentes.***

69.

Volvemos ahora a las raíces que llamamos primitivas. Hemos mostrado, al tomar una raíz primitiva cualquiera como base, que todos los números, cuyos índices son primos a p— 1, tambien serán raíces primitivas, y ninguno aparte de estos. A la vez se conoce el numero de raíces primitivas. Vease art. 53. En general, queda a nuestro arbitrio saber cual raíz primitiva escogeremos como base. De esto se percibe, tambien aquí, como en el cílculo logarítmico, que pueden presentarse diferentes sistemas[[107]](#footnote-108)). Veamos las relaciones que los conectan. Sean a y b dos raíces primitivas, sea m otro nímero. Cuando se toma a a como base, el índice del nímero b ξ β, pero el índice del numero m ξ μ (mod. p — 1); cuando se toma b como base, el índice del nímero a ξ α, el índice de b sin embargo ξ ν (mod. p — 1). Entonces sera αβ ξ 1 (mod. p — 1); puesto que αβ ξ b, de donde ααβ ξ ba ξ a (mod. p) (por hipótesis), por lo tanto αβ ξ 1 (mod. p — 1). Mediante un razonamiento similar, se descubre que ν ξ αμ, por eso μ ξ βν (mod. p — 1). Por lo tanto, si se ha construido una tabla de índices para la base a, facilmente puede convertirse en otra, donde la base es b. Pues si para la base a el índice de b es ξ β, para la base b el índice de a sera

= 1 (mod. p — 1), y multiplicando todos los índices de la tabla por este número, se tendrán todos los índices para la base b.

70.

Aunque un número dado puede tener varios índices, tomadas unas u otras raíces primitivas como base, todas concuerdan en esto: todos tendrán el mismo maximo comun divisor con p — 1. Pues, si por la base a, el índice del numero dado es m, pero por la base b es n, y si los maximos comunes divisores μ y ν con p — 1 se suponen diferentes, uno de ellos sera mayor, por ejemplo μ > ν, y por eso n no dividirá a μ. Pero, denotado el índice de a por a, cuando se toma a b como base, sera (artículo anterior) n = am (mod. p — 1), de donde μ dividirá a n. Q. E. A.

Se percibe tambien que este maximo comun divisor de los índices de un numero dado y de p — 1 no depende de la base porque es igual a pP, donde t denota el exponente al cual pertenece el numero sobre cuyos índices se trata. Pues si el índice para una base cualquiera es k, t sera el numero menor que, multiplicado por k, resultara un multiplo de p — 1 (excepto cero) (veanse artículos 48 y 58), o sea, el valor menor de la expresión k (mod. p — 1) excepto cero. No obstante, que esto es igual al maximo comun divisor de los numeros k y p — 1, se obtiene del artículo 29 sin dificultad.

71.

Ademas se demuestra facilmente que la base siempre puede tomarse de modo que un numero que pertenece al exponente t tiene cualquier índice dado cuyo maximo comun divisor con p — 1 es = pP. Por brevedad, designaremos este por d, si el índice propuesto es = dm, y el índice del numero propuesto = dn, cuando se toma cualquier raíz primitiva como base, entonces m y n serán primos a p-1, o sea a t. Entonces, si ε es el valor de la expresion dn (mod. p — 1) y a la vez es primo a p — 1, αε sera una raíz primitiva. Tomada esta como base, el numero propuesto producirá el índice dm (pues sera aedm = adn = numero propuesto). Pero, del modo siguiente se demuestra que la expresion dn (mod. p — 1) admite valores primos a p — 1. Esta expresion equivaldrá a: m (mod. p-1) o sea m (mod. t) (vease art. 31, 2). Todos sus valores serán primos a t; ya que, si algun valor e tuviera un divisor comun con t, este divisor tambien debería dividir a me, por tanto, tambien me es congruente a n segun t, contrariamente a la hipotesis de que n es primo a t. Por lo tanto, cuando todos los

divisores primos de p — 1 también dividen a t, todos los valores de la expresión (mod. t) serán primos a p — 1, y el número de ellos = d. Sin embargo, cuando p — 1 involucra otros divisores primos f, g, h, etc., que no dividen a t, se toma cualquier valor de la expresion m (mod. t) ξ e. Entonces, puesto que t, f, g, h, etc., son primos entre sí, puede hallarse un námero ε que es congruente a e segán el mádulo t, pero segun f, g, h, etc. es congruente a námeros cualesquiera primos a estos respectivamente (art. 32). Por eso tal numero no sera divisible por ningun factor primo de p — 1, por lo tanto sera primo a p — 1, tal como se esperaba. Finalmente, sin dificultad alguna, se deduce de la teoría de las combinaciones que el numero de tales valores sera = · f1 · · etc.; pero para que no se extienda mucho

esta disgresion, hemos omitido la demostracion, puesto que no nos concierne.

n

m

***Bases adaptadas para usos especiales.***

72.

Aunque generalmente sea muy arbitrario cual raíz primitiva se tomara como base, a veces ciertas bases pueden presentar algunas conveniencias especiales. En la tabla I, siempre hemos tomado el numero 10 como la base cuando este era raíz primitiva; de otra manera hemos determinado la base de modo que el índice del námero 10 sea el menor posible, i.e., = , donde t denota el exponente al cual

pertenecio 10. Pero, lo que ganamos con esto, lo presentaremos en la Seccion VI, donde la misma tabla se aplicara para otros fines. Sin embargo, puesto que aquí esto todavía puede permanecer un poco arbitrario, como aparece en el articulo anterior: para establecer algo fijo, de todas las raíces primitivas, eligimos siempre como base la menor. As í, para p = 73, donde t = 8 y d = 9, ae tiene 722, i.e., 6 valores que son 5, 14, 20, 28, 39, 40. Por esto, tomamos el mínimo, 5, como base.

***Método para la determinación de las raíces primitivas.***

73.

Los metodos para encontrar las raíces primitivas se basan en su mayoría en el tanteo. Si se reune lo que hemos aprendido en el artículo 55, con lo que diremos adelante sobre las soluciones de la congruencia xn ξ 1, se tendrá casi todo lo que puede lograrse con los metodos directos. El ilustre Euler reconoce (Opuscula Analytica, T. I, p. 152) que parece extremadamente difícil encontrar estos numeros, y se refiere a su naturaleza como uno de los misterios mas grandes de los numeros. Pero,

pueden determinarse bastante rápidamente al intentarlo de la siguiente manera. Un conocedor sabrá evitar operaciones prolijas por medio de varios artificios particulares: pero esto se aprende mas rápidamente con práctica que con preceptos.

1o. Tómese libremente un numero a, primo a p (siempre designamos el modulo con esta letra) (casi siempre lleva a los calculos cortos si escogemos el menor posible, e.g., el námero 2); luego determínese su período (art. 46), i.e., los residuos mínimos de sus potencias, hasta encontrar la potencia a^ cuyo residuo mínimo sea 1[[108]](#footnote-109)). Ahora, si t = p — 1, a es una raíz primitiva.

2o. Pero, si t < p — 1, se toma otro námero b que no esta en el período de a, y de modo semejante se investigara su período. Al designar por u el exponente al cual pertenece b, se percibe facilmente que u ni puede ser igual a t, ni a un factor de t; de hecho en los dos casos sería bt = 1; lo cual no puede ser, puesto que el período de a contiene todos los nímeros cuya t-esima potencia es congruente a la unidad (art. 53). Ahora si u es = p — 1, b serí una raíz primitiva; pero si u no es = p — 1, sino un míltiplo de t, hemos logrado esto: que conocemos un numero perteneciente a un exponente mayor, de modo que nuestro proposito, encontrar el nímero perteneciente al exponente máximo, estí próximo. Pero si u no es = p — 1, ni a un multiplo de t, no obstante, podemos encontrar un nímero u que pertenece a un exponente mayor que t, a saber, al exponente igual al mínimo comun multiplo de los nímeros t y u. Sea este = y, así resuelvase y en dos factores primos entre sí, m y n, de modo que uno divide a t, y el otro a uj). Entonces, la mrásima potencia de a sera ξ A, la n-esima potencia de b sera ξ B (mod. p), y el producto AB sera un numero perteneciente al exponente y. Es facil percibir que A pertenece al exponente m, y B al exponente n, de modo que el producto AB pertenecerá a mn, puesto que m y n son primos entre sí. Esto podra demostrarse prácticamente del mismo modo como en el art. 55, II.

3o. Ahora, si y = p — 1, AB sera una raíz primitiva. Si no es el caso, entonces de igual manera que antes se deberá tomar otro numero que no aparece en el período de AB. Esto, o bien, sera una raíz primitiva, o pertenecerá a un exponente mayor que y, o por medio de el (como antes) podra encontrarse un numero que pertenece a un exponente mayor que y. Por tanto, como los numeros que resultan de repeticiones

de esta operación pertenecen a exponentes continuamente crecientes; es claro que, finalmente, se debe encontrar un número que pertenezca al exponente mayor, i.e., una raíz primitiva. Q. E. F.

74.

Estas reglas anteriores serán mas claras mediante un ejemplo. Sea p = 73 para el cual se busca una raíz primitiva. Intentaremos primero con el número 2, cuyo período es el siguiente:

1.2.4.8.16.32.64.55.37.1 etc.

0.1.2.3. 4. 5. 6. 7. 8.9 etc.

Puesto que ya la potencia del exponente 9 es congruente a la unidad, 2 no es una raíz primitiva. Pruebese con otro numero que no aparece en el período de 2, por ejemplo 3, cuyo período es este:

1.3.9.27.8.24.72.70.64.46.65.49. 1 etc.

0.1.2. 3.4. 5. 6. 7. 8. 9.10.11.12 etc.

Por lo tanto, 3 tampoco es una raíz primitiva. En cambio, el mínimo comín míltiplo de los exponentes a los cuales pertenecen 2 y 3 (i.e., los numeros 9 y 12) es 36, el cual se resuelve en los factores 9 y 4 segín los preceptos del artículo anterior. Así que al elevarse 2 a la potencia |, i.e., reteniendo el nímero 2; y 3 a la potencia 3: el producto de estos es 54, que por tanto pertenecerá al exponente 36. Si finalmente se calcula el período de 54, y se intenta con un numero no contenido en el, por ejemplo, el numero 5, se descubrirá que es una raíz primitiva.

***Varios teoremas sobre los períodos y las raíces primitivas.***

75.

Antes de dejar este argumento, presentaremos algunas proposiciones, a las que por su simplicidad conviene prestarles atencion.

***El producto de todos los términos del período de un número cualquiera es = 1, cuando el número de ellos o el exponente al cual pertenece el número es impar, y*** = — 1 ***cuando este exponente es par.***

Ejemplo. Para el modulo 13 el período del nímero 5 consta de estos terminos 1, 5, 12, 8, cuyo producto 480 ξ —1 (mod. 13).

Segun el mismo modulo, el período del numero 3 consta de los terminos 1, 3, 9, cuyo producto 27 ξ 1 (mod. 13).

Demostración. Sea t el exponente al cual pertenece un número, y el índice del número, lo cual siempre puede ser si se determina debidamente la base (art. 71). Entonces, el índice del producto de todos los terminos del período serú

ξ (1 + 2 + 3+ etc. + t - 1)P-— =

t 2

i.e., ξ 0 (mod. p — 1) cuando t es impar, y ξ cuando t es par; por tanto, en el primer caso este producto ξ 1 (mod. p); en el último ξ—1 (mod. p), (art. 62). Q. E. D.

76.

Si ese número en el teorema precedente es una raíz primitiva, su período comprenderú todos los numeros 1, 2, 3, ...p — 1, cuyo producto siempre ξ — 1 (pues p — 1 es siempre par, excepto un caso, p = 2, en el cual —1 y +1 son equivalentes). Este elegante teorema suele enunciarse asú: el producto de todos los números menores que un número primo dado, sumado a uno, es divisible por este primo. Fue publicado primero por el celebre Waring, y adscrito a Wilson, (Meditt. algebr., tercera edición, p. 380). Pero ninguno pudo demostrarlo, y el celebre Waring confeso que la demostracion parecúa mús difícil porque ninguna notacion puede confeccionarse para expresar un número primo. Pero a nuestro juicio tales verdades debúan percibirse por medio de las nociones mús que por las notaciones. Despues, el ilustre Lagrange presento una demostracion (Nouv. Mém. de l’Ac. Berlin, 1771). Se basa en la consideracion de los coeficientes originados en el desarrollo del producto

(x + 1)(x + 2)(x + 3)... (x + p — 1).

De hecho, con poner este producto

ξ xp-1 + Axp-2 + Bxp-3 + etc. + Mx + N

los coeficientes A, B, etc., M serún divisibles por p, y N serú =1 · 2 · 3 · ... · p — 1. Ahora, para x = 1, el producto serú divisible por p; entonces sera ξ 1 + N (mod. p), de donde necesariamente 1 + N podraú dividirse por p.

Finalmente, el ilustre Euler ha presentado una demostraciún en Opusc. analyt. T. I. p. 329 que concuerda con la expuesta por nosotros. Pero si tan distinguidos matematicos no han considerado sin merito a este teorema para sus meditaciones, esperamos no ser censurados si adjuntamos todavía otra demostracion.

77.

Cuando según el módulo p, el producto de dos números a y b es congruente a la unidad, llamaremos a los números a y b asociados, tal como lo hizo Euler. Entonces, segun la sección anterior, cualquier número positivo menor que p tendró un unico asociado positivo menor que p. Puede demostrarse fócilmente que de los números 1, 2, 3,...p — 1, los únicos asociados de si mismos son 1 y p — 1: pues los números asociados de si mismos serún raíces de la congruencia x2 ξ 1; que es de segundo grado, por tanto no puede tener mús que dos raíces, i.e., ninguna otra mas que 1 y p — 1. Excluidos estos de los numeros restantes, 2, 3, ...p — 2 estarún asociados siempre en pares; por tanto el producto de ellos sera ξ 1, de donde el producto de todos 1, 2, 3, ...p — 1, serú ξ p — 1o sea ξ—1. Q. E. D.

Por ejemplo, para p = 13, se asocian los números 2, 3, 4, ... 11 así: 2 con 7; 3 con 9; 4 con 10; 5 con 8; 6 con 11; entonces 2 · 7 ξ 1;3 · 9 ξ 1 etc. Por tanto 2 · 3 · 4 · ... 11 ξ 1, y 1 · 2 · 3... 12 ξ—1.

78.

El teorema de Wilson puede exponerse mas generalmente así: el producto de todos los números, a la vez menores que cualquier nUmero dado A y primos a él mismo, es congruente, segun el modulo A, a la unidad tomada positiva o negativamente. Se debe tomar la unidad negativamente cuando A es de la forma pm, o bien 2pm, donde p denota un número primo diferente de 2, y ademas cuando A = 4; se toma positivamente en todos los casos restantes. El teorema, como fue presentado por el celebre Wilson, esta contenido bajo el primer caso. Por ejemplo, para A = 15, el producto de los numeros 1,2,4, 7, 8, 11, 13, 14 es ξ 1 (mod. 15). Por brevedad no adjuntamos la demostracioún: observamos solamente que puede completarse de modo semejante al del artúculo anterior, excepto que la congruencia x2 ξ 1 puede tener mas de dos raúces, las cuales exigen ciertas consideraciones peculiares. Tambien la demostracion puede derivarse de la consideraciún de los úndices, similarmente como en el artúculo 75, si se agrega lo que pronto expondremos sobre los múodulos compuestos.

79.

Volvemos a la enumeracion de otras proposiciones (art. 75).

La suma de todos los términos del período de un numero cualquiera es ξ 0, como en el ejemplo del artúculo 75, 1 + 5+ 12 + 8 = 26 ξ 0 (mod. 13).

*a\* —* 1

Demostración. Sea a el número de cuyo período se trata, y t el exponente al cual pertenece. La suma de todos los terminos del período serú:

= i + a+aa + aa + etc. + a 1

*a —* 1

(mod. p)

Pero, a\* — 1 ξ 0: por tanto esta suma siempre sera ξ 0 (art. 22), a menos que por casualidad a — 1 sea divisible por p, o sea a ξ 1; por lo tanto, este caso debe excluirse si deseamos llamar período a un solo termino.

80.

El producto de todas las raíces primitivas es ξ 1, excepto el caso único p = 3; pues en este se presenta una sola raíz primitiva, 2.

Demostración. Si se toma una raíz primitiva cualquiera como base, los índices de todas las raíces primitivas serán números primos a p — 1 y a la vez menores que el. Pero la suma de estos numeros, i.e., el índice del producto de todas las raíces primitivas, es ξ 0 (mod. p — 1), de donde el producto ξ 1 (mod. p). En efecto se percibe facilmente que si k es un numero primo a p — 1, tambien p — 1 — k sera primo a p — 1, y por lo tanto la suma de los numeros primos a p — 1 se compone de pares cuya suma es divisible por p — 1 (aunque k nunca puede ser igual a p — 1 — k excepto en el caso p — 1 = 2, o sea p = 3, el cual excluimos; pues es claro, en todos los casos restantes que Pp no es primo a p — 1).

81.

La suma de todas las raóces primitivas es o bien ξ 0 (cuando p — 1 es divisible por algun cuadrado), o bien ξ ±1 (mod. p) (cuando p — 1 es un producto de numeros primos diferentes; si el numero de ellos es par, se toma el signo positivo, pero si es impar, se toma el negativo.)

Ejemplo. 1o. Para p = 13, se tienen las raíces primitivas 2, 6, 7, 11, cuya suma 26 ξ 0 (mod. 13).

2o. Para p = 11, las raíces primitivas son 2, 6, 7, 8, cuya suma 23 ξ +1 (mod. 11).

3o. Para p = 31, las raíces primitivas son 3, 11, 12, 13, 17, 21, 22, 24 cuya suma 123 ξ —1 (mod. 31).

Demostración. Arriba hemos demostrado (art. 55, II), que si p — 1 es = aabC etc. (donde a, b, c, etc. designan numeros primos diferentes), y A, B, C, etc. son numeros cualesquiera pertenecientes a los exponentes aa, b, cY, etc., respectivamente, entonces todos los productos ABC etc. representarán raíces primitivas. Tambien puede demostrarse fácilmente que cualquier raíz primitiva puede representarse por tal tipo de producto, y de hecho de manera ánica[[109]](#footnote-110)).

De esto sigue que estos productos pueden tomarse en lugar de las raíces primitivas mismas. Pero, puesto que en estos productos conviene combinar todos los valores de A con todos los de B, etc., la suma de todos estos productos es un producto de la suma de todos los valores de A, multiplicada por la suma de todos los valores de B, multiplicada por la suma de todos los valores de C, etc., como es conocido de la teoría de combinaciones. Denótense todos los valores de A; B etc., por A, A', A”, etc.; B, B', B”, etc. etc., entonces la suma de todas las raíces primitivas sera:

= (A + A' + etc.)(B + B' + etc.) etc.

Ahora digo que si el exponente α es = 1, la suma A + A' + A” + etc. sera = — 1 (mod. p), pero si α es > 1, esta suma sera = 0, y de manera similar para los restantes β, γ, etc. Tan pronto como esto sea demostrado, la verdad de nuestro teorema sera manifiesta. De hecho, cuando p — 1 es divisible por algán cuadrado, alguno de los exponentes α, β, γ, etc. superara a la unidad, de donde alguno de los factores cuyo producto es congruente a la suma de todas las raíces primitivas sera = 0, y por eso tambien lo serí el producto mismo. Pero cuando p — 1 no puede dividirse por ningun cuadrado, todos los exponentes α, β, γ, etc. serán = 1, de donde la suma de todas las raíces primitivas serí congruente al producto de tantos factores, cada uno de los cuales es = —1, como cantidad de nímeros a, b, c, etc. se tenga. Por eso la suma sera = ±1, segín que el nímero de estos sea par o impar. Ello se demuestra como sigue.

1o. Cuando α = 1 y A es un numero perteneciente al exponente a, los restantes nímeros que pertenecen a este exponente serán A2, A3, . ..Aa-1. Pero

1. + A + A2 + A3 + ... + Aa-1

es la suma de un período completo, de donde = 0 (art. 79), por lo cual

A + A2 + A3 + ... + Aa-1 = —1

2o. Sin embargo, cuando α > 1 y A es un nUmero perteneciente al exponente aa, se tendrán los restantes números que pertenecen a este exponente, si de A2, A3, A4, ...AA -1 se suprimen Aa, A2a, A3a, etc., (vease art. 53). Entonces la suma de ellos seráa

= 1 + A + A2 + ... + Aa“-1 — (1 + A + A2a + ... + Aa“-a)

1. e., congruente a la diferencia de dos períodos, y por eso = 0. Q. E. D.

***Sobre los módulos que son potencias de numeros primos.***

82.

Todo lo que hasta ahora hemos expuesto se ha basado en la suposición de que el modulo es un número primo. Nos queda considerar el caso donde se toma un número compuesto como modulo. Pero como aquí ni se presentan propiedades tan elegantes como en el caso anterior, ni es necesario buscar artificios sutiles para estas, sino más bien casi todo puede extraerse por medio de una aplicacion de los principios anteriores, sería superfluo y tedioso discutir todos los detalles aquí. Así que expondremos brevemente cuales casos son comunes al caso anterior y cuales son propios.

83.

Las proposiciones de los artículos 45-48 ya fueron demostradas en general. Pero la proposicion del art. 49 tiene que cambiarse como sigue:

***Si f denota cuantos números son primos a m y, a la vez, menores que m, i.e., si f*** = ***ipm (art. 38), entonces el exponente t de la potencia menor de un numero dado a primo a m que es congruente a la unidad según el modulo m, será*** = f***, o bien un factor de este número.***

La demostracion de la proposicion del artículo 49 tambien puede valer para este caso, si se sustituyen p por m, p — 1 por f, y los numeros 1, 2, 3, ...p — 1, por los numeros a la vez menores que y primos a m. Dejamos esta tarea al lector.

Además las restantes demostraciones de las cuales hemos hablado allí (art. 50, 51) no pueden aplicarse a este caso sin mucha ambigüedad. Con respecto a las proposiciones de los artículos 52 y siguientes, nace una gran diferencia entre los modulos que son potencias de números primos y los que pueden dividirse por muchos números primos. Por lo tanto, consideraremos los modulos del genero anterior por separado.

84.

Si el múdulo m = pn, donde p es un número primo, serú f = pn-1(p — 1) (art. 38). Ahora, si a este caso se aplican las investigaciones contenidas en los artículos 53 y 54, hechos los cambios necesarios como prescribimos en el artículo anterior, se descubrirá que todo lo que se demostró allí valdrá tambien en este caso, si se demostrara antes que una congruencia de la forma xt — 1 ξ 0 (mod. pn) no puede tener mas que t raíces diferentes. Para un múdulo primo dedujimos esta verdad de las proposiciones múas generales del art. 43, las cuales valen en su mayor generalidad solamente para múodulos que son nuúmeros primos, y por eso no debe aplicarse a este caso. No obstante demostraremos utilizando un metodo especial, que esta proposiciún es verdadera en este caso particular. Luego (seccion VIII) aprenderemos a encontrarla múas fúacilmente.

85.

Nos proponemos demostrar este teorema:

***Si e es el máximo común divisor de los números*** t ***y*** pn-1(p — 1), ***la congruencia xX*** ξ 1 (mod. pn) ***tendrá e raíces diferentes.***

Sea e = kpv tal que k no involucre el factor p, de modo que divida al número p — 1. Entonces la congruencia xX ξ 1, segun el modulo p, tendrá k raíces diferentes denotadas A, B, C, etc., y cualquier raíz de la misma congruencia según el múdulo pn, debe ser congruente, según el módulo p, a alguno de los numeros A, B, C, etc. Ahora demostraremos que la congruencia xX ξ 1 (mod. pn) tiene pv raíces congruentes a A, otras tantas a B etc., todas según el múdulo p. Por esto, el numero de todas las raíces serú kpv o sea e, como hemos dicho. Para llevar a cabo esta demostrackm,demostraremos primero, que si α es una raíz congruente a A segun el modulo p, tambien

α + pn-v, α + 2pn-v, α + 3pn-v, ...α + (pv — 1)pn-v

serán raíces; segundo, que los números congruentes a A según el modulo p diferentes de los que esten comprendidos en la forma a + hpn~v (donde h denota cualquier entero) no pueden ser raíces. De donde es claro que se tendrún pv raíces diferentes, y no mas: lo mismo tendrú que valer tambien para las raíces que son congruentes a cada uno de los números B, C, etc. Tercero, mostraremos como se puede siempre encontrar una raíz congruente a A según p.

86.

TEOREMA. Si, como en el articulo anterior, t es un número divisible por pu pero no por pu+1, tendremos:

(a + hpA)t — at ξ 0 (mod. ρμ+ν), y ξ cO 1 hpAt (mod. ρμ+ν+1)

La última parte del teorema no tiene lugar cuando p = 2 y a la vez μ = 1.

La demostraciún de este teorema puede hacerse mediante el desarrollo de la potencia de un binomio, si se muestra que todos los terminos despues del segundo son divisibles por pA+v+1. Sin embargo, puesto que la consideración de los denominadores de los coeficientes resulta un poco ambigua, preferimos el siguiente metodo.

Si suponemos primero μ > 1 y ν = 1, puesto que

y)(xt 1 + xt 2y + xt 3y2 + etc. + yt 1)

*xt — yf* = (x *-* (o + *hpú)t — oO*

se tendrá Pero

= hpA((a + hp^)t-1 + (a + hp^)t-2a + etc. + at-1) a + hpμ ξ a (mod. p2)

por lo que cada termino (a+hp^)t-1, (a+hp^)t-2a, etc. serú ξ at-1 (mod. p2), y por tanto la suma de todos serú ξ tat-1 (mod. p2) o sea, serú de la forma tat-1 + Vp2, donde V denota un número cualquiera. Por eso, (a + hp^)t — at serú de la forma

at-1hpAt + Vhp^+2, i.e., ξ at-1hp^t (mod. p^+2) y ξ 0 (mod. p^+1)

Por lo tanto el teorema estú demostrado para este caso.

Ahora, si el teorema no fuera vúlido para otros valores de ν, manteniendo todavía μ > 1, necesariamente se presentara algún lúmite abajo del cual el teorema sea valido, pero mús alla falso. Sea φ el menor valor de ν para el cual es falso, de donde se ve facilmente , que si t es divisible por p^-1 pero no divisible por p^, el

teorema será verdadero hasta aquí, pero falso si se sustituye t por tp. Por lo tanto tenemos

(a + hp^)t = cC + at-1hp^t (mod. ρμ+φ) osea = cC + at-1hp^t + upf'+tf

donde u denota algún número entero. Pero ya que el teorema esta demostrado para ν = 1, se tendrá:

(ct + at-1hp^t + up/^+Vf = ctp + atp-1hpf1+11 + atp-tup^+1 (mod. p^+^+1) y por lo tanto tambien

(a + hpf)tp = atp + atp-1 hpf'tp (mod. ρμ+ν+1)

i.e., el teorema tambien es vúlido si se sustituye t por tp, i.e., tambien para ν = φ contra la hipótesis. De donde es claro que el teorema sera valido para todos los valores de ν.

87.

Falta el caso donde μ = 1. Por medio de un metodo enteramente similar al que hemos aplicado en el artúculo anterior, puede demostrarse sin usar el teorema binomial que

(a + hp)t-1 = at-1 + at-2(t — 1)hp (mod. p2) a(a + hp)t-2 = at-1 + at-2(t — 2)hp a2 (a + hp)t-3 = at-1 + at-2(t — 3) hp etc.

de donde su suma (puesto que el número de terminos = t) sera

= tat-1 +

~ +~t 11 (t -1)tat 2hp (mod. p2)

Sin embargo, puesto que t es divisible por p, tambien (t 21)t serú divisible por p en todos los casos, excepto en aquel donde p = 2, sobre el cual ya hemos informado

en

el artúculo anterior. Pero,

en

los casos restantes serú

(t-1)rát-2^ =

a

hp = 0 (mod. p2),

y por tanto también la suma ξ tαt-1 (mod. p2) como en el artículo anterior. El resto de la demostración procede aquí del mismo modo.

Por lo tanto, concluimos en general, excepto en el único caso p = 2, que

(α + Ηρμ)ί ξ αt (mod. ρμ+ν)

y (α + hp^)t no ξ at para cualquier modulo que sea una potencia de p mayor que p^+v, siempre que h no sea divisible por p, y que pv sea la potencia mayor de p que divide al número t.

De aquí, se derivan directamente las proposiciones 1 y 2, que nos habíamos propuesto demostrar: a saber,

primero, si at ξ 1, serú tambien (α + hpn-v)t ξ 1 (mod. pn);

segundo, si algun número α0 es congruente, según el múdulo p, a A, y luego tambien a α, pero no congruente a α segun el múdulo pn-v, y si satisface la congruencia xt ξ 1 (mod. pn). Suponemos α0 es = α + lp^ de modo que l no es divisible por p, entonces sera λ < n — ν, pero entonces (α + lp^)t sera congruente a αt según el modulo p^+v, pero no segun el módulo pn que es una potencia mayor, por lo que α0 no es una raúz de la congruencia xt ξ 1.

88.

Tercero, se debe buscar alguna raúz de la congruencia xt ξ 1 (mod. pn) que sea congruente a A. Mostraremos aquú solamente cúmo puede hacerse esto si ya se conoce una raúz de esta misma congruencia según el modulo pn-1. Es claro que esto es suficiente, ya que podemos ir del múdulo p para el cual A es una raúz, al múdulo p2 y de este a todas las potencias siguientes.

Asú, sea α una raúz de la congruencia xt ξ 1 (mod. pn-1), búsquese una raúz de la misma congruencia, segun el modulo pn. Pongase esta = α + hpn-v-1, la cual debe tener esta forma segun el artículo anterior (consideraremos por separado el caso donde ν = n — 1 pues ν no puede ser mayor que n — 1). Por lo tanto, tendremos

(α + hpn-v-1)t ξ 1 (mod. pn-1)

Pero (α + hpn-v-1)t ξ αt + α^^^-1 (mod. pn)

Así, por consiguiente, si h se determina de modo que 1 ξ αt + αt-1htpn-ν-1 (mod. pn); o sea (puesto que por hipotesis 1 ξ αt (mod. pn-1) y t es divisible por

pv) Qn-i + cX~1hJ- es divisible por p, tendremos la raíz buscada. Que esto se puede hacer es claro a partir de la sección anterior, puesto que hemos supuesto que aquí t no puede dividirse por una potencia de p mayor que pv, por lo tanto oX-1J- es primo a p .

Pero si ν = n — 1, i.e., t es divisible por pn-1 o sea tambien por una potencia mayor de p, cualquier valor de A que satisface a la congruencia xt = 1 segun el modulo p, tambien satisfará a la misma segón el módulo pn. Pues si t = pn-1r, sera t = r (mod. p — 1): de donde, puesto que Aa = 1 (mod. p), seró tambien AT = 1 (mod. p). Ahora sea AT = 1 + hp, tendremos At = (1 + hp)p = 1 (mod. pn)

(art. 87).

89.

Todo lo derivado en el artículo 57 y siguientes con la ayuda del teorema que establece que la congruencia xX = 1 no puede tener mós que t raíces diferentes, tambien vale para un módulo que es una potencia de un nómero primo. Si se les llama raíces primitivas a los números que pertenecen al exponente pn-1(p — 1), es decir, en cuyos períodos aparecen todos los nómeros no divisibles por p, entonces aquó tambien habrá raóces primitivas. Todo lo que antes presentamos sobre los óndices y su aplicación a la resolución de la congruencia xX = 1, tambien puede aplicarse a este caso. Puesto que esto no ha presentado ninguna dificultad, sería superfluo repetir todo aquí. Ademas hemos mostrado como las raíces de la congruencia xX = 1, segun el modulo pn, pueden derivarse de las raíces de la misma congruencia segun el modulo p. Pero todavía hay que agregar algo al caso donde una potencia del numero 2 es modulo, puesto que fue excluido anteriormente.

***Módulos que son potencias de 2.***

90.

***Si se toma alguna potencia del número 2, mayor que la segunda, como módulo, por ejemplo*** *2****n, la potencia*** 2n-2 ***de cualquier numero impar es congruente a la unidad.***

Por ejemplo 38 = 6561 = 1 (mod. 32).

De hecho, cualquier numero impar o esta comprendido en la forma 1 + 4h o bien en — 1 + 4h: de donde la proposición sigue directamente (teorema art. 86).

Puesto que el exponente al cual pertenece cualquier número impar, según el modulo 2n, debe ser divisor de 2n-2, pertenecerá a alguno de los números 1, 2, 4, 8, ... 2n-2, entonces es facil juzgar a cual de ellos pertenece. Si el número propuesto = 4h ± 1, y la mayor potencia de 2 que divide a h es = m (que tambien puede ser = 0, cuando h es impar); entonces el exponente al cual pertenece el número propuesto sera = 2n-m-2 si n > m + 2. Pero, si n = 0 o < m + 2, el número propuesto es = ±1 y pertenecerá o al exponente 1 o al exponente 2. Es claro que un número de la forma ±1 + (2m+2k) (l a cual equivale a 4h ± 1) elevado a la potencia 2n m 2, sera congruente a la unidad según el módulo 2n, pero incongruente si es elevado a una potencia inferior del numero 2, como se deduce del art. 86 con facilidad. Por lo tanto, cualquier numero de la forma 8k + 3 o 8k + 5 pertenecerá al exponente 2n -2.

91.

Se sigue de aquí que no se presentan raíces primitivas en el sentido aceptado antes por nosotros para esta expresiún. Esto es, no hay números cuyos períodos comprenden todos los números menores que el modulo y primos a el. Sin embargo, se percibe facilmente que aquí existe una analogía. De hecho, se encuentra que una potencia impar de un numero de la forma 8k + 3 siempre tiene la forma 8k + 3; mientras que una potencia par siempre es de la forma 8k + 1. Por tanto, ninguna potencia puede ser de la forma 8k + 5 u 8k + 7. Puesto que el período de un numero de la forma 8k + 3 consta de 2n -2 terminos diferentes, cada uno de los cuales es o de la forma 8k + 3 o de la forma 8k +1, y como no se dan mús que 2n-2 numeros menores que el modulo, evidentemente cada numero de la forma 8k +1u8k + 3 es congruente, segun el modulo 2n, a alguna potencia de un numero cualquiera de la forma 8k + 3. De modo similar puede demostrarse que el período de un numero de la forma 8k + 5 consta de todos los numeros de la forma 8k + 1 y 8k + 5. Si, por lo tanto, se toma como base un numero de la forma 8k + 5, se obtendrán índices reales de todos los números de la forma 8k +1 y 8k + 5 tomados positivamente y de todos los de la forma 8k + 3 y 8k + 7 tomados negativamente. Aquí se consideran equivalentes dos índices congruentes segun 2n-2. De este modo, se debe interpretar nuestra Tabla I donde siempre tomamos el numero 5 como base para los modulos 16, 32 y 64 (puesto que para el modulo 8 ninguna tabla es necesaria). Por ejemplo, al numero 19, que es de la forma 8n + 3, y por lo tanto esta tomado negativamente, le corresponde el índice 7 para el modulo 64, esto es 5 7 = —19 (mod. 64). Pero al tomar numeros de las formas 8n +1, 8n+5 negativamente, y los números de las formas 8n+3, 8n+7 positivamente,

ciertos Indices tendrán que considerarse imaginarios. Con la introducción de esto, el cálculo de índices puede reducirse a un algoritmo bastante simple. Pero, puesto que, si deseamos exponer esto con todo rigor, nos llevará mucho tiempo, reservamos este trabajo para otra ocasion cuando quizas intentemos profundizar la teoría de las cantidades imaginarias, la cual, a nuestro juicio, nadie ha reducido a nociones claras. Los expertos pueden encontrar este algoritmo con facilidad; los menos habiles, sin embargo, pueden usar esta tabla si han comprendido los principios presentados arriba, de la misma manera como quienes no saben nada sobre las investigaciones modernas sobre logaritmos imaginarios aán usan logaritmos.

Módulos compuestos de varios primos.

92.

Segán un modulo compuesto de varios primos, casi todo lo que pertenece a los residuos de las potencias puede deducirse de la teoría general de las congruencias. Pero, puesto que despues enseñaremos en detalle a reducir cualquier congruencia, segun un modulo compuesto de varios primos, a congruencias, de las cuales el modulo es o primo o una potencia de un primo, no nos detendremos mías en esto. Solamente observamos que la bellísima propiedad que vale para los otros modulos, a saber que siempre existen numeros cuyo período comprende todos los námeros primos al modulo, aquí no vale, excepto en un ánico caso, cuando el modulo es el doble de un nímero primo, o de una potencia de un nímero primo. De hecho si el modulo m se reduce a la forma AaBbCc etc., donde A, B, C, etc. denotan numeros primos diferentes, y si ademís se denota Aa-1(A — 1) por a, Bb-1(B — 1) por β, etc., y luego z es un nímero primo a m; sera za = 1 (mod. Aa), ζβ = 1 (mod. Bb), etc. Por tanto, si μ es el mínimo comín míltiplo de los nímeros α, β, γ, etc., sera ζμ = 1 segun todos los mídulos Aa, Bb, etc., de donde tambien segun m, que es igual al producto de aquellos. Pero, excepto el caso donde m es el doble de un nímero primo o de una potencia de un numero primo, el mínimo comín míltiplo de los nímeros α, β, γ, etc. es menor que su producto (puesto que los nímeros a, β, γ, etc. no pueden ser primos entre sí, sino que tienen el divisor comín 2). Por tanto, ningín período puede comprender tantos terminos como nímeros menores y primos al modulo, puesto que el numero de estos es igual al producto de α, β, γ, etc. Así, por ejemplo, para m = 1001 la potencia 60 de cualquier nímero primo a m es congruente a la unidad, pues 60 es el mínimo común multiplo de 6, 10 y 12. El caso donde el modulo es el doble de un nímero primo, o el doble de una potencia de un primo es totalmente

análogo al caso donde es primo o una potencia de un primo.

93.

Ya se ha hecho mención de los escritos donde otros geometras han hablado del argumento tratado en esta sección. Para los que desean otros detalles mas amplios, mencionamos en particular los siguientes comentarios del ilustre Euler que, por su perspicacia distinguen a este hombre de los demóas.

***Theoremata circa residua ex divisione potestatum relicta,*** Comm. nov. Petr., VII p. 49 y siguientes.

***Demostrationes circa residua ex divisione potestatum per numeros primos resultantia, ibid.,*** XVIII p. 85 y siguientes.

Tambien puede agregarse Opusculorum analyt. 1, disertaciones 5 y 8.

Sección Cuarta

SOBRE

LAS CONGRUENCIAS DE SEGUNDO GRADO

***Residuos y no residuos cuadráticos.***

94.

TEOREMA. ***Al tomar un numero cualquiera m como módulo, de los nUmeros*** 0, 1, 2, 3 , ...m — 1, ***mas de 2***m +1 ***no pueden ser congruentes a un cuadrado si m es par, ni mas de*** 2***m +*** *2* ***pueden serlo cuando m es impar.***

Demostracion. Puesto que los cuadrados de números congruentes son congruentes, cualquier número que pueda ser congruente a algún cuadrado, tambien sera congruente a algún cuadrado cuya raíz sea < m. Por consiguiente, basta considerar los residuos mínimos de los cuadrados 0, 1, 4, 9 , ... (m — 1)2. Pero se nota facilmente que (m — 1)2 es ξ 1, (m — 2)2 ξ 22, (m — 3)2 ξ 32, etc. De aquí tambien, cuando m es par, los residuos mínimos de los cuadrados (^m — 1)2 y (^m + 1)2, (^m — 2)2 y (2m + 2)2, etc. serán los mismos: cuando m es impar, los cuadrados (^m — 2)2 y 2m + 2)2, (2m — 2)2 y (2m + 3)2, etc. serán congruentes. De donde es evidente que otros nuúmeros no pueden ser congruentes a un cuadrado, mas que aquúellos que sean congruentes a alguno de los cuadrados 0, 1, 4, 9 , ... (2m)2 cuando m es par; y cuando m es impar, cualquier nuúmero que sea congruente a alguún cuadrado necesariamente es congruente a alguno de los números 0, 1, 4, 9 , ... (2m — 2)2. Por lo tanto, en el primer caso se presentarán a lo sumo 2m + 1 residuos mínimos diferentes; en el segundo caso a lo sumo 2m + 2. Q. E. D.

Ejemplo. Según el modulo 13, los números 0, 1, 4, 9, 3, 12, 10 se encuentran como los residuos mínimos de los cuadrados de 0, 1, 2, 3, ...6; despues de esto

aparecen en el orden inverso 10, 12, 3 etc. Por lo tanto, si algún número no es congruente a ninguno de estos residuos mínimos, o sea, no es congruente a ninguno de 2, 5, 6, 7, 8, 11, entonces no puede ser congruente a ningún cuadrado.

Según el modulo 15 se encuentran los residuos 0, 1, 4, 9, 1, 10, 6, 4; despues de esto aparecen en el orden inverso. Aquí, por lo tanto, el numero de residuos que pueden ser congruentes a un cuadrado es menor que 2m + 2, puesto que son 0, 1, 4, 6, 9, 10. Pero los números 2, 3, 5, 7, 8, 11, 12, 13, 14, y los que son congruentes a alguno de estos, no pueden ser congruentes a ningun cuadrado según el modulo 15.

95.

De esto resulta que para cualquier modulo, todos los números pueden separarse en dos clases, una de las cuales contiene los nuúmeros que pueden ser congruentes a algun cuadrado, la otra contiene los que no pueden serlo. Llamaremos a los primeros residuos cuadráticos del número que tomamos como modulo[[110]](#footnote-111)), y los segundos no residuos cuadráticos, o tambien, cuando no se origina ambigüedad alguna simplemente residuos y no residuos. Es claro que basta poner en clases a los números 0, 1, 2, ...m — 1, puesto que todos los números congruentes deberán pertenecer a una misma clase.

Iniciaremos esta investigaciún con los múdulos primos, lo cual deberá por consiguiente entenderse aunque no se exprese verbalmente. Hay que excluir el número primo 2: se consideraran solamente los números primos impares.

***Cuando el mádulo es un námero primo, el numero  
de residuos menores que el mádulo es igual al námero de no residuos menores.***

96.

***Al tomar un námero primo p como modulo, la mitad de los numeros*** 1, 2, 3, ...p — 1 ***serán residuos cuadráticos, los restantes seran no residuos, i.e., se presentaran*** 2 (p — 1) ***residuos y otros tantos no residuos.***

De hecho, se demuestra fácilmente que todos los cuadrados 1, 4, 9, ... 4 (p — 1)2 son incongruentes. En efecto, si pudiera ser r2 ξ (r0)2 (mod. p) y los números r, r0 distintos y no mayores que ^(p — 1), poniendo r > r0, resultaría (r — r0)(r + r0) positivo y divisible por p. Pero cada factor r — r0 y r + r0 es menor que p, por tanto la suposición no puede valer (art. 13). Así, se tienen 2(p — 1) residuos cuadraticos contenidos entre los números 1, 2, 3 , ...p — 1; de hecho, no puede haber mús de ellos puesto que al agregar el residuo 0, se producen 2(p + 1) de ellos, y este número no puede exceder el número de todos los residuos. Por consiguiente, los restantes números serún no residuos y el numero de ellos = 2 (p — 1).

Puesto que cero siempre es un residuo, lo excluimos de nuestras investiga­ciones, lo mismo que a los numeros divisibles por el módulo. Puesto que este caso es claro por sú mismo, unicamente dificultaría la simetría del teorema. Por las mismas razones tambien hemos excluido el modulo 2.

97.

Puesto que mucho de lo que expondremos en esta seccion tambien podrú derivarse de los principios de las secciones anteriores, y como no es inuútil estudiar a fondo la misma verdad por medio de múetodos diferentes, explicaremos esta relaciúon. Se comprende fúcilmente que todos los números congruentes a un cuadrado tienen úndices pares; mientras que los que no pueden de ningun modo ser congruentes a un cuadrado, los tienen impares. Puesto que p — 1 es un número par, tantos indices serún pares como impares, a saber 2(p — 1), y entonces se presentaran tantos residuos como no residuos.

Ejemplo. Para el modulo los residuos son

3 1.

5 1, 4.

7 1, 2,4.

1. 1, 3, 4, 5, 9.

13 1, 3, 4, 9, 10, 12.

17 1, 2, 4, 8, 9, 13, 15, 16

etc.

y el resto de los numeros menores que el modulo son no residuos.

***La cuestión de si un número compuesto es un residuo o un no residuo  
de un número primo dado depende de la naturaleza de los factores.***

98.

TEOREMA. ***El producto de dos residuos cuadraticos de un numero primo p es un residuo; el producto de un residuo con un no residuo es un no residuo; finalmente, el producto de dos no residuos es un residuo.***

Demostracion. I. Sean A y B los residuos resultantes de los cuadrados a? y b2 o sea A ξ a2,B ξ b2. El producto AB sera congruente al cuadrado del numero ab, i.e., es un residuo.

1. Cuando A es un residuo, por ejemplo ξ a2, pero B es un no residuo,

AB será un no residuo. Si fuera un residuo, póngase AB ξ k2, y sea el valor de la expresión a (mod. p) ξ b; así tendríamos a2B ξ a2b2, de donde B ξ b2, i.e., B es

un residuo, contrariamente a la hipótesis.

Otra demostraciún. Entre los numeros 1, 2, 3 , ...p — 1 (el námero de ellos = 2(p — 1)), multipláquense por A todos los que sean residuos. Todos los productos serán residuos cuadraticos, y ciertamente todos serán incongruentes. Ahora, si se multiplica el no residuo B por A, el producto no será congruente a ninguno de los productos que ya se tienen; por lo tanto si fuera un residuo, se tendrían ^ (p + 1) residuos incongruentes, entre los cuales todavía no está el residuo 0, contrariamente al art. 96.

1. Sean A y B no residuos. Entre los námeros 1, 2, 3 , ...p — 1, multipláquense por A todos los que sean residuos. Se tendrán ^ (p — 1) no residuos incongruentes entre sí (II); ahora el producto AB no puede ser congruente a ninguno de ellos. Entonces, si fuera un no residuo, se tendrían ^(p + 1) no residuos incongruentes entre sí, contra el art. 96. Por lo tanto el producto etc. Q. E. D.

Estos teoremas pueden ser derivados mís facilmente de los principios de la seccion anterior. De hecho, puesto que los índices de los residuos siempre son pares, y los índices de los no residuos impares, el índice del producto de dos residuos o de dos no residuos sería par, de donde el producto mismo sería un residuo. Por el contrario, el índice del producto de un residuo y un no residuo sera impar y, por lo tanto, el producto mismo un no residuo.

Cualquier metodo de demostraciín tambien puede aplicarse para estos teoremas: ***el valor de la expresiún*** | (mod. p) ***serú un residuo cuando los números*** a ***y*** b ***sean a la vez residuos o a la vez no residuos; al contrario, serú un no residuo cuando uno de los números*** a ***o*** b ***sea un residuo y el otro un no residuo.*** Tambien pueden obtenerse al aplicar los teoremas precedentes.

99.

En general, el producto de factores cualesquiera es un residuo ya sea cuando todos los factores son residuos o cuando todos son no residuos y el número de ellos es par. Pero cuando el numero de los no residuos que quedan entre los factores es impar, el producto sera un no residuo. Así puede decidirse facilmente si un número compuesto es residuo o no, si de algún modo se conoce cada uno de sus factores. Por lo tanto, hemos incluido solamente los números primos en la tabla II. Esta es la organización de la tabla. En la orilla se han colocado los modulos[[111]](#footnote-112)), con los números primos consecutivos arriba. Cuando uno de estos es un residuo de algún modulo, se coloca un guioún en el espacio correspondiente a los dos, pero cuando el nuúmero primo es un no residuo del modulo, el espacio correspondiente queda en blanco.

***Sobre los módulos que son numeros compuestos.***

100.

Antes de proceder a temas mús difíciles, debemos agregar algo acerca de los modulos no primos.

Si se toma como módulo alguna potencia pn del número primo p (donde suponemos que p no es 2) la mitad de todos los números no divisibles por p y menores que el modulo serán residuos, la otra mitad serú no residuos, i.e., el numero de cada uno = 2 (p — 1)pn-1.

De hecho, si r es un residuo, sera congruente a algun cuadrado cuya raíz no supera la mitad del múdulo, vease art. 94. Ahora se nota fúcilmente que se presentan 2 (p — 1)pn-1 números menores que la mitad del modulo y no divisibles por p. Así, falta demostrar que los cuadrados de todos estos nuúmeros son incongruentes, o sea producen residuos cuadrúticos diferentes. Si los cuadrados de dos números a y b no divisibles por p y menores que la mitad del modulo fueran congruentes, tendríamos aa — b2 o sea (a — b)(a + b) divisible por pn (suponemos que a > b). Pero esto no

puede suceder a menos que, o bien uno de los números a — b,a + b sea divisible por pn, lo que no puede ser, puesto que los dos son < pn; o bien uno por pm y el otro por pn-m, i.e., ambos por p. Pero esto tampoco puede suceder. En efecto, es claro que la suma y diferencia de 2a y 2b tambien serían divisibles por p, de donde tambien a y b, contrariamente a la hipútesis.— De esto se sigue, finalmente, que entre los números no divisibles por p y menores que el modulo se presentan ^ (p — 1)pn residuos;

los restantes, que son la misma cantidad, son no residuos. Q.E.D.— Este teorema también puede derivarse de las consideraciones de los índices tal como en el art. 97.

101.

***Cualquier número no divisible por p, que es un residuo de p, también será un residuo de pn; pero si es un no residuo de p, también seré un no residuo de pn.***

La ultima parte de esta proposición es muy clara. Si la primera parte fuera falsa, entre los numeros menores que pn y a la vez no divisibles por p, habría mas residuos de p que de pn, i.e., mas de 2pn-1(p — 1). Pero, puede verse con facilidad que el numero de residuos del numero p entre esos numeros es precisamente = 1 pn-1(p — 1).

Es igualmente facil encontrar explícitamente un cuadrado congruente, segun el modulo pn, a un residuo dado, si se tiene el cuadrado congruente a este residuo segun el modulo p.

En efecto, si se tiene un cuadrado a? que es congruente al residuo dado A segun el modulo pú, se puede encontrar un cuadrado congruente a A segun el modulo pv (donde se supone ν > μ e = o < 2μ) de la siguiente manera. Pongase la raíz del cuadrado deseado = ±a + xpú. Se ve facilmente que debe tener esta forma, y debe ser a2 = ±2axpú + x2p2ú ξ A (mod. pv), o sea, puesto que 2μ > ν, A — a2 ξ ±2axpú (mod. pv). Si A — a2 = púd, x sera un valor de la expresion ±2a (mod. pv-ú), que es equivalente a ±(mod. pv).

Por lo tanto, dado un cuadrado congruente a A segun el modulo p, se deduce de allí un cuadrado congruente a A segun el modulo p2; de aquí podemos ascender a p4, de allí a p8 etc.

Ejemplo. Propuesto el residuo 6 que es congruente al cuadrado 1 segun el modulo 5, encontramos que es congruente al cuadrado 92 segun 25, congruente a 162 segun 125, etc. [[112]](#footnote-113)

1. Cuando k = o > n, tendremos pkA = 0 (mod. pn), i.e., un residuo.
2. Cuando k < n e impar, pkA sera un no residuo.

De hecho, si tuvieramos pkA = p2x+1 A = s2 (mod. pn), s2 serla divisible por ρ2χ+1 y este únicamente podría ser el caso si s fuera divisible por px+1. Entonces, tambien s2 sera divisible por ρ2χ+2 y asl tambien (puesto que en realidad 2χ + 2 no es mayor que n) pkA i.e., p2x+1A; o sea, A es divisible por p, contrariamente a la hipotesis.

1. Cuando k < n y par. Entonces pkA sera un residuo o un no residuo de pn, segun que A sea un residuo o un no residuo de p. De hecho, cuando A es un residuo de p, sera tambien un residuo de pn-k. Suponiendo que A = a2 (mod. pn-k), obtendremos que Apk = a2pk (mod. pn) y que a2pk es un cuadrado. Pero, cuando A es un no residuo de p, pkA no puede ser un residuo de pn. De hecho, si pkA = a2 (mod. pn), necesariamente a2 sera divisible por pk. El cociente sera un cuadrado congruente a A segun el modulo pn-k, de donde tambien segun el modulo p, contrariamente a la hipotesis. [[113]](#footnote-114) y el número propuesto será también = α2. Pero entonces es claro que tanto a como α serán impares y α < 2n-2.
2. Los cuadrados de todos los námeros impares menores que 2n-2 serán incongruentes segán 2n. De hecho, si r y s son dos números tales, cuyos cuadrados fueran congruentes segán 2n, (r — s)(r + s) sería divisible por 2n (suponiendo que r > s). Pero se ve fácilmente que los námeros r — s y r + s, no pueden ser divisibles a la vez por 4; por lo tanto si uno es divisible solo por 2, el otro deberá ser divisible por 2n-1 para que el producto sea divisible por 2n. Q.E.A., puesto que cada uno es < 2n-2.
3. Si finalmente se reducen estos cuadrados a sus residuos mínimos positivos, se obtendrán 2n-3 residuos cuadráticos diferentes menores que el mádulo[[114]](#footnote-115)) y cada uno sera de la forma 8k + 1. Sin embargo, como existen precisamente 2n-3 námeros de la forma 8k +1 menores que el modulo, todos estos números deben ser residuos.

***Q. E. D.***

Para encontrar un cuadrado congruente a un námero dado de la forma 8k +1 segun el modulo 2n, puede emplearse un metodo como en el art. 101; vease tambien art. 88. — Finalmente, lo mismo que hemos expuesto en general en el art. 102 vale para los nuámeros pares.

104.

Si A es un residuo de pn, se deriva con facilidad de lo anterior lo siguiente acerca del námero de valores diferentes (i.e., de los incongruentes segán el modulo) que admiten una expresión como V = y/A (mod. pn). (Suponemos, como antes, que el námero p es primo y, por brevedad, incluimos aquí el caso n = 1).

1. Si A no es divisible por p, V tiene un valor único para p = 2, n = 1, a saber V = 1; dos valores cuando p es impar, o cuando p = 2, n = 2, a saber, al poner uno de ellos = v, el otro sera = — v; cuatro valores para p = 2, n > 2, en efecto, al poner uno de ellos = v, los restantes serán = —v, 2n-1 + v, 2n-1 — v.
2. Si A es divisible por p, pero no por pn, sea p2^ la potencia más alta de p que divide a A, (de hecho, es claro que este exponente deberá ser par) y tendremos A = ap2^. Entonces, es claro que todos los valores de V serán divisibles por p^, y los cocientes que resultan de la divisián serán valores de la expresián V0 = yfa (mod. pn-2^); de donde producirán todos los valores diferentes de V, al multiplicar

todos los valores de la expresión V' situados entre 0 y ρη μ por ρμ. Por lo tanto se representarán por

νρμ, νρμ + ρη-μ, νρμ + 2ρη-μ, ... νρΡ + (ρμ — 1)ρη-μ

donde el valor indeterminado v representa todos los valores diferentes de la expresion V', de modo que el numero de ellos será ρμ, 2ρμ, o 4ρμ, según que el número de valores de V' (por el caso I) sea 1, 2 o 4.

1. Si A es divisible por ρη, se ve fácilmente, al colocar n = 2m á = 2m — 1, segun sea par o impar, que todos los números divisibles por ρm son valores de V y no hay otros. Por consiguiente todos los valores diferentes serán 0, ρ™, 2ρ™, ... (ρη-™ — 1)ρ™ y el numero de ellos es ρη-™.

105.

Falta el caso donde el modulo m esta compuesto de varios números primos. Sea m = abc. . . donde a, b, c, etc. denotan numeros primos diferentes o potencias de números primos diferentes. Es claro aquí que si n es un residuo de m, tambien sera n un residuo de cada uno de los números a, b, c, etc., de donde n ciertamente sera un no residuo de m, si es un no residuo de alguno de los números a, b, c, etc. Y vice-versa: si n es un residuo de cada uno de a, b, c, etc., tambien serú un residuo del producto m. Pues, al suponer que n ξ A2, B2, C2, etc., mod. a, b, c, etc. respectivamente, es claro, si se deriva un numero N congruente a A, B, C, etc. según el modulo a, b, c, etc. respectivamente (art. 32), se tendrá n ξ N2 segun todos estos modulos y tambien según su producto m. Se nota facilmente como de una combinaciún de cualquier valor de A, es decir -^/ñ (mod. a), con cualquier valor de B, y con cualquier valor de C etc. resulta un valor de N, o de la expresion -^/n (mod. m). Ademas, diferentes combinaciones del producto dan diferentes valores de N y todas las combinaciones dan todos los valores de N. El numero de todos los diferentes valores de N serúa igual al producto de los nuúmeros de valores de A, B, C, etc. que enseñamos a determinar en el artículo anterior. — Ademas, es claro que si un valor de la expresion -^/n (mod. m) o de N es conocido, a la vez sera este un valor de A, B, C, etc. Puesto que seguún el artúculo anterior, pueden deducirse todos los restantes valores de estas cantidades, sigue faúcilmente que, de un valor de N, pueden obtenerse todos los restantes.

Ejemplo. Sea el modulo 315, del cual se desea saber si 46 es residuo o no residuo. Los divisores primos del numero 315 son 3, 5, y 7; y el número 46 es un residuo de cada uno y por tanto tambien residuo de 315. Ademas, puesto que 46 ξ 1, y ξ 64 (mod. 9); ξ 1 y ξ 16 (mod. 5); ξ 4 y ξ 25 (mod. 7), se encuentran las raíces de los cuadrados a los que 46 es congruente según el modulo 315, que son los números 19, 29, 44, 89, 226, 271, 289, 296.

***Criterio general sobre si un numero dado es un residuo de un numero primo dado.***

106.

De lo anterior se concluye: si solo se puede decidir si un numero primo dado es un residuo o un no residuo de un numero primo dado, todos los casos restantes pueden reducirse a esto. Por lo tanto debemos dirigir todos nuestros estudios a investigar criterios verdaderos para este caso. Antes de llevar a cabo esta investigaciún presentaremos un criterio derivado de la seccioún anterior, el cual en la prúactica casi nunca tiene utilidad, pero que por su simplicidad y generalidad debe mencionarse.

***Cualquier numero A no divisible por un numero primo*** *2****m*** +1 ***es un residuo o no residuo de este numero primo segun Am*** *ξ* +1 ***o*** *ξ—* 1 (mod. 2m + 1).

Sea pues a el índice del numero A para el modulo 2m + 1 en un sistema cualquiera; a sera par cuando A es un residuo de 2m + 1, e impar cuando es un no residuo. Pero, el índice del numero Am sera ma, i.e., ξ 0 o ξ m (mod. 2m) segun a sea par o impar. De aquí finalmente en el primer caso Am sera ξ +1, pero en el siguiente ξ—1 (mod. 2m + 1). Vease artículos 57 y 62.

Ejemplo. 3 es un residuo de 13 ya que 36 ξ 1 (mod. 13), pero 2 es un no residuo de 13, puesto que 26 ξ—1 (mod. 13).

Tan pronto como los numeros por examinarse sean moderadamente grandes, este criterio sera completamente inútil a causa de la inmensidad del cúlculo.

***Investigaciones sobre los números primos  
cuyos residuos o no residuos sean números dados.***

107.

Dado un módulo, es muy fácil caracterizar todos los numeros que son residuos o no residuos. Es claro: si se coloca este número = m, deben determinarse los cuadrados cuyas raíces no superan la mitad de m, o tambien números congruentes a

estos cuadrados según m (en la práctica se presentan métodos más fáciles). Entonces, todos los números congruentes a alguno de estos según m serán residuos de m, y todos los números no congruentes a ninguno de ellos serán no residuos. — Pero la situacián inversa, propuesto algún numero, asignar todos los números, de los cuales aquél sea un residuo o no residuo, es un obstáculo mucho mas grande. Este problema, de cuya solución depende lo que hemos propuesto en el artículo precedente, sera estudiado a fondo en lo siguiente, comenzando con los casos mas sencillos.

***Residuo*** —1.

108.

TEOREMA. —1 ***es un residuo cuadratico de todos los números primos de la forma*** 4n +1, ***pero es un no residuo de todos los números primos de la forma*** 4n + 3.

Ejemplo. —1 es un residuo de los números 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc. originado de los cuadrados de los números 2, 5, 4, 12, 6, 9, 23, 11, 27, 34,

1. etc. respectivamente; al contrario, es un no residuo de los números 3, 7, 11, 19,
2. 31, 43, 47, 59, 67, 71, 79, 83, etc.

Ya hemos mencionado este teorema en el artículo 64. La demostracion se obtiene facilmente del art. 106. Pues, para un numero primo de la forma 4n + 1 se tiene (—1)2n ξ 1, pero para un número de la forma 4n + 3 se tiene (—1)2n+l ξ—1. Esta demostracion concuerda con la del artículo mencionado. Sin embargo, por la elegancia y utilidad del teorema, mostraremos otra soluciún. [[115]](#footnote-116)

algunos residuos que son sus propios asociados, i.e., algunas clases que contienen un residuo único, o, si se quiere, contienen el mismo residuo dos veces, y si se pone el número de estas clases = a, y el numero de las restantes = b, entonces el número de todos los residuos C sera = a + 2b. De donde, cuando p es de la forma 4n +1, a sera un numero par. Cuando p es de la forma 4n + 3, a sera impar. Pero, no hay números menores que p, salvo 1 y p — 1, que puedan estar asociados consigo mismos (vease art. 77). En el primer caso, 1 estú entre los residuos; por lo tanto p — 1 (o —1 que vale lo mismo) debe ser un residuo, pero en el segundo caso, debe ser un no residuo. Pues, en un caso sera a = 1, y en el otro = 2, lo cual es imposible.

110.

Tambien esta demostraciún se debe al ilustre Euler, quien tambien encontró por primera vez el metodo anterior (vease Opuscula Analytica, T.1, p. 135). Con facilidad, se vera que ella esta basada en principios semejantes a los de nuestra segunda demostracion del teorema de Wilson (art. 77). Pero si suponemos este teorema, la demostracion podria simplificarse mucho. Es claro que entre los números 1, 2, 3 , ...p — 1 habrá residuos cuadráticos de p y otros tantos no residuos. Por lo que el numero de residuos sera par cuando p es de la forma 4n + 1; impar, cuando p es de la forma 4n + 3. De aquí concluimos que el producto de todos los números 1, 2, 3, , ...p — 1 sera un residuo en el primer caso, un no residuo en el otro caso (art. 99). Pero este producto siempre = — 1 (mod. p); de donde —1 es un residuo en el primer caso y en el segundo caso serú un no residuo.

111.

Así, si r es un residuo de algun número primo de la forma 4n +1, tambien —r sera un residuo de este primo; todos los no residuos de tal numero se mantendrán como no residuos, aunque se cambie el signo[[116]](#footnote-117)). Lo contrario vale para los números primos de la forma 4n + 3, cuyos residuos, cuando se cambia de signo, se convierten en no residuos y viceversa (vease art. 98).

Ademas de lo que precede, es fúcil derivar una regla general: —1 es un ***residuo de todos los numeros no divisibles ni por*** 4 ***ni por ningun numero primo de la forma 4n*** + 3. ***El es un no residuo de todos los restantes.*** Veanse art. 103 y 105.

***Residuos*** +2 ***y*** -2.

112.

Llegamos a los residuos +2 y -2.

Si de la tabla II recogemos todo número primo del cual +2 es un residuo, tendremos: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Es fúcil observar que entre estos números ninguno es de la forma 8n + 3 ni 8n + 5.

Veamos si de esta inducción puede hacerse una certidumbre.

Notamos primero que todo número compuesto de la forma 8n + 3 u 8n + 5 necesariamente involucra un factor primo de una de las dos formas 8n + 3 u 8n + 5. Pues, es claro que números primos de la forma 8n +1 u 8n + 7 pueden formar únicamente números que son de la forma 8n + 1 u 8n + 7. Por lo tanto, si nuestra induccion es cierta en general, no se presentará ningún número de la forma 8n + 3 u 8n + 5 cuyo residuo sea +2. Pero, ciertamente, no existe ningún número de esta forma menor que 100 del cual +2 es un residuo. Sin embargo, si se encuentran tales números mas allú de este límite, sea el menor de todos ellos = t. Así pues t serú o de la forma 8n + 3 o de la forma 8n + 5; +2 serú un residuo de t, pero un no residuo de todos los números semejantes menores que t. Si se pone 2 ξ a2 (mod. t), siempre a podrú tomarse como impar y a la vez < t, (puesto que a tendrá al menos dos valores positivos menores que t cuya suma = t, de los cuales uno es par y el otro impar, veanse art. 104 y 105). Por la misma razún, sea a2 = 2 + tu, es decir tu = a2 — 2, a2 serú de la forma 8n +1, tu por lo tanto de la forma 8n — 1, y así u serú de la forma 8n + 3 u 8n + 5 según sea t de la segunda forma o de la primera forma. Pero, de la ecuaciún a2 = 2 + tu se sigue tambien que 2 ξ a2 (mod. u), i.e., 2 tambien sera un residuo de u. Pero con facilidad se percibe que u < t, de donde t no es el número menor en nuestra induccion, contrariamente a la hipotesis. Asú se sigue claramente que lo que habúamos encontrado por inducciúon para el caso general es verdadero.

Al combinar esto con la proposiciún del art. 111, encontramos los siguientes teoremas:

1. +2 ***será un no residuo y*** —2 ***un residuo de todos los numeros primos de la forma*** 8n + 3.
2. ***Tanto*** +2 ***como*** —2 ***serán no residuos de todos los números primos de la forma*** 8n + 5. [[117]](#footnote-118)

es un residuo de los siguientes números primos: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97[[118]](#footnote-119)). Puesto que ninguno de ellos es de la forma 8n + 5 u 8n + 7, investigaremos entonces si es que esta inducción puede tener la fuerza de un teorema general. Se demuestra de modo semejante al artículo anterior que todo número compuesto de la forma 8n + 5 u 8n + 7 involucra un factor primo de la forma 8n + 5 u 8n + 7, de tal manera que, si nuestra generalizaciún es cierta, —2 no puede ser un residuo de ningún número de la forma 8n + 5 u 8n + 7. Pero si tales números existen, sea el menor de ellos = t y tendremos — 2 = a2 — tu. Si como antes se toma a impar y menor que t, u serú de la forma 8n + 5 u 8n + 7 según que t sea de la forma 8n + 7 u 8n + 5. Pero de a2 + 2 = tu y a < t podrú derivarse fácilmente tambien que u será menor que t. Finalmente, —2 sera un residuo de u, i.e., t no sera el menor numero de los que —2 es residuo, contradiciendo la hipútesis de nuestra inducciún. Por lo que —2 necesariamente es un no residuo de todos los números de las formas 8n + 5 y 8n + 7.

Al combinarse esto con la proposicion del art. 111, se obtienen estos teoremas:

1. Tanto —2 como +2 son no residuos de todos los números primos 8n + 5, tal como vimos en el artúculo anterior.
2. —2 ***es un no residuo y*** +2 ***es un residuo de todos los números primos de la forma*** *8****n*** + 7.

Ademas, en ambas demostraciones habríamos podido tomar a como un número par. Pero entonces, habríamos tenido que distinguir el caso donde a fuera de la forma 4n + 2 del caso en donde a fuera de la forma 4n. El desarrollo procede tal como antes sin dificultad alguna.

114.

Falta el caso en que el número primo es de la forma 8n +1. Pero esto no se puede resolver por el metodo anterior y exige artificios muy particulares.

Sea a cualquier raúz primitiva para el modulo 8n + 1, por lo que a4n = — 1 (mod. 8n + 1) (art. 62). Tal congruencia puede tambien expresarse en la forma (a2n + 1)2 = 2a2n (mod. 8n +1), o bien por (a2n — 1)2 = —2a2n. De donde se sigue que tanto 2a2n como —2a2n son residuos de 8n +1; pero puesto que a2n es un cuadrado no divisible por el modulo, es claro tambien que tanto +2 como —2 serún residuos (art. 98).

115.

No será inútil agregar ahora otra demostración de este teorema. Esta guarda una relación con la anterior como la segunda demostración (art. 109) del teorema del art. 108 con la primera (art. 108). Los peritos notaran facilmente que las dos demostraciones no son tan diferentes como quizós aparentan al principio, tanto en el primer caso como en el segundo.

1. Entre los números 1, 2, 3, ... 4m menores que un modulo primo cualquie­ra de la forma 4m + 1, aparecerán m números que pueden ser congruentes a un bicuadrado, mientras que los restantes 3m no podran ser congruentes.

Esto se deriva facilmente de los principios de la seccion anterior, pero tambien sin estos la demostración es fócil. En efecto, hemos demostrado que para tal modulo — 1 siempre es un residuo cuadrótico. Sea así f2 = — 1. Es claro que si z es un número cualquiera no divisible por el modulo, los bicuadrados de los cuatro numeros +z, —z, +fz, — fz (se percibe con facilidad que dos cualesquiera de ellos son incongruentes) son congruentes entre sí. Ademas, es claro que el bicuadrado de un numero cualquiera que no es congruente a ninguno de estos cuatro no puede ser congruente a los bicuadrados de ellos (en efecto, la congruencia x4 = z4, la cual es de cuarto grado, tendría mas de cuatro raíces, contrariamente al art. 43). De esto se deduce facilmente que todos los numeros 1, 2, 3, ... 4m dan lugar a m bicuadrados no congruentes y que entre estos mismos numeros se encontraran m nómeros congruentes a estos, mientras que los restantes no podran ser congruentes a ningun bicuadrado.

1. Segun un modulo primo de la forma 8n +1, —1 podra ser congruente a un bicuadrado (—1 sera un residuo bicuadrático de este numero primo).

De hecho, el numero de residuos bicuadráticos menores que 8n +1 (excluyendo a cero) sera = 2n, i.e., par. Ademas, se muestra facilmente que, si r es un residuo bicuadrático de 8n +1, tambien sera un residuo el valor de la expresion 1 (mod. 8n + 1). De esto: todos los residuos bicuadráticos podran distribuirse en clases de modo semejante a como los distribuimos en el art. 109. La parte restante de la demostracion procede exactamente de la misma manera que allí.

1. Ahora, sea g4 = — 1 y h un valor de la expresion 1 (mod. 8n + 1). Por tanto, sera

(g ± h)2 = g2 + h2 ± 2gh = g2 + h2 ± 2

= 1). Pero g4 = — 1 así que — h2 = g4h2 = g2 de donde g2 + h2 = 0 y

(ya que gh (g ± h)2 =

±2, i.e., tanto +2 como —2 son residuos cuadráticos de 8n +1. Q. E. D.

116.

La siguiente regla general se deduce fácilmente de lo anterior: +2 es un residuo de cualquier número que no puede dividirse ni por 4 ni por ningún número primo de la forma 8n + 3 u 8n + 5, pero es un no residuo de los restantes (por ejemplo, de todos los námeros de la forma 8n + 3 y 8n + 5 tanto primos como compuestos).

— 2 ***es un residuo de cualquier numero que no puede dividirse ni por 4, ni por ningún primo de la forma 8n*** + 5 ***u 8n***+ 7; ***pero de todos los restantes es un no residuo.***

El sagaz Fermat tambien conoció estos teoremas tan elegantes (Op. Mathem., p. 168). Aunque afirmo tener una demostracion, nunca la presento. Luego, el ilustre Euler la buscá siempre en vano, pero fue el ilustre Lagrange quien logro la primera demostracion rigurosa, (Nouv. Múm. de l’Ac. de Berlin, 1775, p. 349, 351). El ilustre Euler parece no haberla visto cuando escribiá su disertacián conservada en su Opuse. Analyt., (T. I., p. 259).

***Residuos*** +3 ***y —3.***

117.

Pasamos a los residuos +3 y —3. Iniciamos con el segundo de ellos.

De la tabla II encontramos que —3 es un residuo de estos numeros primos: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, entre los cuales no se encuentra ninguno de la forma 6n + 5. Demostramos de la manera siguiente que tampoco afuera de los límites de la tabla existen primos de esta forma, de los cuales —3 es un residuo. Primero, es claro que cualquier nuámero compuesto de la forma 6n + 5 involucra necesariamente algán factor primo de la misma forma. Por lo tanto, hasta el punto en que no exista ningun námero primo de la forma 6n + 5 cuyo residuo sea —3, tampoco existirá un námero compuesto con esta propiedad. Si tales numeros existen fuera de los límites de nuestra tabla, sea el menor de todos = t y sea —3 = a? — tu. Por lo tanto, si a se toma par y menor que t, tendremos u < t y —3 será un residuo de u. Pero cuando a es de la forma 6n ± 2, tu será de la forma 6n +1, de donde u es de la forma 6n + 5. Q. E. A., puesto que hemos supuesto que t es el menor de los números contrariamente a nuestra induccián. Pero cuando a es de la forma 6n, sera tu de la forma 36n + 3, asá que 3tu sera de la forma 12n + 1, por lo que 3u será de la forma 6n + 5; pero es claro que —3 será tambien un residuo de 3u aunque 3u < t, Q. E. A. Por lo tanto es claro que —3 no puede ser un residuo de ningán námero de la forma 6n + 5.

Ya que cualquier numero de la forma 6n + 5 está contenido necesariamente entre aquellos de la forma 12n + 5 o 12n +11 y puesto que la primera es de la forma

4n + 1 y la segunda de la forma 4n + 3, se tienen los siguientes teoremas:

1. ***Tanto*** —3 ***como*** +3 ***son no residuos de cualquier número primo de la forma*** 12n + 5.
2. —3 ***es un no residuo y*** +3 ***es un residuo de cualquier número primo de la forma*** 12n + 11.

118.

Los numeros que encontramos en la tabla II y que tienen residuo +3 son: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97; entre ellos, ninguno es de la forma 12n + 5 o 12n + 7. Puede comprobarse exactamente como en los artículos 112, 113 y 117 que no existe ningún número de las formas 12n + 5 ni 12n + 7 cuyo residuo sea +3, por lo que suprimimos este desarrollo. Combinando estos resultados con los del art. 111 tenemos los siguentes teoremas:

1. Tanto +3 como —3 son no residuos de cualquier numero primo de la forma 12n + 5 (tal como ya encontramos en el artículo anterior).
2. +3 ***es un no residuo y*** —3 ***es un residuo de cualquier numero primo de la forma*** 12n + 7. [[119]](#footnote-120)

Además, es evidente que esta demostración (que es independiente de las precedentes) tambien comprende numeros primos de la forma 12n + 7, a los que ya nos referimos en un artículo anterior.

Conviene observar que se podria usar el metodo de los artículos 109 y 115, pero por brevedad no nos detenemos en estos detalles.

120.

De lo precedente se obtienen fócilmente los siguientes teoremas (ver art. 102, 103 y 105).

1. —3 ***es un residuo de todos los números que no pueden dividirse ni por*** 8, ***ni por 9, ni por ningún numero primo de la forma*** 6n + 5, ***y es un no residuo de todos los restantes.***
2. +3 ***es un residuo de todos los números que no pueden dividirse ni por*** 4, ***ni por 9, ni por ningun primo de la forma*** 12n + 5 ***o*** 12n + 7, ***y es un no residuo de todos los restantes.***

Se tiene aquí este caso particular:

—3 es un residuo de todos los numeros primos de la forma 3n + 1, o lo que es lo mismo, de todos los que son residuos de 3. Pero es un no residuo de todos los nómeros primos de la forma 6n + 5, o excluido 2, de todos los primos de la forma 3n + 2, i.e., de todos los primos que son no residuos de 3. Se ve fócilmente que todos los casos restantes se siguen naturalmente de este.

Fermat ya conocía las proposiciones sobre los residuos +3 y —3, Opera de Wallis, T. II, p. 857. Pero el ilustre Euler fue el primero en dar demostraciones, Comm. nov. Petr., T. VIII, p. 105 y siguientes. Esto resulta mós admirable puesto que las demostraciones de las proposiciones pertenecientes a los residuos +2 y —2 estan basadas en artificios bastante parecidos. Vease tambien el comentario del ilustre Lagrange en Nouv. Mém. de l’ Ac. de Berlin, 1775, p. 352.

***Residuos*** +5 ***y*** —5.

121.

Por induccion se descubre que +5 no es un residuo de ningun numero impar de la forma 5n + 2 o 5n + 3, i.e., de ningun numero impar que sea no residuo de 5. Se demuestra que esta regla no tiene excepcion alguna. Sea el numero menor que constituya una excepción de esta regla = t, este por lo tanto es un no residuo del

número 5, pero 5 es un residuo de t. Sea a2 = 5 + tu tal que a sea par y menor que t. Entonces u serú impar y menor que t, pero +5 sera un residuo de u. Ahora si a no es divisible por 5, tampoco lo sera u. Pero es claro que tu es un residuo de 5, por lo que, puesto que t es un no residuo de 5, tampoco lo sera u, i.e., existe un no residuo impar del nuúmero 5 cuyo residuo es +5, pero menor que t, contrariamente a la hipútesis. Si por otro lado a es divisible por 5, se pone a = 5b y u = 5v de donde tv = — 1 ξ 4 (mod. 5), i.e., tv sera un residuo del número 5. En lo restante la demostraciún procede de manera analoga al caso anterior.

122.

Tanto +5 como —5 serán no residuos de todos los números primos que simultáneamente son no residuos de 5 y de la forma 4n + 1, i.e., de todos los números primos de la forma 20n + 13 o 20n + 17. Pero +5 serú un no residuo y —5 un residuo de todos los números primos de la forma 20n + 3 o 20n + 7.

Puede demostrarse de modo parecido que —5 es un no residuo de todos los números primos de las formas 20n +11, 20n + 13, 20n + 17 y 20n + 19. Se nota facilmente de aquí que +5 es un residuo de todos los números primos de la forma 20n+11 o 20n+19, pero no residuo de todos los de la forma 20n+13 o 20n+17. Puesto que cada número primo, aparte de 2 y 5 (cuyos residuos son ±5), esta contenido en alguna de las formas 20n + 1, 3, 7, 9, 11, 13, 17, 19, es claro que se puede juzgar ahora a todos, excepto a los que son de la forma 20n + 1 o de la forma 20n + 9. [[120]](#footnote-121)

Pero la verificación de esta inducción no es tan fácil. Cuando se presenta un nómero primo de la forma 20n + 1, o mas generalmente de la forma 5n + 1, este asunto puede resolverse de un modo similar al de los artículos 114 y 119. De hecho, sea a un numero cualquiera perteneciente al exponente 5 para el modulo 5n + 1, el cual evidentemente existe por la sección anterior, y se tendrá a5 ξ 1, o sea (a — 1)(a4 + a3 + a2 + a +1) ξ 0 (mod. 5n + 1). Pero no puede ser a ξ 1, por eso tampoco a — 1 ξ 0; necesariamente sera a4 + a3 + a2 + a + 1 ξ 0. Por lo tanto tambien 4(a4 + a3 + a2 + a +1) = (2a2 + a + 2)2 — 5a2 sera ξ 0, i.e., 5a2 sera un residuo de 5n +1, de donde tambien lo seró 5, ya que a2 es un residuo no divisible por 5n +1 (pues a no es divisible por 5n +1 porque a5 ξ 1). Q. E. D.

Pero el caso donde se presenta un nómero primo de la forma 5n + 4 exige artificios mós sutiles. Puesto que las proposiciones que necesitamos aquí se tratarón con móas generalidad en lo que sigue, aquó lo tocamos brevemente.

1. Si p es un número primo y b un no residuo cuadrático dado de p, el valor de la expresióon

t (x + \/b)p+1 — (x — x/b)p+1

(A)... 7

(se observa con facilidad que el desarrollo de esta carece de irracionales) siempre sera divisible por p, cualquiera que sea el nómero que se tome para x. De hecho, es claro de la inspección de los coeficientes que se obtienen del desarrollo de A, que todos los terminos desde el segundo al penóltimo (inclusive) son divisibles por p y

p — 1

que A ξ 2(p + 1)(xp + xb) (mod. p). Pero ya que b es un no residuo de p, sera b ~2 ξ—1 (mod. p), (art. 106); pero xp siempre es ξ x (sección anterior), de donde A ξ 0. Q. E. D.

1. En la congruencia A ξ 0 (mod. p) la indeterminada x tiene exponente p y todos los numeros 0, 1, 2, ...p — 1 serán raóces de ella. Ahora, tomese a e como un divisor de p +1. La expresion

(x + 7b)e — (x — x/b)6

7b

(la cual denotamos por B), si se desarrolla, no tendrá irracionales, la indeterminada x tendrá exponente e — 1, y resulta de los primeros elementos del anólisis que A es divisible (algebraicamente) por B. Ahora digo que existen e — 1 valores de x, que sustituidos en B, hacen B divisible por p. En efecto, si A ξ BC, x tendró exponente p — e +1 en C, y la congruencia C ξ 0 (mod. p) tendrá no mós que p — e + 1 raíces.

De donde resulta evidente que todos los e — 1 números restantes entre 0, 1, 2, 3, ...p — 1, serún raíces de la congruencia B = 0.

1. Ahora supúngase que p es de la forma 5n + 4, e = 5, b es un no residuo de p, y el número a se determina tal que

(a + Vb)5 — (a — Vb)5

Vb

es divisible por p. Pero esa expresión es

= 10a4 + 20a2 b + 2b2 = 2((b + 5a2)2 — 20a4)

Por lo tanto, tambien (b + 5a2)2 — 20a4 serú divisible por p, i.e., 20a4 es un residuo de p; pero ya que 4a4 es un residuo no divisible por p (de hecho, se comprueba facilmente que a no puede dividirse por p), tambien 5 serú un residuo de p. Q. E. D.

El teorema enunciado en el comienzo de este artículo resulta verdadero. Notamos que las demostraciones para ambos casos se deben al ilustre Lagrange, Mem. de l’Ac. de Berlin, 1775, p. 352 y siguientes.

Sobre ±7.

124.

Por un metodo similar se demuestra:

—7 es un no residuo de cualquier número que sea no residuo de 7.

Y por induction se puede concluir:

—7 es un residuo de cualquier número primo que sea residuo de 7.

Pero nadie ha demostrado esto rigurosamente hasta ahora. La demostracioún es facil para los residuos de 7 cuya forma es 4n — 1; en efecto, por el metodo conocido del artúculo precedente puede mostrarse que +7 siempre es un no residuo de tales números primos y así —7 es un residuo. Pero con esto se logra poco, ya que, los casos restantes no pueden tratarse con este metodo. Solo podemos resolver un caso de modo similar a los artúculos 119 y 123. A saber: si p es un numero primo de la forma 7n + 1, y a pertenece al exponente 7 para el múdulo p, se observa facilmente que:

(2a3 + a2 — a — 2)2 + 7(a2 + a)2

4(a7 — 1)

a1

es divisible por p, de donde — 7(a2 + a)2 será un residuo de p. Pero (a2 + a)2, como un cuadrado, es un residuo de p y no divisible por p; puesto que se supone que a pertenece al exponente 7, no puede ser ni ξ 0, ni = — 1 (mod. p), i.e., ni a ni a +1 serán divisibles por p, ni tampoco lo será el cuadrado (a + 1)2a2. De donde tambien es evidente que —7 sera un residuo de p. Q.E.D.— Pero los numeros primos de la forma 7n + 2 o 7n + 4 no se prestan a ninguno de los metodos tratados hasta ahora. Esta demostración tambien fue encontrada primeramente por el ilustre Lagrange en la misma obra.— Posteriormente, en la Seccion VII, enseñaremos mas generalmente que la expresián \_:ί1) siempre puede reducirse a la forma X2 ^ pY2 (donde hay

que tomar el signo superior cuando p es numero primo de la forma 4n +1 y el inferior cuando es de la forma 4n + 3). Aquí X e Y denotan funciones racionales de x, libres de fracciones. El ilustre Lagrange no desarrollá su analisis mas allá del caso p = 7 (vea p. 352 de su obra).

Preparación para la investigación general.

125.

Puesto que los metodos precedentes no son suficientes para asegurar las demostraciones generales, es momento para exponer otro máetodo libre de este defecto. Iniciamos con un teorema cuya demostracion por mucho tiempo nos eludio, aunque a primera vista parezca tan obvio como para que algunos ni siquiera hayan reconocido la necesidad de una demostracion. Es este: Cualquier nómero, exceptó los cuadrados tomados positivamente, es un no residuo de algunos nómeros primos. Pero ya que usamos este teorema solamente como una ayuda para demostrar otros, no explicamos mas que aquellos casos que necesitaremos para este fin. Los casos restantes se daran mas adelante. Demostremos por tanto que cualquier nómero primo de la forma 4n+1 tomado positiva o negativamente[[121]](#footnote-122)) es un no residuo de algunos nómeros primos, y, de hecho, (si es > 5) de algunos primos que son menores que si mismo.

Primero, cuando se presenta un námero primo p de la forma 4n +1 (> 17; aunque — 13N3 y — 17N5) tomado negativamente, sea 2a el primer námero par mayor que ^/p; entonces se ve fácilmente que 4a2 siempre será < 2p o sea 4a2 — p < p. Pero 4a2 — p es de la forma 4n + 3 mientras que +p es un residuo cuadrático de 4a2 — p (ya que p ξ 4a2 (mod. 4a2 — p)). Por eso si 4a2 — p es un número primo, —p será un no residuo de el; si no, necesariamente algán factor de 4a2 — p será de la forma 4n + 3; como +p tambien debe ser un residuo de el, —p será un no residuo. Q. E. D.

Para un número primo tomado positivamente distinguimos dos casos. Primero sea p un número primo de la forma 8n + 5; sea a cualquier número positivo < \j\p. Entonces 8n + 5 — 2a2 sera un numero positivo de la forma 8n + 5 u 8n + 3 (segun que a sea par o impar) y por lo tanto necesariamente divisible por algún primo de la forma 8n + 3 u 8n + 5, puesto que el producto de cualquier cantidad de números de la forma 8n +1 y 8n + 7 no puede tener ni la forma 8n + 3 ni 8n + 5. Sea este producto = q, así que 8n + 5 ξ 2a2 (mod. q). Pero 2 serú un no residuo de q (art. 112); así

tambien 2a2 [[122]](#footnote-123)) y 8n + 5. Q. E. D.

126.

Que cualquier número primo de la forma 8n +1 tomado positivamente siempre es un no residuo de algún número primo menor que el, no puede demostrarse por artificios tan obvios. Como esta verdad es de gran importancia, no podemos excluir la demostración rigurosa aunque sea algo prolija. Comencemos como sigue:

LEMA: Si se tienen dos series de números,

A, B, C, etc.... (I), A', B', C', etc.... (II)

(no interesa si el numero de terminos en un caso es el mismo que en el otro o no) confeccionadas de manera que, si p denota un número primo cualquiera o la potencia de un numero primo, cuando p divide algún túrmino de la segunda serie (o varios), habrá por lo menos tantos términos de la primera serie divisibles por p. Entonces, afirmo que el producto de todos los numeros *(*I) sera divisible por el producto de todos los numeros *(*II*)*.

Ejemplo. Conste (I) de los numeros 12, 18, 45; (II) de los numeros 3, 4, 5, 6, 9. Entonces, si tomamos sucesivamente los números 2, 4, 3, 9, 5, encontramos que hay 2, 1, 3, 2, 1 terminos en (I) y 2, 1, 3, 1, 1 terminos en (II) que son, respectivamente, divisibles por dichos números y el producto de todos los terminos (I) = 9720 es divisible por el producto de todos los terminos (II), 3240.

Demostraciún. Sea el producto de todos los terminos (I) = Q, y el producto de todos los terminos de la serie (II) = Q'. Es evidente que cualquier número primo que es divisor de Q' tambien serú divisor de Q. Ahora mostraremos que cualquier

factor primo de Q' tiene un grado en Q al menos tan alto como lo tiene en Q'. Sea tal divisor p y supongamos que en la serie (I) hay a terminos divisibles por p, b terminos divisibles por p2, c terminos divisibles por p3, etc. Las letras a0, b', c', etc. denotan lo similar de la serie (II), y se ve facilmente que p tiene exponente a + b + c + etc. en Q, y a' + b' + c' + etc. en Q'. Pero ciertamente a' no es mayor que a, b' no es mayor que b etc. (por hipótesis); por lo que a' + b' + c' + etc. ciertamente no sera > a + b + c + etc.— Puesto que ningún numero primo puede tener mayor exponente en Q' que en Q, Q sera divisible por Q' (art. 17). Q. E. D.

127.

LEMA: En la progresión 1, 2, 3, 4, ...n no puede haber más términos divisibles por cualquier nUmero h, que en la progresián a, a +1, a + 2, ...a + n — 1, que contiene el mismo námero de terminos.

En efecto se nota sin dificultad que si n es un multiplo de h, en ambas progresiones habrá jh terminos que serán divisibles por h; si n no es multiplo de h, pongase n = eh + f, de manera que f sea < h. En la primera serie e terminos serán divisibles por h, y en la segunda lo serán e o e +1 terminos.

Como corolario de esto se sigue una proposicion conocida de la teoría de los números figurados; a saber, que

a(a + 1)(a + 2) ··· (a + n — 1)

1 · 2 · 3 · ...n

siempre es un numero entero. Pero si no nos equivocamos, nadie lo ha demostrado directamente.

Finalmente, este lema puede expresarse en forma mas general:

En la progresion a, a + 1, a + 2, ...a + n — 1 existen por lo menos tantos terminos congruentes segun el modulo h a un numero dado cualquiera r como terminos divisibles por h haya en 1, 2, 3, ...n.

128.

TEOREMA. Sea a un numero cualquiera de la forma 8n +1, p cualquier námero primo a a cuyo residuo es +a, y finalmente m un námero arbitrario: entonces yo afirmo que en la progresián

a, -(a — 1), 2(a — 4), -(a — 9), 2(a — 16), ... 2(a — m2) o -(a — m2)

1. 2 2

según que m sea par o impar, existen por lo menos tantos términos divisibles por p como existan en la progresión:

1, 2, 3, ... 2m + 1

Denotamos por (I) la primera progresión, por (II) la segunda.

Demostracion. I. Cuando p = 2, en (I) todos los terminos aparte del primero, i.e., m terminos serán divisibles; habrá igual número tambien en (II).

1. Sea p un numero impar, o el doble de un numero impar, o el cuadruplo de un numero impar, y a = r2 (mod. p). Entonces, en la progresion —m, — (m — 1), — (m—2), ... +m (la que tiene el mismo numero de terminos que (II) y que denotamos por (III)) por lo menos tantos terminos serán congruentes a r, segun el modulo p, como terminos en (II) sean divisibles por p (artículo precedente). Entre ellos no pueden haber dos iguales en magnitud que difieran en signo[[123]](#footnote-124)). Cada uno de ellos tendrá un valor correspondiente en la serie (I), el cual sera divisible por p. Por supuesto, si ±b es un termino de la serie (III) congruente a r segun el modulo p, a — b2 sera divisible por p. Por lo tanto, si por un lado b es par, el termino de la serie (I), 2(a — b2) sera divisible por p. Por otro lado, si b es impar, el termino ^(a — b2) sera divisible por p: pues es evidente que a— sera entero par, dado que a — b2 es divisible por 8, pero p es divisible a lo sumo por 4 (de hecho, por hipotesis a es de la forma 8n + 1 y b2, por ser el cuadrado de un numero impar, es de la misma forma; por lo que la diferencia sera de la forma 8n). De esto finalmente se concluye que tantos terminos en la serie (I) son divisibles por p, como en (III) sean congruentes a r segun el modulo p, i.e., igual numero o mas de los que son divisibles por p en (II).
2. Sea p de la forma 8n y a = r2 (mod. 2p). Entonces se observa facilmente que a, que por hipotesis es un residuo de p, sera tambien un residuo de 2p. Entonces, en la serie (III) habrá por lo menos tantos terminos congruentes a r, segun p, como en la (II) sean divisibles por p, y todos ellos serán de magnitudes diferentes. Pero a cada uno de ellos corresponderá algun termino divisible por p en (I). En efecto, si +b o —b = r (mod. p), sera b2 = r2 (mod. 2p) j), de donde el termino 2(a — b2) sera

divisible por p. Por lo que en (I) serán divisibles por p por lo menos tantos términos como en (II). Q. E. D.

129.

TEOREMA. Si a es un número primo de la forma 8n + 1, necesariamente habrá algún numero primo menor que 2\Ja + 1 del cual a sea un no residuo.

Demostraciún. Sea a un residuo de todos los primos menores que 2\Ja + 1. Entonces, se observara con facilidad que a tambien será un residuo de todos los námeros compuestos menores que 2\Ja + 1 (refierase a las reglas por las cuales aprendimos a deducir si un nuámero dado es un residuo de un nuámero compuesto o no: art. 105). Sea m el mayor entero menor que -^/a. Entonces en la serie

a 2(a - ^ 2(a - 4), 1(a - 9), ... 2(a - m2) o 2(a - m2) (I)

serán divisibles por algán námero menor que 2yfa + 1 tantos o mas terminos como en esta:

1, 2, 3, 4, ... 2m + 1 (art. precedente) (II)

De esto se sigue que el producto de todos los terminos en (I) es divisible por el producto de todos los terminos en (II) (art. 126). Pero esto o es = a(a — 1)(a — 4) ■■■ (a — m2) o bien la mitad de este producto (segun que m sea par o impar). Por lo que el producto a(a — 1)(a — 4) ■■■ (a — m2) puede dividirse por el producto de todos los terminos en (II), y, puesto que todos estos terminos son primos a a, tambien lo sera su producto, omitido el factor a. Pero el producto de todos los terminos de (II) tambien puede presentarse así:

(m +1) ■ ((m + 1)2 — 1) ■ ((m + 1)2 — 4) ■■ ■ ■ ((m + 1)2 — m2)

Por lo tanto

1. a — 1 a — 4 a — m2

m +1 (m + 1)2 — 1 (m + 1)2 — 4 (m + 1)2 — m2

sera un numero entero, aunque sea un producto de fracciones menores que la unidad: puesto que en efecto -^/a necesariamente debe ser irracional, sera m +1 > -^/a. Y por lo tanto (m + 1)2 > a. De esto finalmente se concluye que nuestra suposición no puede tener lugar. Q. E. D.

Ahora, puesto que ciertamente a > 9, tendremos 2^Ja +1 < a. Por lo tanto existirá algun primo < a del cual a es un no residuo.

Por inducción se apoya un teorema general (fundamental),  
y se deducen algunas conclusiones de él.

130.

Después de haber demostrado rigurosamente que cada número primo de la forma 4n +1, tomado positivo o negativamente, es un no residuo de algún número primo menor que el mismo, pasamos entonces a una comparaciún mús exacta y mas general de los nuúmeros primos, para ver cuando uno es un residuo o un no residuo del otro.

Con todo rigor, hemos demostrado arriba que —3 y +5 son residuos o no residuos de todos los nuúmeros primos que son residuos o no residuos respectivamente de 3 y 5.

Se encuentra por inducciún que los números —7, —11, +13, +17, —19, —23, +29, —31, +37, +41, —43, —47, +53, —59, etc., son residuos o no residuos de todos los nuúmeros primos, los cuales tomados positivamente, resultan residuos o no residuos de estos primos respectivamente. Esta inducción puede llevarse a cabo facilmente con ayuda de la tabla II.

Quienquiera, con un poco de atencion, notará que de estos números primos aquellos con signo positivo son los de la forma 4n + 1, y los de signo negativo son los de la forma 4n + 3. [[124]](#footnote-125)

la forma 4n + 3. Finalmente la letra R puesta entre dos cantidades indicará que la primera es un residuo de la siguiente, mientras que la letra N tendrá el significado contrario. Por ejemplo, +5R11, ±2N5 indicara que +5 es un residuo de 11, pero +2 y —2 son no residuos de 5. Ahora, al unir el teorema fundamental con los teoremas del art. 111 fáacilmente se deduciráan las siguientes proposiciones.

1.

2.

3.

4.

Si

± *aRa'*

± aNa'

*+aRb* 1  
*—aNb }*

+aNb 1  
aRb

5. ± bRa

6.

7.

8.

± bNa

+bRb' I — bNb'

+bNb'

bRb'

seraá ± a'Ra ± a'Na ± bRa

± bNa

+aRb

—aNb

+aNb — aRb

+b'Nb —b'Rb

' +b'Rb

b'Nb

132.

En esta tabla estan contenidos todos los casos que pueden ocurrir al comparar dos námeros primos: lo que sigue corresponderá a numeros cualesquiera, pero sus demostraciones son menos obvias.

|  |  |  |
| --- | --- | --- |
|  | Si | sera |
| 9. | ± aRA... | ... ± ARa |
| 10. | ± bRA... | í +ARb ... \ —ANb |
| 11. | + aRB... | ... ± BRa |
| 12. | — aRB... | ... ± BNa |
| 13. | + bRB... | í —BRb ... \ +BNb |
| 14. | — bRB... | í +BRb ... i -BNb |

Puesto que los mismos principios conducen a las demostraciones de todas estas proposiciones, no sera necesario desarrollarlas todas: la demostración de la proposición 9 que adjuntamos puede servir como ejemplo. Ante todo se notara que cada nómero de la forma 4n + 1 puede tener o ningón factor de la forma 4n + 3, o dos, o cuatro, etc., i.e., el nómero de tales factores (entre los cuales varios pueden ser iguales) siempre sera un numero par. Por otro lado, cualquier numero de la forma 4n + 3 tendrá un numero impar de factores de la forma 4n + 3 (i.e., o uno, o tres, o cinco etc.). El numero de factores de la forma 4n +1 permanece indeterminado.

La Proposición 9 se demuestra de la siguiente forma. Sea A el producto de los factores primos a', a", a'", etc., b, b', b", etc.; donde el nómero de factores b, b', b", etc. es par (puede tambien que no haya ninguno, lo que se reduce a lo mismo). Ahora, si a es un residuo de A, tambien seró un residuo de todos los factores a', a'', a''', etc., b, b', b'', etc.; de donde por las proposiciones 1 y 3 del artículo precedente cada uno de estos factores serán residuos de a; por lo tanto tambien el producto A, lo mismo que -A; sin embargo, si —a es un residuo de A y por lo tanto de los factores a', a'', etc., b, b', etc., cada uno de a', a'', etc. sera un residuo de a, y cada uno de b, b', etc. un no residuo. Pero como el numero de estos óltimos es par, el producto de todos, esto es A, sera un residuo de a, y así tambien lo seró —A.

133.

Iniciamos ahora una investigation mas general. Consideraremos dos numeros impares cualesquiera P y Q, primos entre só, provistos de signos cualesquiera. Concíbase a P resuelto en sus factores primos sin consideración de su signo, y se denotará por p el nómero de estos factores para los cuales Q sea un no residuo. Si algón nómero primo, del cual Q es un no residuo, aparece varias veces entre los factores de P, tambien deberán ser contados varias veces. De modo semejante, sea q el nómero de factores primos de Q de los cuales P es un no residuo. Entonces los nómero p y q tendrán cierta relation dependiente de la naturaleza de los nómeros P y Q. En efecto, si uno de los nómeros p o q es par o impar la forma de los numeros P y Q mostrara si el otro es par o impar. Se presentará esta relation en la siguiente tabla.

Los nómeros p y q serón al mismo tiempo pares o al mismo tiempo impares

cuando los números P y Q tienen las formas:

|  |  |  |
| --- | --- | --- |
| 1. | + Λ | +A0 |
| 2. | + Λ | —A0 |
| 3. | + A, | +B |
| 4. | + A, | —B |
| 5. | — A, | —A0 |
| 6. | + B, | —B0 |

En el caso contrario, uno de los numeros p o q sera par, y el otro impar, cuando los nuúmeros P y Q tienen las formas:

|  |  |  |
| --- | --- | --- |
| 7. | — A, | +B |
| 8. | — A, | —B |
| 9. | + B, | +B0 |
| 10. | — B, | —B0[[125]](#footnote-126)) |

Ejemplo. Dados los numeros -55 y +1197, que representan el cuarto caso, entonces 1197 es un no residuo de un solo factor primo de 55, en efecto, del número 5, mientras que -55 es un no residuo de tres factores primos de 1197, a saber, de los números 3, 3 y 19.

Si P y Q denotan numeros primos, estas proposiciones se convierten en las que hemos tratado en el art. 131. De hecho, aquí p y q no pueden ser mayores que 1; por lo que cuando p se toma par, necesariamente sera = 0, i.e., Q serú un residuo de P, pero cuando p es impar, Q sera un no residuo de P, y vice-versa. Así, si se escribe a y b en lugar de A y B, se sigue de 8 que si —a es un residuo o no residuo de b, — b serú un no residuo o residuo de a, lo que coincide con 3 y 4 del art. 131.

Por lo general es evidente que Q no puede ser un no residuo de P a no ser que p = 0. Por lo tanto, si p es impar, ciertamente Q sera un no residuo de P.

De aquí tambien pueden derivarse sin dificultad las proposiciones del artículo precedente.

Por otra parte, pronto sera evidente que esta representación general es mas que una observaciúon estúeril, puesto que la demostracioún completa del teorema fundamental apenas podría completarse sin ella.

134.

Ahora nos dirigimos a deducir estas proposiciones.

1. Como antes, tómese P resuelto en sus factores primos sin tomar en consideración los signos y Q resuelto en factores de cualquier modo pero donde, no obstante, se considera el signo de Q. Se combina cada uno de aquellos factores con cada uno de estos. Si s denota el nómero de todas las combinaciones en las cuales el factor de Q es un no residuo del factor de P, entonces p y s serán al mismo tiempo pares o impares. De hecho, sean f, f', f'', etc. los factores primos de P, y entre los factores en los que esta resuelto Q, sea m el numero que son no residuos de f, m' el de los no residuos de f', m'' el de los no residuos de f'', etc. Entonces se vera facilmente que

s = m + m' + m'' + etc.

y que p expresa cuantos numeros entre m, m', m'', etc. son impares. De donde es evidente que s sera par cuando p sea par, pero impar cuando p sea impar.

1. Esto vale generalmente para cualquier forma en que Q sea resuelto en factores. Pasemos a los casos particulares. Consideraremos primero el caso donde uno de los numeros P es positivo, pero el otro, Q, es o bien de la forma +A o bien de la forma —B. Se resuelven P y Q en sus factores primos, donde se les da un signo positivo a cada uno de los factores de P, pero a los factores individuales de Q el signo positivo o el negativo segun sean de la forma a o b. Entonces, como se requiere, es evidente que Q sera de la forma +A o —B. Se combinan cada uno de los factores de P con cada uno de los de Q y se denotara como antes por s el numero de combinaciones en que cada factor de Q es un no residuo del factor de P, y de modo semejante por t el numero de combinaciones en que cada factor de P es un no residuo del factor de Q. Se sigue del teorema fundamental que estas combinaciones serán identicas, de donde s = t. Finalmente de lo que hemos demostrado se sigue que p = s (mod. 2), q = t (mod. 2), y así p = q (mod. 2).

Así pues se tienen las proposiciones 1, 3, 4 y 6 del art. 133.

Las restantes proposiciones pueden derivarse directamente por metodos similares, pero requieren de una nueva consideracion. Sin embargo, se derivan mas facilmente de lo anterior por los metodos siguientes.

1. De nuevo P y Q denotan numeros impares cualesquiera, primos entre sí, p y q el numero de factores primos de P y Q de los que Q y P son no residuos respectivamente. Finalmente sea p0 el numero de factores primos de P de los cuales

—Q es un no residuo (cuando Q es negativo es evidente que — Q indicará un número positivo). Ahora se distribuyen todos los factores primos de P en cuatro clases.

1. Factores de la forma a, de los cuales Q es un residuo.
2. Factores de la forma b, de los cuales Q es un residuo. Sea χ el número de

ellos.

1. Factores de la forma a, de los cuales Q es un no residuo. Sea ψ el número de ellos.
2. Factores de la forma b, de los cuales Q es un no residuo. Sea ω el número de ellos.

Entonces se ve facilmente que p = ψ + ω, p = χ + ψ.

Cuando P es de la forma ±A, χ + ω y tambien χ — ω, serán numeros pares:

por lo que p = p + χ — ω ξ p (mod. 2). Pero cuando P es de la forma ±B, se

descubre por un razonamiento similar que los números p y p serán incongruentes, segun mod. 2.

1. Apliquemos esto a cada uno de los casos. Primero, sean tanto P como Q de la forma +A, entonces de la proposiciún 1 tendremos p ξ q (mod. 2); pero p ξ p (mod. 2); por lo que tambien p ξ q (mod. 2). Lo cual concuerda con la proposiciún 2.— De modo semejante si P es de la forma —A, Q de la forma +A, sera p ξ q (mod. 2) de la proposiciún 2 la que ya hemos demostrado. De esto si p ξ p tendremos p ξ q. Así pues, tambien la proposiciún 5 esta demostrada.

De la misma manera se deriva la proposición 7 de la 3, la proposición 8 o de la 4 o de la 7; la 9 de la 6; la 10 de la 6.

Demostración rigurosa del teorema fundamental.

135.

Las proposiciones del artículo 133 no se han demostrado por medio del artículo precedente, sino que se mostro que la validez de ellas depende de la validez del teorema fundamental que hemos supuesto. Por el metodo de esta misma deduccion es evidente que estas proposiciones valdran para numeros P y Q si el teorema fundamental vale para todos los factores primos de estos numeros comparados entre sí, y aun si no fuera valido en general. Por lo tanto ahora avanzamos hacia la demostracion del teorema fundamental. Enunciamos antes de ella la siguiente aclaracion.

Diremos que el teorema fundamental es verdadero hasta algUn numero M, si vale para dos numeros primos cualesquiera de los cuales ninguno supera a M.

De modo semejante debe entenderse si decimos que los teoremas de los artículos 131, 132 y 133 son verdaderos hasta algún termino. Se nota fácilmente que si el teorema fundamental es valido hasta algún termino, estas proposiciones tendrún que ser vúlidas hasta el mismo termino.

136.

Por inducción puede confirmarse fúcilmente que el teorema fundamental vale para números pequeños, de tal manera se determina un límite hasta el cual sea vúlido. Suponemos que esta induccion esta hecha; es completamente indiferente hasta donde la hayamos realizado. De tal manera bastaría confirmarlo hasta al número 5, pero esto se logra con la simple observación de que +5N3, ±3N5.

Ahora, si el teorema fundamental no es verdadero en general, existirú algun Imite T hasta el cual valdrá, de manera que ya no valga mas para el próximo número mayor T +1. Esto es lo mismo que si dijeramos que existen dos numeros primos, de los cuales el mayor es T + 1 y que comparados entre sú contradicen el teorema fundamental, y dijeramos que otros pares cualesquiera de números primos, siendo ambos menores que T + 1, cumplen con este teorema. De donde se sigue que las proposiciones de los artúculos 131, 132, 133 tambien deberán ser validas hasta T. Pero mostraremos ahora que esta suposiciún no puede subsistir. Los casos siguientes deberán distinguirse segun las formas diferentes que pueden tener, tanto T + 1 como el número primo menor que T + 1 que contradiría el teorema. Denotemos este número primo por p.

Cuando tanto T + 1 como p son de la forma 4n + 1, el teorema fundamental puede ser falso de dos maneras, a saber, si al mismo tiempo fuera o bien ±pR(T + 1) y ±(T + 1)Np

o bien a la vez ±pN(T + 1) y ±(T + 1)Rp

Cuando tanto T + 1 como p son de la forma 4n + 3, el teorema fundamental sería falso si al mismo tiempo tuvieramos

|  |  |  |  |
| --- | --- | --- | --- |
| o bien | +pR(T + 1) | y | — (T + 1)Np |
| (o lo que es lo mismo | —pN (T + 1) | y | + (T + 1)Rp) |
| o bien | +pN (T + 1) | y | — (t + 1)Rp |
| (o sea | —pR(T + 1) | y | + (T +1)Np) |

Cuando T + 1 es de la forma 4n + 1, y p es de la forma 4n + 3, el teorema fundamental sería falso si tuvieramos

o bien ±pR(T +1) y +(T + 1)Np (o — (T + 1)Rp)

o bien ±pN(T +1) y — (T + 1)Np (o + (T + 1 )Rp)

Cuando T + 1 es de la forma 4n + 3 y p de la forma 4n +1, el teorema fundamental sería falso si tuvieramos

o bien +pR(T + 1) (o —pN(T + 1)) y ±(T + 1)Np

o bien +pN(T + 1) (o —pR(T + 1)) y ±(T + 1)Rp

Si se puede demostrar que ninguno de estos ocho casos puede tener lugar, sería

cierto al mismo tiempo que la validez del teorema fundamental no está acotada por

ningún límite. Ahora pasamos a este asunto, pero, puesto que algunos de estos casos son dependientes de otros, no convendraí mantener el mismo orden que hemos usado aquí para enumerarlos.

137.

Primer caso. Cuando T +1 es de la forma 4n + 1 (= a), y p es de la misma forma, si ±pRa, entonces no puede ser que ±aNp. Esto era el primer caso arriba.

Sea +p = e2 (mod. a), donde e es par y < a (esto siempre es posible). Ahora deben distinguirse dos casos.

1. Cuando e no es divisible por p, se pone e2 = p + af y f sera positivo de la forma 4n + 3 (o sea de la forma B), < a, y no divisible por p. Además tendremos e2 = p (mod. f), i.e., pRf de donde por la proposicián 11 del art. 132 ±fRp (en efecto p, f < a, y para ellos, estas proposiciones valdrán). Pero tambien afRp, por lo tanto ±aRp.
2. Cuando e es divisible por p, se pone e = gp y así e2 = p + aph o sea pg2 = 1 + ah. Entonces, h será de la forma 4n + 3 (B), y primo a g2 y p. Ademas, tendremos pg2Rh pues tambien pRh, y de esto (proposicián 11, art. 132) ±hRp. Y tambien —ahRp, porque —ah = 1 (mod. p); por lo tanto tambien será ^aRp. [[126]](#footnote-127)
3. Cuando e no es divisible por p, tampoco f será divisible por p. Además de esto f será positivo de la forma 4n +1 (o sea A), y < a, pero +pRf; por lo tanto (proposición 10 del art. 132) +fRp. Pero tambien +faRp, de donde tendremos +aRp, o -aNp.
4. Cuando e es divisible por p, sea e = pg y f = ph. Así que tendremos g2p = 1 + ha. Entonces h sera positivo de la forma 4n + 3 (B), y primo a p y g2. Además +g2pRh, así que +pRh; de esto (proposicion 13, art. 132) -hRp. Pero -haRp, de donde +aRp y -aNp.

139.

Tercer caso. Cuando T +1 es de la forma 4n + 1 (= a), p de la misma forma y ±pNa, entonces no puede ser que ±aRp. (Segundo caso arriba).

Tomemos algun námero primo menor que a, del cual +a sea un no residuo, el cual, hemos demostrado arriba, existe. Conviene considerar aquí dos casos por separado, segun que este numero primo sea de la forma 4n + 1 o 4n + 3; pues no se ha demostrado que existan tales námeros primos de ambas formas.

I. Sea ese námero primo = a' y de la forma 4n +1. Entonces tendremos ±a'Na (art. 131) ya que ±a'pRa. Sea por lo tanto e2 ξ a'p (mod. a) y e par, < a. Entonces deberáan distinguirse cuatro casos.

1. Cuando e no es divisible ni por p ni por a'; ponemos e2 = a'p ± af tomado el signo de tal manera que f sea positivo. Entonces será f < a, primo a a' ya p y para el signo superior, de la forma 4n + 3, para el inferior de la forma 4n +1. Por brevedad denotaremos por [x,y] el numero de factores primos del námero y de los cuales x es un no residuo. Entonces será a'pRf y así [a'p, f ] = 0. De esto [f, a'p] sera un numero par (las proposiciones 1 y 3 del art. 133), i.e., o bien = 0, o bien = 2. Por lo que f será o bien un residuo de ambos numeros a' y p o bien de ninguno. Pero lo primero es imposible ya que ±af es un residuo de a' y ±aNa' (hipotesis); de donde ±fNa'. De esto f tiene que ser un no residuo de ambos números a' y p. Pero puesto que ±afRp, tendremos ±aNp. Q. E. D.
2. Cuando e es divisible por p pero no por a', sea e = gp y g2p = a' ± ah, el signo determinado tal que h sea positivo. Entonces tendremos h < a, primo a a', g y p, para el signo superior de la forma 4n + 3, pero para el inferior de la forma 4n + 1. De la ecuacion g2p = a' ± ah, si se la multiplica por p y a', puede deducirse

sin dificultad alguna que

pa Rh (a)

±ahpRa0 (β)

aahRp (γ)

Sigue de (a) que [pa0,h] = 0, por lo que (proposiciones 1 y 3, art. 133) [h,pa0] es par, i.e., h será un no residuo o de ambos p y a0, o de ninguno. En el primer caso, sigue de (β) que ±apNa0, y ya que por hipótesis ±aNa0, sera ±pRa0. De esto, por el teorema fundamental que vale para los námeros p y a0, puesto que son menores que T +1, tendremos ±a0Rp. Ya que hNp, entonces por (γ), ±aNp. Q. E. D. En el segundo caso, sigue de (β) que ±apRa0, de esto ±pNa0, ±a0Np, y finalmente de esto y de hRp se tiene de (γ) que ±aNp. Q. E. D.

1. Cuando e es divisible por a0 pero no por p. Para este caso la demostracion procede de un modo semejante al precedente y no es necesario detenerse en esta.
2. Cuando e es divisible tanto por a0 como por p, y por tanto tambien por el producto a0p (hemos supuesto que los numeros a0 y p son diferentes, puesto que en el caso contrario, aNp estará contenido en la hipotesis aNa0). Sea e = ga0p y g2a0p = 1 ± ah. Entonces tendremos h < a, primo a a0 y p, para el signo superior de la forma 4n + 3, y para el inferior de la forma 4n +1. Pero se observa fácilmente que de esta ecuacion pueden deducirse las siguientes:

a0pRh (a)

±ahRa0 (β)

±ahRp (γ)

De (a), que coincide con (a) en 2), se sigue igualmente como allí. Esto es, al mismo tiempo se tiene o bien hRp, hRa0, o bien hNp, hNa0. Pero en el primer caso, por (β) sera aRa0, contrariamente a la hipotesis; por lo cual será hNp, y así tambien por

(γaNp.

II. Cuando ese numero primo es de la forma 4n + 3, la demostracián es tan similar a la precedente que no es importante adjuntarla. Para quienes desean desarrollarla (lo que recomendamos bastante), notamos que despues de haber llegado a la ecuacion e2 = bp ± af (denotando a b como aquel námero primo) sera átil si se consideran por separado ambos signos.

140.

Cuarto caso. Cuando T + 1 es de la forma 4n +1 (= a), p de la forma 4n + 3, y ±pNa, no podran ser ni +aRp ni -aNp. (El sexto caso arriba).

También por brevedad omitimos la demostración de este caso, puesto que es completamente similar a la demostración del tercer caso.

141.

Quinto caso. Cuando T +1 es de la forma 4n + 3 (= b), p de la misma forma, y +pRb o -pNb, no será ni +bRp ni -bNp. (Tercer caso arriba).

Sea p = e2 (mod. b), y e par y < b.

1. Cuando e no es divisible por p. Pongase e2 = p + bf y f sera positivo, de la forma 4n + 3, < b y primo a p. Ademas tendremos pRf, por tanto por la proposición 13, art. 132, -fRp. De esto y de +bfRp tenemos —bRp y así +bNp. Q. E. D.
2. Cuando e es divisible por p, sea e = pg y g2p = 1 + bh. Entonces tendremos h de la forma 4n +1 y primo a p, p = g2p2 (mod. h), por tanto pRh. De esto es +hRp (proposición 10, art. 132), y de —bhRp se sigue que —bRp o sea +bNp. Q. E. D.

142.

Sexto caso. Cuando T +1 es de la forma 4n + 3 (= b), p de la forma 4n + 1, y pRb, no puede ser ±bNp. (El septimo caso arriba.)

Omitimos la demostración, que es totalmente semejante a la precedente. [[127]](#footnote-128)

II. Cuando e es divisible por p, sea e = pg, y g2p = — 1 + bh. Entonces será h positivo, de la forma 4n + 3, primo a p y < b. Además tendremos —pRh, de donde (proposición 14, art. 132) +hRp. De bhRp sigue que +bRp o —bNp. Q. E. D.

144.

Octavo caso. Cuando T +1 es de la forma 4n + 3 (= b), p de la forma 4n + 1, y +pNb o —pRb, no puede ser ±bRp. (El ultimo caso arriba).

La demostración es como en el caso precedente.

Método análogo para la demostración del teorema del art. *11f.*

145.

En la demostración precedente siempre tomamos para e un valor par (art. 137­144). Conviene observar tambien que pudimos usar un valor impar, pero entonces hubieramos tenido que introducir para esto mas distinciones. Quienes se deleitan con estas investigaciones las encontrarán átiles si ponen esfuerzo en el desarrollo de estos casos. Ademas, los teoremas pertenecientes a los residuos +2 y —2 entonces deberían suponerse; pero como nuestra demostración está completa sin usar estos teoremas, obtenemos de esto un metodo nuevo para demostrarlos. Este no se debe desdeñar, ya que es mas directo que los metodos que utilizamos arriba para demostrar que ±2 es un residuo de cualquier numero primo de la forma 8n +1. Supondremos que los casos restantes (que abarcan los námeros primos de las formas 8n + 3, 8n + 5, 8n + 7) ya han sido demostrados mediante los máetodos tratados arriba, y que este teorema solamente ha sido establecido por inducción. No obstante, llevaremos esta inducción a un nivel de certidumbre mediante las siguientes reflexiones.

Si ±2 no es un residuo de todos los numeros primos de la forma 8n +1, póngase el menor primo de esta forma del cual ±2 es un no residuo = a, asó que el teorema vale para todos los primos menores que a. Entonces, se toma algón numero primo < 2a, del cual a es un no residuo (del articulo 129 se deduce con facilidad que tal nómero existe). Sea este nómero = p, por el teorema fundamental resultara pNa. De esto, ±2pRa.— Por eso, sea e2 ξ 2p (mod. a), de manera que e sea impar y < a. Entonces deberóan distinguirse dos casos.

I. Cuando e no es divisible por p. Sea e2 = 2p + aq, asó que q seró positivo, de la forma 8n + 7 o de la forma 8n + 3 (segón que p sea de la forma 4n + 1 o 4n + 3), < a, y no divisible por p. Todos los factores primos de q se distribuirón en cuatro clases, a saber: sean e aquellos de la forma 8n +1, f de la forma 8n + 3, g de la forma 8n + 5, h de la forma 8n + 7. Sea E el producto de los factores de la primera clase y los productos de los factores de la segunda, tercera, y cuarta clases respectivamente F, G, H[[128]](#footnote-129)). Hecho esto, consideraremos primero el caso donde p es de la forma 4n + 1 y q de la forma 8n + 7. Entonces se ve facilmente que 2RE y 2RH, de donde pRE y pRH y de esto finalmente ERp y HRp. Ademas 2 sera un no residuo de cualquier factor de la forma 8n + 3 u 8n + 5, y por eso tambien p; y este factor sera un no residuo de p; de donde se concluye facilmente que FG será un residuo de p si f + g es par, no residuo si f + g es impar. Pero f + g no puede ser impar; de hecho, enumerando todos los casos se nota facilmente que EFGH o sea q sera de la forma 8n + 3 u 8n + 5 si f + g es impar, sean como sean e, f, g, h por separado, contrariamente a la hipátesis. Por lo tanto, tendremos FGRp, EFGHRp, o sea qRp, y finalmente aqRp implica aRp, contrariamente a la hipótesis. Segundo, cuando p es de la forma 4n + 3, puede demostrarse de modo semejante que sera pRE, así que ERp y —pRF, y en consecuencia FRp, finalmente g + h es par y así GHRp, de donde finalmente se sigue que qRp y aRp, contrariamente a la hipátesis.

II. Cuando e es divisible por p, la demostracián puede prepararse de modo semejante y puede ser desarrollada sin dificultad por los expertos (para quienes se escribio este artículo). Por brevedad la omitimos.

La resolución del problema general.

146.

Por el teorema fundamental y las proposiciones pertenecientes a los residuos — 1 y ±2, siempre puede determinarse si un numero dado cualquiera es un residuo o un no residuo de un námero primo dado. Pero sera átil presentar de una manera clara lo que hemos dicho arriba para que se tenga reunido todo lo necesario para la resoluciáon.

PROBLEMA. Propuestos dos números cualesquiera P y Q, descubrir si uno de ellos Q es un residuo o no residuo del otro P.

Resolution. I. Sea P = α°ΑβcY etc. donde a, b, c, etc. denotan námeros primos diferentes positivos (puesto que se toma el valor absoluto de P). Por brevedad, en este artículo hablaremos simplemente de una relation de dos námeros x e y si el

primero x es un residuo o no residuo de y. Por tanto, la relación de Q y P depende de las relaciones de Q y aa; Q y be etc. (art. 105).

1. Para saber la relación de Q y aa (y de los restantes Q y be etc.) deben distinguirse dos casos.
2. Cuando Q es divisible por a. Pongase Q = Q'ae de manera que Q' no sea divisible por a. Entonces si e = α o e > α tendremos QRaa, pero si e < α e impar tendremos QNaa: finalmente si e < α y par, Q tendrá con aa la misma relacion que tiene Q' con aa-e. Así este caso se reduce al caso:
3. Cuando Q no es divisible por a. Aquí de nuevo distinguimos dos casos.
4. Cuando a = 2. Entonces siempre tendremos QRaa cuando α = 1; pero cuando α = 2, se requiere que Q sea de la forma 4n + 1. Finalmente, cuando α = 3 o > 3, Q debe ser de la forma 8n +1. Si se cumple esta condicion tendremos QRaa.
5. Cuando a es algón otro nómero primo. Entonces Q tendró con aa la misma relacion que tiene con a. (Vease art. 101).
6. Investíguese la relacion de un nómero cualquiera Q con un numero primo (impar) a de la manera siguiente. Cuando Q > a, sustitóyase en lugar de Q el menor residuo positivo de el segun el modulo a[[129]](#footnote-130)). Este tendró la misma relación con Q que tiene a.

Ahora resuelvase Q, o el numero tomado en su lugar, en sus factores primos p, p', p", etc., adjuntando el factor —1 cuando Q es negativo. Entonces resulta que la relacion de Q con a depende de las relaciones de cada uno de p, p', p', etc. con a. A saber, si entre aquellos factores, 2m son no residuos de a, resultara QRa, pero si son 2m + 1 factores, tendremos QNa. Se nota facilmente que si entre los factores p, p, p', etc. dos o cuatro o seis de ellos o en general 2k resultan iguales, ellos pueden con seguridad eliminarse.

1. Si entre los factores p, p', p' se encuentran —1 y 2, la relacion de estos con a puede encontrarse en los artículos 108, 112, 113, 114. La relacion de los restantes con a depende de las relaciones de a con ellos (teorema fundamental y proposiciones del art. 131). Sea p uno de ellos, y se encontrara (tratando los numeros a y p del mismo modo como antes se trataron Q y a, que eran respectivamente mayores) que la relacion de a con p o puede determinarse mediante los artículos 108-114 (si en efecto el menor residuo de a (mod. p) no tiene ningun factor primo impar), o depende de la relacion de p con ciertos numeros primos menores que p. Lo mismo vale para los restantes factores p0, p00, etc. Ahora se ve facilmente que continuando con esta

operación finalmente se llega a números cuyas relaciones pueden determinarse por las proposiciones de los art. 108-114. Con un ejemplo sera mús claro.

Ejemplo. Se quiere la relacion del número +453 con 1236. Tenemos 1236 = 4· 3 · 103; +453R4 por II.2(A); +453R3 por II.1. Por lo tanto queda examinar la relacion de +453 con 103. Ella serú la misma que tendrú +41 (= 453 (mod. 103)) con 103; la misma que +103 con 41 (teorema fundamental) o sea de -20 con 41. Pero —20R41; puesto que -20 = —1 · 2 · 2 · 5; — 1R41 (art. 108); y +5R41 porque 41 = 1 y es un residuo de 5 (teorema fundamental). De esto se sigue que +453R103, y finalmente de esto +453R1236. Y es cierto que 453 = 2972 (mod. 1236)

Sobre las formas lineales que contienen todos los números primos  
de los cuales un número dado cualquiera es un residuo o no residuo.

147.

Dado un número cualquiera A, pueden presentarse ciertas formulas bajo las cuales estarún contenidos todos los numeros primos a A de los cuales el residuo es A, o sea todos los que pueden ser divisores de los números de la forma x2 — A (denotando x2 como un cuadrado indeterminado)[[130]](#footnote-131)). Pero por brevedad examinaremos unicamente los divisores que son impares y primos a A, puesto que los restantes facilmente pueden reducirse a este caso.

Primero, sea A o un numero primo positivo de la forma 4n + 1, o negativo de la forma 4n — 1. Entonces, según el teorema fundamental, todos los números primos que, tomados positivamente, son residuos de A, serán divisores de x2 — A; todos los números primos (excepto el número 2 que siempre es divisor), que son no residuos de A serán no divisores de x2 — A. Denotense todos los residuos de A menores que A (excluyendo cero) por r, r', r'', etc.; todos los no residuos por n, n', n", etc. Entonces cualquier numero primo contenido en alguna de las formas Ak + r, Ak + r', Ak + r'', etc. sera divisor de x2 — A, pero cualquier primo contenido en alguna de las formas Ak + n, Ak + n', etc. sera un no divisor, k es un numero entero indeterminado. Llamamos formas de los divisores de x2 — A a las primeras, y formas de los no divisores a las segundas. El número de cada una de las dos sera 2(A — 1). Ahora, si B es un numero compuesto impar y ARB, todos los factores primos de B estarán contenidos en alguna de las primeras formas y por tanto lo estarú B mismo. Por lo

que cualquier número impar contenido en una forma de los no divisores, será un no divisor de la forma x2 — A. Pero este teorema no puede invertirse puesto que, si B es un no divisor compuesto impar de la forma x2 — A, habrá entre los factores primos de B algunos no divisores. Si el numero de ellos es par, B mismo se encontrará en alguna forma de los divisores. Vease art. 99.

Ejemplo. Para A = —11 se encuentran estas : 11k + 1, 3, 4, 5, 9 como las formas de los divisores de x2 + 11, mientras que las formas de los no divisores serán 11k + 2, 6, 7, 8, 10. Por lo tanto, —11 sera un no residuo de todos los numeros impares que estan contenidos en algunas de las segundas formas, pero sera un residuo de todos los primos pertenecientes a algunas de las primeras formas.

Se presentaran formas semejantes para divisores y no divisores de x2 — A, donde A denota un numero cualquiera. Pero se observa facilmente que conviene considerar los valores de A que no sean divisibles por ningun cuadrado. En efecto, si A = a2A', todos los divisores[[131]](#footnote-132)) de x2 — A tambien serán divisores de x2 — A0, y de modo semejante los no divisores. Distinguiremos tres casos, 1) cuando A es de la forma + (4n + 1) o — (4n — 1). 2) cuando A es de la forma — (4n +1) o + (4n — 1). 3) cuando A es par o sea de la forma ±(4n + 2).

148.

Primer caso, cuando A es de la forma + (4n +1) o — (4n — 1). Resuelvase A en sus factores primos y asígnese a los que son de la forma 4n +1 el signo positivo, y a los de la forma 4n — 1, el signo negativo (de donde el producto de todos ellos sera = A). Sean a, b, c, d, etc. estos factores. Distribuyanse todos los numeros menores que A y primos a A en dos clases: en la primera clase, todos los numeros que son no residuos o de ninguno de los numeros a, b, c, d, etc., o de dos, o de cuatro, o en general de un numero par de ellos; en la segunda clase, los que son no residuos de uno de los números a, b, c, etc., o de tres etc., o generalmente de un numero impar de ellos. Se denotaran los primeros por r, r', r'', etc.; los ultimos por n, n', n", etc. Entonces las formas Ak + r, Ak + r', Ak + r'', etc. serán formas de los divisores de x2 — A, y las formas Ak + n, Ak + n', etc. serán formas de los no divisores de x2 — A (i.e., un número primo cualquiera, aparte de 2, será divisor o no divisor de x2 — A segUn que esté contenido en alguna de las primeras formas o de las segundas respectivamente). En efecto, si p es un numero primo positivo y un residuo o no residuo de uno de

los números a, b, c, etc., este mismo número será un residuo o un no residuo de p (teorema fundamental). Por lo tanto, si entre los números a, b, c, etc. hay m de los cuales p es un no residuo, otros tantos serán no residuos de p; de donde, si p esta contenido en alguna de las primeras formas, m serú par y ARp, pero si lo esta en alguna de las últimas, m serú impar y ANp.

Ejemplo. Sea A = +105 = (-3)(+5)(-7). Entonces los números r, r', r'', etc. serán estos: 1, 4, 16, 46, 64, 79 (que son no residuos de ninguno de los numeros 3, 5 y 7); 2, 8, 23, 32, 53, 92 (que son no residuos de los numeros 3 y 5); 26, 41, 59, 89, 101, 104 (que son no residuos de los números 3 y 7); 13, 52, 73, 82, 97, 103 (que son no residuos de los numeros 5 y 7). Los números n, n', n'', etc. serán estos: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Los primeros seis son no residuos de 3, los seis posteriores no residuos de 5, luego siguen los no residuos de 7 y finalmente los que son no residuos de todos los tres a la vez.

Se deduce facilmente de la teoría de combinaciones y de los artículos 32 y 96, que el numero de enteros r, r', r'', etc. sera:

— t(1 +

1(1 - 1)  
1 · 2

+ i(i - 1)(/ - 2)(1 - 3) 1 · 2 · 3 · 4

+ ···)

el número de enteros n, n', n'', etc. sera:

+ ···)

— t(i +1(1 - W - 2)

123

+ 1(1 - 1)---(1 - 4) + 1-2---5

donde i denota el número de enteros a, b, c, etc.;

t = 2 l(a - 1)(b - 1)(c - 1) etc.

y se deben continuar ambas series hasta que se paren. (En efecto, se presentaran t números que son residuos de todos los a, b, c, etc., t ^ que son no residuos de dos, etc., pero la brevedad no permite explicar esta demostraciún ampliamente). La suma[[132]](#footnote-133)) de cada una de las series es = 21-1. De hecho, la primera proviene de esta

+···

1 + (i - 1) +

(i - 1)(l - 2)  
1 · 2

sumando el segundo y tercer túermino, el cuarto y el quinto etc.; la segunda se deriva de esta misma, sumando el primer túermino y el segundo, el tercero y el cuarto etc. Por tanto se presentarán tantas formas divisores de x2 - A como se presentan formas no divisores, a saber ^(a - 1)(b - 1)(c - 1) etc.

149.

Podemos contemplar a la vez el segundo y tercer caso. De hecho A siempre puede ponerse = (—1)Q, o = (+2)Q, o = (—2)Q, donde Q designa un número de la forma + (4n + 1), o — (4n — 1), los cuales consideramos en el artículo precedente. Sea en general A = aQ de manera que tambien α = —1o α = ±2. Entonces A sera un residuo de todos los números de los cuales ambos α y Q son residuos, o ambos no residuos; pero sera un no residuo de todos los números de los cuales únicamente uno u otro de los numeros α y Q es un no residuo. De esto, las formas de los divisores y de los no divisores de x2 — A se derivan facilmente. Si α = —1, se distribuyen todos los números menores que 4A y primos al mismo en dos clases: en la primera, los que estan en alguna forma de los divisores de x2 — Q y a la vez de la forma 4n +1, junto con los que estan en alguna forma de los no divisores de x2 — Q y al mismo tiempo de la forma 4n + 3; en la segunda, todos los demás. Sean los miembros de la primera clase r, r', r'', etc.; los de la segunda n, n', n", etc. A sera un residuo de todos los números primos contenidos en alguna de las formas 4Ak + r, 4Ak + r', 4Ak + r'', etc. y un no residuo de todos los nuúmeros primos contenidos en alguna de las formas 4Ak + n, 4Ak + n', etc. Si α = ±2, distribúyanse todos los números menores que 8Q y primos al mismo, en dos clases: en la primera, los que estan contenidos en alguna forma de los divisores de x2 — Q y a la vez en alguna de las formas 8n + 1 y 8n + 7 para el signo superior, o de las formas 8n + 1 y 8n + 3 para el inferior, junto con los que estún contenidos en alguna forma de los no divisores de x2 — Q y al mismo tiempo en alguna de estas formas 8n + 3 y 8n + 5 para el signo superior, o de estas 8n + 5 y 8n + 7 para el inferior; en la segunda clase, todos los demas. Entonces, denotados los números de la primera clase por r, r', r'', etc., y los números de la segunda clase por n, n', n'', etc., ±2Q sera un residuo de todos los números primos contenidos en alguna de las formas 8Qk + r, 8Qk + r', 8Qk + r'', etc.; pero un no residuo de todos los primos en alguna de las formas 8Qk + n, 8Qk + n', 8Qk + n'', etc. Ademas, puede demostrarse fúcilmente que aquí tambien hay tantas formas divisores de x2 — A como no divisores.

Ejemplo. De este modo se encuentra que +10 es un residuo de todos los números primos contenidos en alguna de las formas 40k + 1, 3, 9, 13, 27, 31, 37, 39; pero un no residuo de todos los primos contenidos en alguna de las formas 40k + 7, 11, 17, 19, 21, 23, 29, 33.

150.

Estas formas tienen muchas propiedades bastante notables, de las cuales, sin embargo, indicamos únicamente una. Si B es un número compuesto, primo a A, tal que 2m de sus factores primos esten contenidos en alguna forma de los no divisores de x2 — A, B estarú contenido en alguna forma divisor de x2 — A; pero si el numero de factores primos de B contenidos en alguna forma de los no divisores de x2 — A es impar, B tambien estarú contenido en una forma de los no divisores. Omitimos la demostración que no es difícil. De esto, sigue que no súlo cada número primo sino tambien todo número impar primo a A, que estú contenido en alguna forma de los no divisores, serúa un no divisor, pues necesariamente alguún factor primo de tal nuúmero debe ser un no divisor.

Sobre los trabajos de otros acerca de estas investigaciones.

151.

El teorema fundamental, que ha sido considerado como uno de los maús elegantes de este genero, no ha sido presentado hasta ahora en la forma tan simple como estú enunciado arriba. Esto tiene que sorprendernos aún mas; ya que otras proposiciones fundamentadas en el, de las cuales hubiera podido deducirse fácilmente el teorema, ya eran conocidas por el ilustre Euler. Sabúa que existen ciertas formas en las cuales estan contenidos todos los divisores primos de los números de la forma x2 — A, y otras formas en las cuales estún comprendidos todos los no divisores primos de los mismos números, de tal manera que unas excluyan las otras y habúa descubierto un metodo para hallar estas formas. Pero todos sus esfuerzos para hallar una demostracion fueron en vano, y solo diú un poco de validez a lo que habúa descubierto por inducciún. En una memoria titulada Novae demostrationes circa divisores numerorum formae xx + nyy, que fue presentada en la academia de San Petersburgo el 20 de noviembre de 1775, y que fue conservada despues de la muerte de este hombre ilustre en T. I. Nov. Act. de esta academia p. 47 y siguientes, parece haber creúdo que habúa logrado sus propúsitos, pero se cometiú un error. En efecto en la p. 65 esta supuesto túcitamente que existen tales formas de los divisores y de los no divisores[[133]](#footnote-134)), de donde no era difícil derivar cuales deben ser; pero el metodo que

él uso para comprobar esta proposición no parece idóneo. En otra obra, De criteriis aequationis fxx + gyy = hzz utrumque resolutionem admittat necne, Opusc. Anal. T. I. (donde f, g, h son dados, x, y, z indeterminados) el descubrio por induccion que si la ecuacion era resoluble para algun valor de h = s, tambien era resoluble para todo valor primo congruente a s segun el modulo 4fg. De esta proposicion, la suposicion sobre la cual hemos hablado puede demostrarse sin mucha dificultad. Pero la demostracion de este teorema tambien eludio sus esfuerzos[[134]](#footnote-135)), lo cual no es raro ya que a nuestro juicio se debía proceder a partir del teorema fundamental. Ademas, la verdad de esta proposicion saldrá con espontaneidad de lo que enseñaremos en la siguiente seccion.

Despues de Euler, el gran Lagrange trabajo activamente en el mismo argumento en el distinguido tratado Recherches d’analyse indéterminée, Hist.de l’Ac. des Sc., 1785, p. 465 y los siguientes, donde llego al teorema que si se observa es identico al teorema fundamental. En efecto, al designar p y q dos numeros primos

... , . . q — 1 p — 1 y

positivos, los residuos absolutamente mínimos de las potencias p~2 y q~r segun los modulos q y p respectivamente serán ambos +1 o ambos —1 cuando p o q sea de la forma 4n + 1. Pero cuando tanto p como q sean de la forma 4n + 3, un residuo mínimo sera +1, y el otro —1, p. 516, de lo que, segun el artículo 106, se deriva que la relación (en el significado del art. 146) de p a q y de q a p es la misma cuando o p o q sea de la forma 4n +1; la opuesta cuando tanto p como q sean de la forma 4n + 3. Esta proposicion esta contenida entre las proposiciones del artículo 131 y sigue tambien de las proposiciones 1, 3 y 9 del art. 133; alternativamente el teorema fundamental puede derivarse de ella. El gran Legendre tambien intento una demostracion, sobre la cual, puesto que es muy ingeniosa, hablaremos ampliamente en la siguiente seccion. Sin embargo, ya que en ella se suponen muchas cosas sin demostracion (como el mismo confiesa p. 520: Nous avons supposé seulement etc.), algunas de las cuales hasta ahora no han sido demostradas por nadie, y otras, segun nuestro juicio, no pueden demostrarse sin el teorema fundamental mismo, parece que el metodo que siguio no se puede llevar a su fin, y que nuestra demostracion tendrá que ser la primera. Ademas mas abajo presentaremos otras dos demostraciones del

importante teorema, diferentes de la anterior y diferentes entre sí.

Sobre las congruencias no puras del segundo grado.

152.

Hasta este momento hemos tratado la congruencia pura x2 ξ A (mod. m) y hemos enseñado a determinar si es resoluble o no. La investigación de las raíces mismas se reduce por el artículo 105 al caso donde m o es primo o la potencia de un primo; pero el segundo por art. 101 se reduce al caso donde m es primo. Para este caso, lo que presentamos en el artículo 61 y siguientes junto con lo que enseñaremos en las Secciones V y VIII, comprende todo lo que puede hacerse por metodos directos. Sin embargo, estos son infinitamente más prolijos donde son aplicables que los indirectos que ensenñaremos en la Seccion VI, y por tanto son memorables no tanto por su utilidad en la practica sino por su propia belleza. Las congruencias no puras del segundo grado facilmente pueden reducirse a las puras. Dada la congruencia

ax + bx + c ξ 0

para resolverse segun el modulo m, equivaldrá a la congruencia

4a2 x2 + 4abx + 4ac ξ 0 (mod. 4am)

i.e., cualquier numero que satisfaga una de ellas tambien satisfará la otra. Pero esta segunda puede ponerse de la forma

(2ax + b)2 ξ b2 — 4ac (mod. 4am)

de donde todos los valores de 2ax + b menores que 4am pueden encontrarse si es que existen. Si designamos estos por r, r', r'', etc., todas las soluciones de la congruencia propuesta podran deducirse de las soluciones de las congruencias

2ax *ξ* r — b, 2ax *ξ* r' — b, etc. (mod. 4am)

las cuales aprendimos a encontrar en la Seccion II. Ademas, observamos que la solucion puede acortarse bastante mediante varios artificios; por ejemplo, en lugar de la congruencia propuesta puede encontrarse otra

a'x2 + 2b'x + c' ξ 0

que le sea equivalente, y en la cual a! divida a m; la brevedad no permite aquí explicarlo, pero puede referirse a la ultima sección.

Sección Quinta

SOBRE

LAS FORMAS Y LAS ECUACIONES INDETERMINADAS  
DE SEGUNDO GRADO.

Propósito de la investigación: definición y notación de las formas.

153.

En esta sección, trataremos principalmente las funciones de dos indetermi­nadas x e y de esta forma:

ax + 2bxy + cy

donde a, b y c son enteros dados. Llamaremos a estas funciones formas de segundo grado o simplemente formas. En esta investigation se basa la resolution del famoso problema de encontrar todas las soluciones de cualquier ecuacion indeterminada del segundo grado involucrando dos incognitas, donde estas incógnitas pueden asumir tanto valores enteros como racionales. Este problema ciertamente ya fue resuelto por el ilustre Lagrange con toda generalidad. Ademós, muchos aspectos de la naturaleza de las formas, como la construccioón de demostraciones, fueron encontrados tanto por este gran geómetra como por el ilustre Euler y antes por Fermat. Sin embargo, mediante una cuidadosa investigacioón de las formas, se nos presentaron tantos detalles nuevos que juzgamos valioso el trabajo de retomar completamente todo el argumento; primero, porque hemos conocido los descubrimientos difundidos en varios lugares por aquellos hombres, segundo, porque el metodo para tratar esto es, en su mayor parte, propio a nosotros, y, finalmente, porque nuestros nuevos hallazgos ciertamente no podrón comprenderse sin una exposition de los otros. Nos parece que no hay duda alguna de que muchos excelentes resultados de este genero todavía estón ocultos a

quienes se interesan en esta materia. Además, siempre presentaremos la historia de las proposiciones importantes en el lugar apropiado.

Cuando no nos conciernen las indeterminadas x e y, denotaremos por (a, b, c) a la forma ax2 + 2bxy + cy2. Por lo tanto, esta expresión denotará de manera indefinida una suma de tres partes: el producto del námero dado a por un cuadrado indeterminado cualquiera, el producto del duplicado del nuámero b por esta indeterminada y otra indeterminada, y el producto del námero c por el cuadrado de esta segunda indeterminada. E.g., (1, 0, 2) expresa la suma de un cuadrado y el duplicado de un cuadrado. Ademas, aunque las formas (a,b,c) y (c,b,a) denotan lo mismo, si solo se consideran sus términos, difieren, sin embargo, si tambien prestamos atencion al orden. Por esto las distinguiremos con cuidado en lo que sigue; mas adelante se pondraá en claro lo que ganamos con esto.

Representación dé los numeros; él determinante.

154.

Diremos que un námero dado se representa por una forma dada si se puede dar valores enteros a las indeterminadas de la forma de modo que sea igual al námero dado. Tendremos el siguiente:

TEOREMA. Si el numero M puede representarse por la forma (a, b, c) de manera que los valores de las indeterminadas, por los que esto se produce, son primos entre si, entonces b2 — ac será un residuo cuadrático del número M.

Demostracion. Sean m y n los valores de las indeterminadas; i.e.,

22 am2 + 2bmn + cn2 = M

y tomense los námeros μ y v de modo que sea pm + vn = 1 (art. 40). Entonces por multiplicacián puede demostrarse facilmente:

/2 2\/2 2 \

(am2 + 2bmn + cn2)(av2 — 2bpv + cp )

= (p(mb + nc) — v (ma + nb))2 — (b2 — ac)(mp + nv )2

o sea

M (av2 — 2bpv + cp2) = (p(mb + nc) — v (ma + nb))2 — (b2 — ac).

Por lo tanto será

b2 — ac = (μ(mb + nc) — v(ma + nb))2 (mod. M)

i.e., b2 — ac será un residuo cuadrático de M.

Llamaremos al námero b2 — ac, de cuya índole dependen las propiedades de la forma (a,b,c), tal como lo enseñaremos en lo siguiente, el determinante de esta forma.

Los valores de la expresión Vb2 — ac (mod. M)  
a los cuales pertenece la representación del número M por la forma (a,b,c).

155.

Así

p(mb + nc) — v (ma + nb)

sera un valor de la expresión

b2

— ac (mod. M)

Pero es claro que los numeros μ y v pueden determinarse de infinitas maneras de modo que μm + vn = 1, y así producirán unos y otros valores de esta expresion. Veremos que relacion tienen entre sí. Sea no solo μm + vn = 1 sino tambien μ'm + v'n = 1 y pongase

μ(mb + nc) — v(ma + nb) = v, μ' (mb + nc) — ν' (ma + nb) = v'.

Multiplicando la ecuacion μm+vn = 1 por μ', la otra μ'm + Vn = 1 por μ, y restando sera μ' — μ = n(^ v — μν'), y al mismo tiempo multiplicando aquella por ν' y esta por v, restando sera v' — v = m^v' — μ'ν). De esto inmediatamente resulta

v — v = (μ'ν — μν ')(am2 + 2bmn + cn2) = (μ'ν — μv')M

o sea, v' = v (mod. M). Por lo tanto, de cualquier modo que se determinen μ y v, la formula μ(mb + nc) — v(ma + nb) no puede presentar valores diferentes (i.e., no congruentes) de la expresion Vb2 — ac (mod. M). Así pues, si v es un valor cualquiera de esta formula, diremos que la representacion del numero M por la forma

ax2 + 2bxy + cy2 donde x = m e y = n, pertenece al valor v de la expresión y/ti^—ac (mod. M). Además puede mostrarse fácilmente que, si algún valor de esta fórmula fuera v y v' = v (mod. M), se puede tomar en lugar de los números μ y ν que dan v los otros μ' y ν' que dan v'. En efecto, si se hace

μ' = μ +

n(v' — v)

M

ν = ν —

m(v' — v)

M

serúa

μ^ + ν'η = μm + νη = 1

y el valor de la formula producido por μ' y ν' excederá el valor producido por μ y ν en la cantidad (μ'ν — μν')M, que es = ^m + v«)(v' — v) = v' — v o sea aquel valor seró = v'.

156.

Si se tienen dos representaciones de un mismo numero M por una misma forma (a, b, c) en las cuales las indeterminadas tienen valores primos entre sí, ellas pueden pertenecer o al mismo valor de la expresión y/b2 — ac (mod. M) o a valores diferentes. Sea

1. 2 »2 / i /2

M = am2 + 2bmn + cn2 = am + 2bm n + cn

y

Es claro que si

μ( mb + nc)

I 1 / / | / / 1

μm + νπ = 1, μm + νn =1

ν (ma + nb)

μ'^^ + n'c) — ^(m'a + n'b) (mod. M)

entonces la congruencia siempre permanecerá valida, cualesquiera que sean los valores apropiados para μ y ν, μ' y ν'. En tal caso decimos que ambas representaciones pertenecen a un mismo valor de la expresión \/b2 — ac (mod. M); pero si la congruencia no vale para algunos valores de μ y ν, μ' y ν', no valdró para ninguno, y diremos que las representaciones pertenecerán a valores diferentes. Pero si

(μ' (m'b + n'c) — ν' (m'a + n'b))

μ(mb + nc) — ν (ma + nb)

se dice que las representaciones pertenecen a valores opuestos de la expresion b2

— ac. Tambien se usaran todas estas denominaciones cuando se tratan de varias representaciones de un mismo número por formas diferentes, pero que tienen el mismo determinante.

Ejemplo. Sea propuesta la forma (3, 7, -8) cuyo determinante es = 73. Por esta forma se tendrán estas representaciones del número 57:

1. · 132 + 14 · 13 · 25 - 8 · 252; 3 · 52 + 14 · 5 · 9 - 8 · 92

Para la primera, puede ponerse μ = 2, ν = -1 de donde resulta el valor de la

expresión λ/73 (mod. 57) a la cual pertenece la representaciúon

= 2(13 · 7 - 25 · 8) + (13 · 3 + 25 · 7) = -4

De modo semejante se descubrirá que la segunda representacion, al hacer μ = 2, ν = -1, pertenece al valor +4. Por lo cual las dos representaciones pertenecen a valores opuestos.

Antes de proseguir, observamos que las formas de determinante = 0 estún excluidas totalmente de las investigaciones siguientes. De hecho, ellas perturban uúnicamente la elegancia de los teoremas ya que exigen un tratamiento particular.

Una forma que implica otra o contenida en ella; la transformación propia e impropia.

157.

Si la forma F, cuyas indeterminadas son x e y, puede transmutarse en otra, F', cuyas indeterminadas son x' e y0 por las sustituciones

x = ax + ey , y = γx' + óy

de modo que α, β, γ, δ sean enteros; diremos que la primera implica la segunda o que la segunda está contenida en la primera. Sea F la forma

22 ax2 + 2bxy + cy ,

F la forma

22

a x + 2b x y + cy

y se tendrán las tres ecuaciones siguientes

22 a = aa2 + 2baγ + cγ

b' = ααβ + b(aó + βγ) + cγδ

c = αβ2 + 2beó + có2

Multiplicando la segunda ecuación por si misma, la primera por la tercera, restando y removiendo las partes canceladas, resultara

b/2 — a'c' = (b2 — αο)(αδ — βγ)2

De donde se deduce que el determinante de la forma F' es divisible por el determinante de la forma F y el cociente de ellos es un cuadrado. Por lo tanto es claro que estos determinantes tendrán el mismo signo. Además, si la forma F' puede transmutarse por una sustitucián similar en la forma F, i.e., si tanto F' esta contenida en F como F está contenida en F', los determinantes de las formas serán iguales[[135]](#footnote-136)) y (αδ — βγ)2 = 1. En este caso diremos que las formas son equivalentes. Por esto, para la equivalencia de formas, la igualdad de los determinantes es una condicion necesaria, aunque aquella no se deduzca solo de esta.— Llamaremos a la sustitucion x = aX + βy/, y = γΧ + δy/ una transformación propia, si αδ — βγ es un námero positivo, impropia si αδ — βγ es negativo. Diremos que la forma F' esta contenida en la forma F propiamente o impropiamente si F puede transmutarse en la forma F/ por una transformacián propia o impropia. Asi si las formas F y F' son equivalentes, será (αδ — βγ)2 = 1, asi que si la transformacián es propia, αδ — βγ = 1, si es impropia, αδ — βγ = —1. Si varias transformaciones son al mismo tiempo propias, o al mismo tiempo impropias, las llamaremos semejantes; sin embargo, una propia y una impropia se llaman desemejantes.

La equivalencia propia e impropia.

158.

Si los determinantes de las formas F y F' son iguales y si F' estó contenida en F, entonces F estaró contenida en F', propia o impropiamente, segón que F' estó contenida en F propia o impropiamente.

Consideremos que F se transforma en F' poniendo

x = αχ0 + βy/, y = γχ0 + δy/

y F' se transformará en F poniendo

X = δχ — βy, y0 = —γχ + αy.

En efecto, por esta sustitución resulta lo mismo de F' que de F al poner

x = α(δχ — βy) + β(-γχ + ay), y = γ(δχ — βy) + δ(-γχ + ay)

o sea

x = (αδ — βγ)χ, y = (αδ — βγ )y

De esto queda manifiesto que F se hace (αδ — βγ)2F, i.e., de nuevo, F (artículo anterior). Tambien esta claro que la segunda transformación sera propia o impropia, segun que la primera sea propia o impropia.

Si tanto F' estó contenida propiamente en F como F lo estó en F', las llamaremos formas propiamente equivalentes; si alternativamente estón contenidas impropiamente, las llamaremos impropiamente equivalentes.— En lo restante, se vera pronto el uso de estas distinciones.

Ejemplo. La forma 2x2 — 8xy + 3y2 se cambia, por la sustitucion x = 2x0 + y0, y = 3x0 + 2y0, en la forma — 13x02 — 12x0y0 — 2y02, y esta se transforma en la primera mediante la sustitucion x0 = 2x — y, y0 = —3x + 2y. Por lo que las formas (2, —4, 3) y (—13, —6, —2) son propiamente equivalentes.

Los problemas que ahora trataremos son estos :

1. Propuestas dos formas cualesquiera que tienen el mismo determinante, se debe investigar si son equivalentes o no, si lo son propia o impropiamente o ambas (puesto que esto tambien puede suceder). Cuando tienen determinantes diferentes, se debe investigar por lo menos si la una implica la otra, propia o impropiamente o ambas. Finalmente, se debe hallar todas las transformaciones de la una en la otra, tanto las propias como las impropias.
2. Dada una forma cualquiera, se debe determinar si un nómero dado puede representarse por ella y determinar todas las representaciones. Pero, ya que las formas de determinante negativo requieren otros metodos diferentes que las formas de determinante positivo, primero trataremos lo comón a los dos, y luego consideraremos cada góenero por separado.

Formas opuestas.

159.

Si la forma F implica la forma F0, y ésta implica la forma F00, también la forma F implicara la forma F00.

Sean las indeterminadas de las formas F, F', F00, respectivamente x e y, x0 e y0, x00 e y00, y transfórmese F en F0 al poner

x = αχ0 + py0, y = yx0 + hy0

y F0 en F00 al poner

x = α x + p y , y = y x + o y Es claro que F seró transmutada en F00 al poner

x = a(a0x00 + p 0y00) + p(y0x00 + O0y00), y = y (αΥ0 + p0y00) + O(y0x00 + O0y00)

o

x = (αα0 + Py0)x00 + (ap0 + pO0)y00, y = (ya0 + Oy0)x00 + (yp0 + OO0)y00

Así F implicaró F00.

Porque

(αα0 + Py0)(yP0 + δδ0) — (ap0 + po0)(ya0 + Oy0) = (αδ — Py)(a0O0 — p 0y0)

sera positivo si tanto αδ — py como α0δ0 — p0y0 son positivos o ambos son negativos, y sera negativo si uno de estos numeros es positivo y el otro negativo, la forma F implicara la forma F00 propiamente si F implica F0 y F0 a F00 del mismo modo, e impropiamente si es de modos diferentes.

De esto resulta que si se tienen las formas cualesquiera F, F0, F00, F000, etc., cada una de las cuales implica la siguiente, la primera implicara la ultima propiamente si el numero de formas que implican impropiamente a su sucesor es par, e impropiamente si este numero es impar.

Si la forma F es equivalente a la forma F0 y la forma F0 es equivalente a la forma F00, entonces la forma F será equivalente a la forma F00 propiamente si la forma F equivale a la forma F0 del mismo modo como la forma F0 equivale a la forma F00, e impropiamente si son equivalencias de modos diferentes.

De hecho, ya que las formas F y F0 son respectivamente equivalentes a las formas F0 y F00, entonces aquellas implicaran estas, y así F implica a F00, tanto como las ultimas implican a las primeras. Por lo tanto, F y F00 serán equivalentes. Pero se

sigue de lo anterior que F implicará F'' propiamente o impropiamente, según que la equivalencia de F y F', y F' y F" sea del mismo modo o de modo diferente. De la misma manera F'' implicara F. Por lo tanto, F y F'' serán propiamente equivalentes en el primer caso, e impropiamente equivalentes en el segundo.

Las formas (a, —b, c), (c, b, a), (c, — b, a) son equivalentes a la forma (a, b, c), con las dos primeras impropiamente, con la Ultima propiamente.

Ya que ax2 + 2bxy + cy2 se transforma en ax'2 — 2bx'y' + cy'2, al colocar x =

x' + 0· y', y = 0 · x' — y', esta transformaciún es impropia pues (1)(-1) — (0)(0) = — 1;

22

pero se transforma en cx' +2bx'y'+ay' por la transformación impropia x = 0 · x'+y', y = x' + 0 · y'; y en la forma cx' — 2bx'y' + ay' por la transformaciún propia x = 0 · x' — y', y = x' + 0 · y'.

De esto queda claro que cualquier forma equivalente a la forma (a, b, c) equivaldrá propiamente o a ella misma o a la forma (a, —b,c). Al mismo tiempo, si tal forma implica la forma (a, b, c) o esta contenida en ella misma, ella implicara la forma (a, b, c) o la forma (a, —b, c) propiamente o estará contenida propiamente en una de las dos. Llamaremos a (a, b, c) y (a, —b, c) formas opuestas.

Formas contiguas.

160.

Si las formas (a, b, c) y (a',b,c) tienen el mismo determinante, y si ademús c = a' y b = —b' (mod. c), o sea b + b' ξ 0 (mod. c), llamaremos a estas formas contiguas. Cuando es necesaria una determinaciún mas exacta, diremos que la primera es contigua a la parte primera de la segunda, la segunda a la parte última de la primera.

Así, por ejemplo, la forma (7, 3, 2) es contigua a la parte última de la forma (3, 4, 7); la forma (3, 1, 3) a ambas partes de su opuesta (3, —1, 3).

Formas contiguas siempre son propiamente equivalentes. En efecto la forma ax2 + 2bxy + cy2 se transforma en su contigua por la sustituciún x = —y', y = x' + ^+L·y' (la cual es propia porque 0 · () — (1 · — 1) = 1), como se demuestra fúcilmente con la ayuda de la ecuaciún b2 — ac = b'2 — cc', donde por hipotesis es un entero. Por otra parte, estas definiciones y conclusiones no valen si c = a' = 0. Pero este caso no puede ocurrir aquí mas que en formas cuyo determinante es un cuadrado.

Las formas (a, b, c) y (a',b,c) son propiamente equivalentes si a = a', b ξ b' (mod. a). En efecto, la forma (a, b, c) equivale propiamente a la forma (c, —b, a)(artículo anterior), pero esta última será contigua a la parte primera de la forma

(a,b,c).

Divisores comunes de los coeficientes de las formas.

161.

Si la forma (a,b,c) implica la forma (a',b',c'), cualquier divisor común de los números a, b y c tambiún dividirú a los números a', b' y cC y cada divisor común de los números a, 2b y c dividirá a a', 2b' y c'.

De hecho, si la forma ax2 + 2bxy + cy2 mediante la sustitución x = ax' + βy', y = jx' + óy' se transforma en la forma a'x' + 2b'x'y' + <f y' , se tendrún estas ecuaciones:

aa2 + 2baj + cj2 = a' aaβ + b (aó + βγ) + cjó = b' aβ2 + 2bβδ + có2 = c'

de donde se sigue la proposiciún (para la segunda parte de la proposition, en lugar de la segunda ecuacion se usa 2ααβ + 2b (aó + βγ) + 2cjó = 2b'.)

De esto se deduce que el múximo común divisor de los numeros a, b (2b), c divide al múximo comun divisor de los números a', b' (2b'), c'. Si ademas la forma (a',b',c) implica la forma (a,b,c), i.e., si las formas son equivalentes, el maximo común divisor de los números a, b (2b), c sera igual al maximo común divisor de los números a', b' (2b'), c', puesto que tanto aquel debe dividir a este, como este a aquel. Por eso, si en este caso a, b (2b), c no tienen un divisor comun, i.e., si el maximo comun divisor = 1, tampoco tendra a , b (2b ), c un divisor comun.

El nexo de todas las transformaciones semejantes  
de una forma dada en otra forma.

162.

Problema. Si la forma

AX2 + 2BXY + CY2 ... F

**9** **9**

*implica la forma*

ax2 + 2bxy + cy ... f

y si se da alguna transformación de la primera en la segunda: de ésta se deducen todas las transformaciones restantes semejantes a esta misma.

Solución. Sea la transformación dada X = αχ + βy, Y = γχ + óy. Supongamos primero que la otra semejante a esta es X = a'x + β^, Y = γ'χ + ó'y, de donde investigaremos lo siguiente. Dados los determinantes de las formas F y f = D y d y aó — βγ = e, a'ó' — β'γ' = e', tendremos (art. 157) d = De2 = De'2, y puesto que por hipótesis e y e' tienen los mismos signos, e = e'. Se tendrán así las siguientes seis ecuaciones:

|  |  |
| --- | --- |
| Αα2 + 2Βαγ + Cy2 = α | (1) |
| Αα'2 + 2Βα'γ' + Cy'2 = α | (2) |
| Ααβ + Β(αδ + βγ) + Cyó = b | (3) |
| Αα'β' + Β(α'δ' + β'γ') + Cy'ó' = b | (4) |
| Αβ2 + 2Ββδ + CÓ2 = c | (5) |
| Αβ'2 + 2Ββ'δ' + Có'2 = c | (6) |

Si por brevedad denotamos los nómeros

Aaa + Β (αγ' + γα') + Ογγ'

Α(αβ' + βα') + B(aó' + βγ' + γβ' + δα') + C (γδ' + δγ')

Αββ' + B (βδ' + δβ') + Cóó'

por α', 2b', c', de las ecuaciones precedentes deduciremos otras nuevas\*)

a'2 — D^y' — γα')2 = α2 (7)

2a'b' — D^y' — γα')(αδ' + βγ' — γβ' — δα') = 2ab (8)

4b'2 — D(^ó' + βγ' — γβ' — δα')2 + 2ee') = 2b2 + 2ac

de donde resulta, sumando 2Dee' = 2d = 2b2 — 2ac

4b'2 — D(αó/ + βγ' — γβ' — δα')2 = 4b2 (9)

a'c' — D^ó' — γβ')(βγ' — δα') = b2

\*) Estas ecuaciones se originan así: la (7) viene de (1) · (2) (i.e., si la ecuación (1) se multiplica por la ecuación (2), o mejor, si la parte primera de la primera se multiplica por la parte primera de la segunda, y la parte óltima de la primera por la parte óltima de la segunda, y luego se ponen iguales los productos). La (8) viene de (1) · (4) + (2) · (3); la siguiente, la cual no estó numerada de (1) · (6) + (2) · (5) + (3) · (4) + (3) · (4); la siguiente, sin nómero, de (3) · (4); la (11) de (3) · (6) + (4) · (5);

la (12) de (5) · (6). Siempre usaremos una notación semejante en lo siguiente. Pero debemos dejar

los cóalculos a los lectores.

de donde, restando D(αδ — βγ)(α'δ' — β'γ') = b2 — ac se tiene

a'c' — D(aj' — γα')(βδ' — δβ') = ac (10)

2b' c' — D(a^ + βγ' — γβ' — δα')(βδ' — δβ') = 2bc (11)

c'2 — D(βδ' — δβ')2 = c2 (12)

Ahora supongamos que el máximo común divisor de los números a, 2b, c es m, y los números A, B, C determinados de tal manera que

Aa + 2Bb + Cc = m

(art. 40). Multipliqúense las ecuaciones (7), (8), (9), (10), (11), (12) respectivamente por A2, 2AB, B2, 2AC, 2BC, C2 y sumense los productos. Ahora si por brevedad ponemos

Aa' + 2Bb' + Cc' = T (13)

Α(αγ' — γα') + B(aA' + βγ' — γβ' — δα') + ^βδ' — δβ') = U (14)

donde claramente T y U serian enteros, resultarai

T2 — DU2 = m2

Asi llegamos a esta conclusion elegante: de dos transformaciones semejantes cualesquiera de la forma F en f se deduce la resolución de la ecuación indeterminada t2 — Du2 = m2 en enteros, es decir t = T, u = U. Además como en nuestros razonamientos no hemos supuesto que las transformaciones son diferentes, una transformación tal considerada dos veces debe producir una solución. Entonces, por razón de que α' = α, β' = β, etc., sera a' = a, b' = b, c' = c, por tanto T = m, U = 0, que es una solucián obvia por si misma.

Ahora, primero consideremos conocidas una transformacián y una solucion de la ecuacion indeterminada, y luego investiguemos cámo puede deducirse la otra transformacián y cámo α', β', γ', δ' dependen de α, β, γ, δ, T, U. Para este fin,

multiplicamos primero la ecuacion (1) por δα' — βγ', la (2) por αδ' — γβ', la (3) por αγ' — γα', la (4) por γα' — αγ' y sumamos los productos, de donde resultara

De modo semejante, de

(δβ' - βδ')((1) - (2)) + (αδ' - βγ' - γβ' + δα')((3) + (4)) + (αγ' - γα')((5) - (6)) se tiene

2(e + e')b' = 2(αδ' - βγ' - γβ' + δα)δ (16)

Finalmente, de (δβ' - βδ')((3) - (4)) + (αδ' - γβ')(5) + (δα' - βγ')(6) resultara

(e + e')c' = (αδ' - βγ' - γβ' + δα')c (17)

Sustituyendo estos valores ((15), (16), (17)) en la (13) se obtiene

(e + e')T = (αδ' - βγ' - γβ' + δα')(Αα + 2Bb + Cc)

o

2eT = (αδ' - βγ' - γβ' + δα')m (18)

de donde T puede deducirse con mas facilidad que de la (13). — Combinando

esta ecuación con (15), (16), (17) se obtiene ma' = Ta, 2mb' = 2Tb, mc' = Tc. Sustituyendo estos valores de a', 2b', c' en las ecuaciones (7)-(12) y escribiendo m2 + DU2 en lugar de T2 despues de las alteraciones necesarias se transforman

( f f\ 2 2 2τ *t2*

en estas:

( αγ - γα ) m = a U

(αγ' - γα')(αδ' + βγ' - γβ' - δα')m2 = 2abU2 (αδ' + βγ' - γβ' - δα')2m2 = 4b2U2 (αγ' - γα')(βδ' - δβ')m2 = acU2 (αδ' + βγ' - γβ' - δα')(βδ' - δβ')m2 = 2bcU2

(βδ' - δβ')2m2 = c2U2

De esto con la ayuda de la ecuacion (14) y de Aa + 2Bb + Cc = m, se deduce facilmente (multiplicando la primera, la segunda y la cuarta; la segunda, la tercera y la quinta; la cuarta, la quinta y la sexta respectivamente por A, B, C y sumando los productos):

(αγ' - γα')Um2 = maU2 (αδ' + βγ' - γβ' - δα')Um2 = 2mbU2 (βδ' - δβ' )Um2 = mcU2

y de esto, dividiendo por mU[[136]](#footnote-137))

aU = (αγ0 — γo')m (19)

2bU = (oó' + βγ' — γβ' — óo')m (20)

cU = (βδ' — óe')m (21)

de tales ecuaciones puede deducirse algún U con más facilidad que de la (14). — De modo semejante se concluye que no importa cúmo se determinen A, B, C (porque puede ser de infinitas maneras diferentes), tanto T como U tomarán el mismo valor.

Ahora si la ecuación (18) se multiplica por o, la (19) por 2β, la (20) por —o, la suma da

2aeT + 2(βα — ob)U = 2(oó — βγ)α^ = 2eo'm.

De modo semejante de β(18) + β(20) — 2o(21)

2βeT + 2^b — oc)U = 2(oó — βγ)β'^. = 2eβ'm

Además de γ(18) + 2ó(19) — γ(20) es

2γeT + 2(óa — γb)U = 2(oó — βγ)γ'm = 2eγ'm

Finalmente, de ó(18) + ó(20) — 2γ(21) resulta

2óeT + 2(ób — γφ = 2(oó — βγ)ó'm = 2eó'm

Si en estas formulas se sustituyen para a, b, c sus valores de (1), (3), (5) se obtiene

o'm = oT — (oB + γC)U ^m = βΤ — (βΒ + óC)U γ' m = γΤ + (oA + γΒ^ ó'm = óT + (βΑ + óB)U t)

Del análisis anterior se deduce que no existe ninguna transformación semejante de la forma F en la f que no este contenida en la formula

X = —(at — (aB + *yC)u)x* + (βί — (βΒ + 5C)u)y

m m

Y = —(γί + (aA + γ B)u)x + (δί + (βΑ + SB)u)y

*(I*)

mm

donde t y u denotan nómeros enteros indeterminados que satisfacen la ecuación t2 — Du2 = m2. De esto no hemos podido concluir que todos los valores de t y u que satisfacen aquella ecuación proporcionaran transformaciones adecuadas al sustituirlos en la formula (I). Sin embargo,

1. Por medio de las ecuaciones (1), (3), (5) y t2 — Du2 = m2, puede confirmarse fócilmente que la forma F siempre puede transformarse en la forma f por una sustitucion proveniente de valores cualesquiera de t y u. Por brevedad, suprimimos un calculo mas prolijo que difícil.
2. Cada trasformación deducida de la fórmula seró semejante a la propuesta

porque

— (at — (aB + γ C)u) — ^+(βΑ+δΒ)u) (βt — (βΒ + δC)u) — (Yt+(aA+γ B)u)

m m m m

= —^^δ — βγ)^2 — Du2) = αδ — βγ m2

1. Si las formas F y f tienen determinantes diferentes, puede ocurrir que

la fórmula (I) para algunos valores de t y u produzca sustituciones que impliquen fracciones: estas deben rechazarse. Todas las restantes serón transformaciones

adecuadas y no existiran otras.

1. Si las formas F y f tienen el mismo determinante, y por tanto son equivalentes, la formula (I) no presentara ninguna transformation que implique

fracciones, de donde en este caso dará la solución completa del problema. Esto lo demostramos como sigue:

Del teorema del artículo anterior, resulta en este caso que m será un comán divisor de los numeros A, 2B y C. Ya que t2 — Du2 = m2, es t2 — B2u2 = m2 — ACu2, por lo que t2 — B2u2 será divisible por m2: de esto tambien 4t2 — 4B2u2, y por lo tanto (porque 2B es divisible por m) tambien 4t2 por m2, y por eso 2t por m. De esto (t + Bu) y LL(t — Bu) serán enteros, y ambos son pares o ambos impares (ya que la diferencia entre ellos, LLBu, es par). Si ambos fueran impares, tambien su producto sería impar, pero ya que el cuadruplo del numero (t2 — B2u2), el cual

hemos mostrado como entero, es necesariamente par; entonces este caso es imposible, y por tanto LL(t+Bu) y LL (t — Bu) son siempre pares, de donde L (t+Bu) y L(t—Bu) seran enteros. De esto se deduce sin dificultad que los cuatro coeficientes en la (I) son siempre enteros. Q. E. D.

De lo anterior se concluye que, si se tienen todas las soluciones de la ecuacioán t2 — D2u2 = m2, se derivaran todas las transformaciones de la forma (A,B,C) en (a, b, c) semejantes a la transformacián dada. Desde luego, ensenaremos a encontrar estas soluciones en lo siguiente. Observamos que el námero de soluciones es siempre finito cuando D es negativo o un cuadrado positivo; pero es infinito cuando D es positivo y no un cuadrado. Cuando se presenta este caso, y cuando D no es = d (ver arriba 3), se debe investigar cuidadosamente la manera en que se puedan conocer a priori los valores de t y u que producen sustituciones libres de fracciones. Pero para este caso, expondremos mas adelante otro metodo libre de este problema.

Ejemplo. La forma x2 + 2y2 se transforma por la sustitucián propia x = 2x' + 7y',y = x' + 5y' en la forma (6, 24, 99): se desean todas las transformaciones propias de la primera en la segunda. Aquá D = —2,m = 3, y por lo tanto la ecuacion por resolverse es: t2 + 2u2 = 9. Ella se satisface de seis maneras diferentes poniendo t = 3, —3, 1, —1, 1, —1; u = 0, 0, 2, 2, —2, —2 respectivamente. La tercera y sexta resolucion dan sustituciones en fracciones, por lo que deben rechazarse. De los restantes resultan cuatro sustituciones:

|  |  |  |
| --- | --- | --- |
|  | 2x' + 7y' | x' + 5y' |
|  | 1  to  1  —a | —x' — 5y' |
| x= | — 2x' — 9y' y | x' + 3y' |
|  | 2x' + 9y' | —x' — 3y' |

de las cuales la primera es la propuesta.

Formas ambiguas.

163.

Ya hemos dicho que puede ser que alguna forma F implique otra tanto propia como impropiamente. Es claro que esto ocurre si entre las formas F y F' pudiera interponerse otra, G, de modo que F implique G, G implique F', y la forma G sea impropiamente equivalente consigo misma. Si, en efecto, se supone que F implica G propia o impropiamente: como G implica a G impropiamente, F implicara a G impropia o propiamente respectivamente y, por tanto, en los dos casos tanto propia como impropiamente (art. 159). Del mismo modo, no importa la forma en que se suponga que G implica F0, F siempre debe implicar F' tanto propia como impropiamente. En el caso obvio donde el termino medio de la forma es = 0, se ve que tales formas son impropiamente equivalentes a si mismas. De hecho, tal forma sera opuesta a si misma (art. 159) y por lo tanto impropiamente equivalente. En general cada forma (a, b, c) en la cual 2b es divisible por a está provista de esta propiedad. En efecto, la forma (c, b, a) sera contigua (art. 160) a la primera parte de esta y propiamente equivalente a ella. Sin embargo, (c, b, a) por art. 159 es impropiamente equivalente a la forma (a, b, c); por lo que (a,b,c) equivaldrá a si misma impropiamente. Llamaremos ambiguas a tales formas (a, b, c) en las cuales 2b es divisible por a.

Así tendremos este teorema:

La forma F implicara la forma F' tanto propia como impropiamente, si puede encontrarse una forma ambigua contenida en F que implica a F'. Es evidente que esta proposición tambien puede invertirse:

Teorema sobre el caso en que una forma esta contenida  
en otra al mismo tiempo propia e impropiamente.

164.

Teorema. Si la forma

(F) (F')

Ax2 + 2Bxy + Cy

*implica la forma*

A'x'2 + 2B' xy + Cy02

tanto propia como impropiamente, entonces puede encontrarse una forma ambigua contenida en F y que implica a F'.

Supongamos que la forma F se transforma en la forma F' tanto por la sustitución

χ = αχ' + βy', y = γχ' + óy

como por esta diferente a ella

x = αχ + β y , y = γχ + óy

Entonces, denotados los números αδ — βγ y α'ó' — β'γ' por e y e' se tendrá B'2 — A'C' = e2(B2 — AC) = e'2(B2 — AC); de esto e2 = e'2, y, ya que por la hipotesis e y e' tienen signos opuestos, e = —e' o e + e' = 0. Es claro que si en F' para x' se sustituye δ'χ'' — βΥ', y para y', —γ'χ'' + αΥ' se producirá la misma forma como cuando en la F se escribe

α(δ'χ'' — βΥ') + β(—γ'χ'' + αΥ')

o bien 1) para χ i.e.

y para y i.e.

o bien 2) para χ y para y

(αδ' — βγ' )χ'' + (βα' — αβ' )y''  
γ (δ χ — β y ) + δ(—γχ + αy )

(γδ' — δγ' )χ'' + (δα' — γβ' )y''

α'(δ'χ'' — βΥ') + β'(—γ'χ'' + α'/) i.e., eV

γ (δ χ — β y ) + δ (—γχ + «y ) i.e., ey

Así pues, denotados los números αδ' — βγ', βα' — αβ', γδ' — δγ', δα' — γβ' por α, b, c, d, la forma F se transformara en la misma forma por las dos sustituciones

χ = αχ'' + by'', y = cx'' + dy''; χ = e^'', y = e'y'',

de donde obtendremos las siguientes tres ecuaciones:

|  |  |
| --- | --- |
| Aa2 + 2Bac + Cc2 = Ae'2 | (1) |
| Aab + B (ad + bc) + Ccd = Be'2 | (2) |
| Ab2 + 2Bbd + Cd2 = Ce'2 | (3) |
| Pero de los mismos valores de a, b, c, d se encuentra:  ad — bc = ee' = —e2 = —e'2 | (4) |

De aquí y de d(1) — c(2)

(Aa + Bc)(ad — bc) = (Ad — Bc)e'2

A(a + d) — 0

y por tanto

Además, de (a + d)(2) — b(1) — c(3) se tiene

(Ab + B(a + d) + Cc)(ad — bc) — (—Ab + B(a + d) — Cc)e' y por lo tanto

/2

B(a + d) — 0

Finalmente de a(3) — b(2) obtenemos

(Bb + Cd)(ad — bc) — (—Bb + Ca)e

2

y por lo tanto

C (a + d) — 0

Por esto, como no todos A, B, C pueden ser — 0, sera necesario que a + d — 0, o a — —d.

De a(2) — b(1) tenemos

(Ba + Cc)(ad — bc) — (Ba — Ab)e‘

2

de donde

Ab — 2Ba — Cc — 0. (5)

De las ecuaciones e + e' — 0, a + d — 0, o

αδ — βγ + α'δ' — β'γ' — 0, αδ' — βγ' — γβ' + δα' — 0

resulta (α + α')(δ + δ') — (β + β')(γ + γ') o

(α + α') : (γ + γ') — (β + β') : (δ + δ').

Sea la razán[[137]](#footnote-138)) m : n igual a esta razón con námeros mínimos, de modo que m y n sean primos entre sí, y se toman μ, ν de manera que μm + vn — 1. Ademas sea r el

máximo común divisor de los números a, b, c, cuyo cuadrado divida a2 + bc, o bc — ad, o e2; por lo que r también dividirú a e. Determinado esto así, si se supone que la forma F se transforma por la sustituciún

ve ae

x = mt + u, y = nt u

en la forma Mt2 + 2Ntu + Pu2 (G), esta serú ambigua e implicara la forma F0.

Demostración. I. Para que sea evidente que la forma G es ambigua, mostraremos

M (ba2 — 2αμν — cv2) = 2Nr

de donde, ya que r divide a a,b,c, entonces 1 (b^2 — 2αμν — cv2) sera un entero, y por lo tanto 2N un multiplo de M. De hecho tenemos:

M = Am2 + 2Bmn + Cn2, Nr = (Amv — B(ma — nv) — Cna)e (6)

Ademús se confirma mediante calculos fúciles que

2e + 2a = e — e' + a — d = (α — α')(δ + δ') — (β — β 0)(γ + γ0)

2b = (α + α')(β — β0) — (α — α')(β + β')

De esto, puesto que m(γ + γ0) = n^ + α0), m(δ + δ0) = n^ + β') sera

m(2e + 2a) = —2nb o

me + ma + nb = 0 (7)

Del mismo modo encontramos que

2e — 2a = e — e0 — a + d = (α + α0)(δ — δ0) — (β + β 0)(γ — γ0)

2c = (γ — γ0)(δ + δ0) — (γ + γ 0)(δ — δ0)

y de esto n(2e — 2a) = —2mc o

ne — na + mc = 0 (8)

Ahora si se suma m2(bμ2 — 2aμv — cv2) a (1 — mμ — nv )(mv (e — a) + ^μ + 1) b) + (me + ma + π^^μν + v) + (ne — na + mc)mv2

que evidentemente = 0 pues

1. — μιη — vn = 0, me + ma + nb = 0, ne — na + mc = 0

al desarrollar los productos y remover las partes canceladas, resulta 2mve + b. Por lo cual sera

m2(b^2 — 2αμv — cv2) = 2mve + b (9)

Del mismo modo sumando a mn(bμ2 — 2αμν — cv2) lo siguiente:

(1 — mμ — nv )((nv — mμ)e — (1 + mμ + nv )a) — (me + ma + nb)m^2 + (ne — na + mc)nv2

se encuentra

mn(bμ2 — 2aμv — cv2) = (nv — m^)e — a (10)

Finalmente sumando a ^ψμ — 2αμv — cv2) lo siguiente:

(mμ + nv — 1)(nμ(e + a) + (nv + 1)c) — (me + ma + nb)nμ2 — (ne — na + mc)(nμv + μ) obtenemos

n2^2 — 2aμv — cv2) = —2nμe — c (11)

Ahora se deduce de la (9), la (10) y la (11) que

(Am2 + 2Bmn + Cn2)^2 — 2αμv — cv2)

= 2e(Amv + B(nv — m-μ) — Cnμ) + Ab — 2Ba — Cc

o por la (6),

M^μ2 — 2αμv — cv2) = 2Nr. Q. E. D.

1. Para demostrar que la forma G implica la forma F0, demostraremos primero, que G se transforma en F0 al poner

(S)

t = (μα + vq)x0 + (μβ + ví)y0,

u = - (na — mq)x0 +— (ne — mí)y0

segundo, que e («α — mq) y e (ne — mí) son enteros.

1. Puesto que F se transforma en G al ponerse

ve μe

x = mt + u, y = nt u

la forma G se transformará por la sustitución (S) en la misma forma en que se transforma F al ponerse

x = m((^a + vj)x' + (μβ + vá)y') + ν ((ηα — mj )x' + (ηβ — mó)y') i.e., = α^μ + ην )x' + β(mμ + ην )y' o = ax0 + βy'

y y = η((μα + vj)x' + (μβ + vó)y') — μ((ηα — mj )x' + (ηβ — mó)y')

i.e., = γ(ην + m^)x' + δ(ην + mμ)y' o = jx' + áy'

Mediante esta sustitución F se transforma en F'; por lo tanto G se transformaró en F' por la sustitución (S).

2. De los valores de e, b y d se encuentra a'e + jb — ad = 0, o, ya que d = —a, ηαΑ + ηαα + n7b = 0; de esto, usando la (7), ηα^ + ηαα = mje + mja o

(ηα — mj )a = (mj — na')e (12)

Ademós, α^ = —am(e + a), jmb = —m(a'e + αα) y por lo tanto

(ηα — mj)b = (α' — α)me (13)

Finalmente, j'e — ja + ac = 0; de esto multiplicando por η y sustituyendo para ηα su valor de (8) obtenemos

(ηα — mj )c = (j — j' ^e (14)

De modo semejante se saca e'e + áb — ed = 0 o sea nβ'e + η^ + ηβα = 0, y, por lo tanto, por la (7), ηβ'e + ηβα = máe + máa o

(ηβ — má)a = (má — nβ')e (15)

Ademós βη = —βm(e + a), ámb = —m(β'e + βα) y por tanto

(ηβ — má)b = (β' — β)me (16)

Finalmente á'e — δα + βc = 0; de esto multiplicando por η y sustituyendo ηα por suvalor de la (8):

Ahora, como el máximo común divisor de los números a, b, c es r, pueden encontrarse enteros A, B, C de modo que

Aa + Bb + Cc = r

Hecho esto, de la (12), la (13), la (14); la (15), la (16) y la (17) se obtiene

r

A(m-7 — na') + B (a' — a)m + C(7 — γ')η = - (na — m'y)

A (mó — ηβ') + Β(β' — β)m + C(ó — ó')n = - (ηβ — mó)

y por lo tanto e (na — mj), e (ηβ — mó) son enteros. Q. E. D.

165.

Ejemplo. La forma 3x2 + 14xy — 4y2 se transforma en — 12x'2 — 18x'y' + 39y'2, tanto propiamente, con poner

x = 4x' + 11y', y = — x — 2y ,

como impropiamente, con poner

x = —74x' + 89y', y = 15x' — 18y'

Aquí, por lo tanto, a + α', β + β', γ + γ', ó + ó' son —70, 100, 14, —20; y —70 : 14 = 100 : —20 = 5 : —1. Así, pongamos m = 5, n = —1, μ = 0, ν = —1. Los números a, b, c son —237, —1170, 48, de los cuales el maximo comun divisor = 3 = r; finalmente e = 3. De esto la transformación (S) sera x = 5t — u, y = —t. Por ella la forma (3, 7, —4) se transforma en la forma ambigua t2 — 16tu + 3u2.

Si las formas F y F' son equivalentes, entonces la forma G contenida en la forma F tambien estará contenida en F'. Sin embargo, puesto que tambien implica la misma forma F', sera equivalente a ella y por tanto tambien a la forma F. Por lo tanto, en este caso el teorema se enuncia asú:

Si F y F' son equivalentes tanto propia como impropiamente, podrá encon­trarse una forma ambigua equivalente a las dos. Ademas en este caso e = ±1, y por lo tanto r que divide a e, será = 1.

Lo anterior es suficiente acerca de la transformaciúon de las formas en general; así que pasaremos a la consideracion de las representaciones.

Generalidades sobre las representaciones de los números  
por las formas y su nexo con las transformaciones.

166.

Si la forma F implica la forma F', cualquier número que puede representarse por F' también podrá ser representado por F.

Sean x e y, x' e y' las indeterminadas de las formas F y F' respectivamente, y supongamos que se representa al número M por F'. Al hacer x' = m e y' = n, la forma F se transforma en F' por la sustituciún

x = ax' + βy', y = jx' + 6y'

Entonces, evidentemente, si se pone

x = am + βη, y = γm + δη

F se transforma en M.

Si M puede representarse de varias maneras por la forma F', e.g. poniendo x' = m' e y' = n', seguirún varias representaciones de M por F. De hecho, si fuera tanto

am + βη = am + βη como γ m + δη = jm' + δη

sería o bien αδ — βγ = 0, y por lo tanto tambien el determinante de la forma F = 0 (contrariamente a la hipótesis), o bien m = m', η = η'. De esto resulta que M puede representarse al menos de tantas maneras diferentes por F como por F .

Por ende, si tanto F implica F' como F' implica F i.e., si F y F' son equivalentes, y el nuúmero M puede representarse por una de las dos, tambiúen puede representarse por la otra, de tantas maneras diferentes para la una como para la otra.

Finalmente, observamos que en este caso el maximo común divisor de los números m y η es igual al múximo común divisor de los números am + βη y jm + δη. Sea aquel = Δ, y tomemos los numeros μ y v de modo que resulte pm + νη = Δ. Entonces, tendremos

(δμ — jv)(am + βη) — (βμ — av )(jm + δη) = ^δ — βγ)(μm + νη) = ±Δ

De esto, el maximo común divisor de los números am + βη y jm + δη dividirá a Δ, y tambien Δ lo dividira a el; pues, evidentemente dividirá a am + βη y jm + δη. Por lo que, necesariamente aquel sera = Δ. Por lo tanto, cuando m y η son primos entre sí, tambien am + βη y jm + δη lo serán.

167.

Teorema. Si las formas

ax2 + 2 bxy + cy2 (F)

t /2 . 0,/ i i i / /2 / j-,/\

ax +2bxy + cy (F )

son equivalentes, el determinante de ellas = D, y la última se transforma en la primera al poner

x = ax + βy, y0 = γχ + óy

y si además el número M se representa por F, escribiendo x = m, y = n, y, por lo tanto, por F' haciendo

x = am + βη = m0, y0 = γ m + ón = n0

de modo que m sea primo a n y por tanto también m0 a n', entonces ambas representaciones pertenecemn o al mismo valor de la expresión \JD (mod. M) o a valores opuestos segUn que la transformacién de la forma F0 en F sea propia o impropia.

Demostracion. Se determinarán los números μ y ν de manera que resulte pm+vn = 1 y pongase

δμ — γν r -βμ + αν ,

αδ — βγ P , αδ — βγ

(los cuales serán enteros pues αδ — βγ = ±1). Entonces tendremos

1. (cf. final del artículo anterior)

p'm' + v0n0

Además sea

p(bm + cn) — v (am + bn) = V, p0(b0m0 + c0n0) — v0(a0m0 + b0n0) = V0

y V y V0 serán valores de la expresión \[D (mod. M) a los cuales pertenecen la primera y la segunda representaciones. Si en V0 para μ0, v0, m0, n0 se sustituyen los valores de ellos, pero en V

para a, α0α2 + 2^αγ + ^γ2

para b, α0αβ + ^(αδ + βγ) + ^γδ

para c, a^2 + 2^βδ + c0ó2

se encontrará por cálculo que V = V'(aó — βγ).

Por esto tendremos o bien V = V' o V = —V' segun que αδ — βγ = +1 o = —1, i.e., las representaciones pertenecerán al mismo valor de la expresión \JD (mod. M) o a los valores opuestos, segán que la transformation de F' en F sea propia o impropia. Q. E. D.

Si de esta manera se tienen varias representaciones del námero M por la forma (a,b,c) por medio de valores primos entre si de las indeterminadas pertenecientes a valores diferentes de la expresián \[D (mod. M), entonces las representaciones correspondientes por la forma (a',b',c') pertenecerán a los mismos valores respectivos. Si no existe representaciáon alguna del nuámero M por ninguna forma perteneciente a un cierto valor del determinante, tampoco existiraá ninguna otra perteneciente a este valor y equivalente a el.

168.

TEOREMA. Si el número M se representa por la forma ax2 + 2bxy + cy2, asignando los valores m y n primos entre sí a x e y, y si el valor de la expresiún \[D (mod. M), al cual pertenece esta representación, es N, entonces las formas *(a,b,c)* y *(M,* *N,* *NM*-'D) serún propiamente equivalentes.

Demostracion. Es claro que, por el artículo 155, pueden encontrarse námeros enteros μ y v de modo que

mp + nv = 1, μ(bm + cn) *—* v (am + bn) = N.

Usando esto, la forma (a, b, c) se transforma mediante la sustitucián x = mx' — vy' e y = nx' + μψ, la cual claramente es propia, en una forma cuyo determinante es = D(mp + nv)2, i.e., = D, o en una forma equivalente. Tal forma, si se pone

= (M',N nm7D), ser+

M' = am2 + 2bmn + cn2 = M, N' = *—*mva + (mp *—* nv )b + npc = N.

Por lo que la forma en la cual se transforma (a, b, c) por esta transformacián será (M,N, ). Q.E.D.

Además, de las ecuaciones

mp + nv = 1, p(mb + nc) — v (ma + nb) = N

se deduce

*μ*

nN + ma + nb  
am2 + 2bmn + cn2

nN + ma + nb mb + nc — mN

M , V = M

las cuales serán, por lo tanto, números enteros.

Además, hay que notar que esta proposición no vale si M Nserá indeterminado\*).

0; pues el termino

169.

Si se tienen varias representaciones del námero M por (a, b, c) pertenecientes al mismo valor N de la expresián \J~D (mod. M) (donde siempre suponemos que los valores de x e y son primos entre sí), tambien se deducirán varias transformaciones propias de la forma (a, b,c) ... (F) en (M, N, NM'D) ... (G). De hecho, si tal representacián proviene de los valores x = m' e y = n', (F) tambien se transforma en (G) por la sustitucián

, r m'N — m'b — n'c , , , n'N + m'a + n'b ,

x = m x + y , y = n x + y .

MM

Viceversa, de cada transformation propia de la forma (F) en (G), se deriva una representation del numero M por la forma (F) perteneciente al valor N. Si (F) se transforma en (G), al poner x = mx' — vy' e y = nx' + μy', entonces M se representa por (F) al poner x = m e y = n, y puesto que aquí m-μ + nv = 1, el valor de la expresion y/Ü (mod. M), al cual pertenece la representacián, sera μ^^. + cn) — v(am + bn), i.e., N. De varias transformaciones propias y diferentes resulta el mismo námero de representaciones diversas pertenecientes a Nf). De esto

\*) De hecho, si deseamos extender la terminología a este caso, podemos decir que si N es el valor de la expresión VD (mod. M), o sea N2 = D (mod. M), significará que N2 — D es un

múltiplo de M, y por lo tanto = 0.

f) Si se supone que la misma representación proviene de dos transformaciones propias diferentes, ellas tendrán que ser:

1) x = mx’ — vy', y = nx' + μy'; 2) x = mx' — ν'y', y = nx' + y!y'

Sin embargo, de las dos ecuaciones

my + nv = my' + nv', y(mb + nc) — v(ma + nb) = μ'(mb + nc) — v '(ma + nb) se deduce fácilmente que o bien M = 0 o bien μ = μ', v = ν'. Pero ya hemos excluido a M = 0.

se concluye fácilmente que, si se tuvieran todas las transformaciones propias de la forma (F) en la (G), resultaran de estas todas las representaciones de M por (F) pertenecientes al valor N. De donde, la cuestión de investigar las representaciones de un numero dado por una forma dada (en la cual se dan valores primos entre si a las indeterminadas) se reduce a la cuestion de investigar todas las transformaciones propias de esta forma en la forma equivalente dada.

Ahora, aplicando a esta lo que aprendimos en el articulo 162, se colige con facilidad que si la representation de algun numero M por la forma (F) perteneciente al valor N es esta x = α e y = γ; la formula general que comprende todas las representaciones del mismo numero por la forma (F) perteneciente al valor N sera:

at — (ab + γο)η γί + (αα + γδ)η

x = , y =

m m

donde m es el maximo común divisor de los numeros α, 2b, c, y t y u representan todos los numeros que satisfacen la ecuacion t2 — Du2 = m2.

170.

Si la forma (α, b, c) es equivalente a alguna forma ambigua y por lo tanto equiv­alente a la forma (M,N, N), tanto propia como impropiamente, o propiamente equivalente a las formas (M, N, )y(M, —N, ^), se tendran las representa­

ciones del numero M por la forma (F) perteneciente tanto al valor N como al valor —N. Y recíprocamente, si se tienen varias representaciones del numero M por la misma forma (F) pertenecientes a valores opuestos N y — N de la expresion VD (mod. M), la forma (F) sera equivalente a la forma (G) tanto propia como impropi­amente y podra encontrarse una forma ambigua a la cual sea equivalente (F).

Estas generalidades sobre las representaciones son suficientes por ahora. Hablaremos mas adelante sobre las representaciones en las cuales las indeterminadas tienen valores no primos entre sí. En lo que atane a las otras propiedades, las formas cuyo determinante es negativo deben ser tratadas de modo totalmente diferente que las formas de determinante positivo; por lo tanto consideraremos ahora las dos por separado. Así, comenzamos con las mas faciles.

Sobre las formas de un determinante negativo.

171.

PROBLEMA. Dada una forma cualquiera *(a,b,ar),* cuyo determinante nega-

Demostracion. I. En la progresion de formas (a, b, a'), (a',b,a), (a'',b',a'') etc., cada una es contigua a su antecedente; por lo cual la última serú propiamente equivalente a la primera (artículos 159 y 160).

II. Como b(m) es el residuo menor absoluto de — b(m ^, segun el múdulo

(m), no serú mayor que ^ a(m) (art. 4).

a

*tivo = -D, donde D es un numero positivo, se debe encontrar una forma* (A, B, C) *propiamente equivalente a ésta, en la cual* A *no es mayor que yj*3*D, ni mayor que C, ni menor que* 2*B.*

Resolución. Suponemos que en la forma dada no valen a la vez las tres condiciones; de lo contrario no serla necesario buscar otra forma. Sea b' el menor residuo absoluto del número —b según el módulo a'[[138]](#footnote-139)), y a" = b J+D, el cual sera un entero; ya que b'2 ξ b2, b'2 + D ξ b2 + D ξ aa' ξ 0 (mod. a'). Si a'' < a', resulta de nuevo que b'' es el menor residuo absoluto de — b', segun el módulo a'', y a''' = b a+D. Si de nuevo a''' < a'' sea de nuevo b''' el menor residuo absoluto de — b'' según el módulo

1. Ya que a(m)a(m+1) = D + b(m)b(m) y a(m+1) no es < a(m), tampoco serú a(m)a(m) > d + b(m)b(m) y como b(m) no es > ±a(m), tampoco sera > D + ±a(m)a(m) y 4 a(m)a(m) no serú > D y finalmente a(m) no > J3 D.

4 ^ Lh ±±W 0^1 <X .Ly y HUCLllllvI?lluvia Lh Hw "W 3 J

Ejemplo. Dada la forma (304, 217, 155) cuyo determinante = —31, se encuentra la progresion de las formas:

'"' \_ b'''2+D

Esta operación continuaró, hasta llegar en la progresión etc., a un termino a(m+1), el cual no es menor que su antecedente a(m). Esto debe ocurrir finalmente, ya que se tendría una progresion infinita de números enteros decrecientes. Entonces la forma (a(m),b(m),a(m +1)) satisfarú todas las condiciones.

a

///

y sea a =

a , a , a , a

(304, 217,155), (155, —62, 25), (25,12, 7), (7, 2,5), (5, —2, 7)

La ultima es la buscada. Del mismo modo, para la forma (121,49,20) cuyo determinante = —19, se encuentran las equivalentes (20, —9, 5), (5, —1, 4), (4, 1, 5): por lo que (4, 1, 5) seraú la forma buscada.

Llamaremos formas reducidas a tales formas (A, B,C) cuyo determinante es negativo y en las cuales A ni es mayor que ^4D, ni mayor que C, ni menor que 2B. Por lo que para cada forma de un determinante negativo podremos encontrar una forma reducida propiamente equivalente a ella.

172.

PROBLEMA. ***Encontrar las condiciones bajo las cuales dos formas reducidas no idénticas (a, b, c) y*** (a0,b0,c0) ***con el mismo determinante, -D, puedan ser propiamente equivalentes.***

Resolución. Supongamos, lo cual es posible, que a0 no es > a, y que la forma ax2 + 2bxy + cy2 se transforma en a0x02 + 2b,x'y' + c0y02 por la sustitución propia x = αχ0 + βy0, y = γχ0 + óy0. Entonces se tendrán las siguientes ecuaciones

|  |  |
| --- | --- |
| aa2 + 2baγ + cγ2 = a0 | (1) |
| aaβ + b(aó + βγ) + cγδ = b0 | (2) |
| aó — βγ = 1 | (3) |

De la (1) resulta aa0 = (aa + bγ)2 + D72; por lo cual aa0 sera positivo; y como ac = D + b2, a0c0 = D + b02, tambien serán positivos ac y a0c0; por lo tanto todos a, a0, c, c0 tendrán el mismo signo. Pero, ni a ni a0 es > \J4D y, por tanto, tampoco aa0 es > |D; por lo cual mucho menos puede ser Dy2(= aa0 — (aa + by)2) mayor que 3D. De esto, γ será o = 0, o = ±1.

1. Si γ = 0, se deduce de la (3) que o bien son a = 1,ó = 1, o a = —1,ó = —1. En ambos casos, resulta de la (1) que a0 = a, y de la (2) que b0 — b = ±βα. Pero, b no es > 1 a ni b0 > 1 a0 y tampoco > 1 a. Por consiguiente, la ecuacion b0 — b = ±βα no puede darse, a no ser que sea

o bien b = b0, de donde resultaría c0 = b Q+D b = c; por lo que las

formas (a, b, c), (a0,b0,c0) serían identicas (contrariamente a la hipotesis),

o bien b = —b0 = ±1 a. En este caso, tambien sería c0 = c y la forma (a0,b0,c0) sería (a, —b,c), i.e., la forma opuesta a (a, b, c). Al mismo tiempo, es evidente que estas formas serían ambiguas ya que 2b = ±a.

1. Si γ = ±1, de la (1) resulta aa2 + c — a0 = ±2ba. Pero c no es menor que a, y por lo tanto no menor que a0; de esto aa2 + c — a0, o sea 2ba no es menor que aa2. Por lo que, como 2b no es mayor que a, tampoco a sera menor que a2; de donde necesariamente a = 0, á = ±1.
2. Si α = 0, de la (1) tenemos a' = c, y puesto que a ni es mayor que c, ni menor que a', será necesariamente a' = a = c. Ademas de la (3) tenemos que βγ = —1 de donde de la (2) b + b' = ±δc = ±δα. De modo semejante a como se dedujo de la (I) tendremos:

o bien b = b', en tal caso las formas serían identicas (contrariamente a la hipótesis),

o bien b = —b', en tal caso las formas (a, b, c), (a',b',c') serían opuestas.

1. Si α = ±1, resulta de la (1) que ±2b = a + c — a'. Por lo tanto como ni a ni c < a', tampoco sería 2b < a ni < c. Pero, 2b ni es > a, ni > c, de donde necesariamente ±2b = a = c, y de la ecuacián ±2b = a + c — a' sera tambien = a'. Por lo tanto de la (2) resulta que

b' = a(ae + γδ) + b(aó + βγ)

o, puesto que αδ — βγ = 1,

b' — b = a(ae + γδ) + 2bβγ = a(ae + γδ ± βγ)

por lo cual necesariamente como antes

o bien b = b', de donde las formas (a, b, c) y (a',b,c) son identicas (contrariamente a la hipotesis),

o bien b = —b', y, por tanto, aquellas formas son opuestas. A la vez, en este caso las formas serían ambiguas; ya que a = ±2b.

De todo esto se concluye que las formas (a, b,c) y (a',b,c) no pueden ser propiamente equivalentes, a no ser que fueran opuestas, y al mismo tiempo o bien ambiguas o bien a = c = a' = d. En estos casos, pudo verse fácilmente que las formas (a, b, c) y (a',b,c) son propiamente equivalentes. De hecho, si las formas son impropiamente opuestas y, además ambiguas, tambien tendrán que ser propiamente equivalentes. Si a = c, la forma (, a — b, a) sera contigua a la forma (a, b, c) y

por ende será equivalente; pero puesto que D + b2 = ac = a2 es = 2a — 2b,

la forma (2a — 2b, a — b, a) es ambigua; por lo cual (a, b, c) tambien equivaldrá a su opuesta propiamente.

Igualmente, ahora puede deducirse fácilmente que cuando dos formas reduci­das (a, b,c) y (a',b,c) son no opuestas pueden ser impropiamente equivalentes. En efecto serán impropiamente equivalentes si (a, b, c) y (a', — b',cr), las cuales no son identicas, son propiamente equivalentes, y viceversa. Es evidente que la condicián

bajo la cual aquellas sean impropiamente equivalentes es que sean idénticas además de ser ambiguas o que a = c. Las formas reducidas que no son ni identicas ni opuestas tampoco pueden ser propia ni impropiamente equivalentes.

173.

PROBLEMA. ***Dadas dos formas F y*** F0, ***con el mismo determinante negativo, se debe investigar si son equivalentes.***

Resolución. Básquense dos formas reducidas f y f0 propiamente equivalentes a las formas F y F' respectivamente. Si las formas f y f0 son propiamente o impropiamente equivalentes, o equivalentes de ambos modos, entonces F y F' tambien lo son; pero si f y f0 no son equivalentes de ninguna manera, tampoco lo son F y F0.

Del artículo anterior pueden presentarse cuatro casos:

1. Si f y f0 no son ni identicas ni opuestas, tampoco F y F0 serían equivalentes de ningán modo.
2. Si f y f0 son, primero, o identicas u opuestas y, segundo, o ambiguas, o tienen sus terminos extremos iguales, F y F0 serían tanto propia como impropiamente equivalentes.
3. Si f y f0 son identicas, pero ni son ambiguas ni tienen terminos extremos iguales, F y F0 solo serían propiamente equivalentes.
4. Si f y f0 son opuestas, pero ni son ambiguas ni tienen terminos extremos iguales, F y F0 solo serían impropiamente equivalentes.

Ejemplo. Para las formas (41, 35, 30) y (7,18,47) cuyo determinante = -5, se encuentran las formas reducidas no equivalentes (1, 0, 5) y (2, 1, 3); por lo que las formas originales de ningán modo serán equivalentes. A las formas (23, 38, 63) y (15, 20, 27) equivale la misma forma reducida (2, 1, 3), y como ella es al mismo tiempo ambigua, las formas (23, 38, 63) y (15, 20, 27) serían equivalentes tanto propia como impropiamente. A las formas (37, 53, 78) y (53, 73, 102) equivalen las formas reducidas (9, 2, 9) y (9, -2, 9), y puesto que estas son opuestas y sus terminos extremos iguales, las formas dadas serían equivalentes propia e impropiamente a la forma opuesta. [[139]](#footnote-140)

formas pueden encontrarse mediante dos métodos. Denotaremos las formas reducidas indefinidas del determinante — D por (a, b, c) donde deben determinarse todos los valores de a, b, c.

Primer método. Tómense para a todos los números positivos y negativos no mayores que ^!D, de los cuales —D sea un residuo cuadrótico, y para cada a se hace b sucesivamente igual a todos los valores de la expresión V—D (mod. a), no mayores que 2a, tomados tanto positiva como negativamente; para cada uno de los valores determinados de a y b se pone c = . Si resultan de este modo unas formas en las

cuales c < a, estas deberán rechazarse, pero las restantes son claramente reducidas.

Segundo método. Tómense para b todos los números positivos y negativos, no mayores que \\f4jD o sea yjjD. Para cada b, resuelvase b2 + D de todas las maneras como pueda hacerse en dos factores menores que 2b (tambien debe tomarse en cuenta la diversidad de los signos). Cuando los factores son diferentes, pongase el menor factor = a y el otro = c. Como a no es > \J4D, todas las formas originadas de esta manera serán claramente reducidas. Finalmente es claro que no puede existir ninguna forma reducida que no se encuentre por ambos móetodos.

Ejemplo. Sea D = 85. Aquí el límite de los valores de a es -y/3|0, que esta entre 10 y 11. Los numeros entre 1 y 10 (inclusive), de los cuales —85 es residuo cuadrático, son 1, 2, 5 y 10. De aquí se tienen doce formas:

(1, 0, 85), (2,1,43), (2, —1,43), (5,0,17), (10, 5,11), (10, —5,11); (—1, 0, —85),

(—2,1, —43), (—2, —1, —43), (—5, 0, —17), (—10, 5, —11), (—10, —5, —11).

Con el otro metodo, se tiene y^!5 para el límite de los valores de b, el cual esta situado entre 5 y 6. Para b = 0, resultan las formas

(1,0, —85), (—1,0, —85), (5,0,17), (—5,0, —17),

para b = ±1 resultan (2, ±1,43) y (—2, ±1, —43).

Para b = ±2 no existe ninguna, ya que 89 no puede resolverse en dos factores de los cuales sean ambos < 4. Lo mismo vale para ±3 y ±4. Finalmente para b = ±5 resultan

(10, ±5,11) y (—10, ±5, —11). [[140]](#footnote-141)

restantes estarán provistas de esta propiedad notable: que cualquier forma del mismo determinante sería propiamente equivalente a una y sólo una de ellas (al contrario otras serían propiamente equivalentes entre sí). De donde, resulta claro que todas las formas del mismo determinante pueden distribuirse en tantas clases como formas permanezcan, a saber, se ponen en la misma clase todas las formas propiamente equivalentes a una forma reducida. Así para D = 85, permanecen las formas

(1, 0, 85), (2,1,43), (5,0,17), (10, 5,11)

(-1, 0, -85), (-2,1, -43), (-5, 0,-17), (-10,5,-11).

Por lo que, todas las formas del determinante -85 podran distribuirse en ocho clases segón sean propiamente equivalentes o a la primera forma, o a la segunda etc. Desde luego, es claro que las formas colocadas en la misma clase serán propiamente equivalentes, y las formas de diferentes clases no pueden ser propiamente equivalentes. Pero mas adelante desarrollaremos con mucho detalle este argumento concerniente a la clasificación de las formas. Aquí añadimos una sola observación. Mostramos antes que si el determinante de la forma (a, b, c) en negativo = -D, entonces a y c tendrón el mismo signo (porque ac = b2 + D, y por lo tanto es positivo). Por la misma razon se percibe fócilmente que, si las formas (a, b, c) y (a/,b/,c/) son equivalentes, todos los a, c, a0, c0 tendrón el mismo signo. De hecho, si la primera se transforma en la segunda por la sustitución x = αχ0 + βy/, y = qx0 + by0, sera aa2 + 2baq + cq2 = a0, de esto aa0 = (aa + bβ)2 + Dq2 y por tanto ciertamente es no negativo. Puesto que ni a ni a0 puede ser = 0, aa0 seró positivo y por eso los signos de a y a0 serón los mismos. De esto es claro que las formas cuyos terminos extremos son positivos esrán completamente separadas de aquellas cuyos terminos extremos son negativos. Solo basta considerar estas formas reducidas, las que tienen sus terminos extremos positivos; puesto que las restantes son iguales en nuómero y provienen de ellas al asignar signos opuestos a los terminos extremos. Lo mismo vale para las formas rechazadas o retenidas de las reducidas. [[141]](#footnote-142)

aquéllas cuyos terminos extremos son positivos.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D |  |  |  |  |
| 1 | (1,0,1). |  |  |  |
| 2 | (1, 0, 2). |  |  |  |
| 3 | (1,0,3), | (2,1, 2). |  |  |
| 4 | (1, 0,4), | (2,0, 2). |  |  |
| 5 | (1,0,5), | (2,1,3). |  |  |
| 6 | (1,0,6), | (2,0,3). |  |  |
| 7 | (1,0, 7), | (2,1,4). |  |  |
| 8 | (1,0,8), | (2, 0,4), | (3,1, 3). |  |
| 9 | (1,0,9), | (2,1,5), | (3, 0, 3). |  |
| 10 | (1, 0,10), | (2,0,5). |  |  |
| 11 | (1, 0,11), | (2,1,6), | (3,1,4), | (3, —1,4) |
| 12 | (1, 0,12), | (2, 0,6), | (3, 0,4), | (4, 2,4). |

Sería superfluo continuar esta tabla, dado que enseñaremos luego un método mucho mas adecuado para construirla.

Es evidente que cada forma del determinante —1 es propiamente equivalente a la forma x + y si sus terminos extremos son positivos, pero equivalente a — x — y si son negativos. Cada forma del determinante —2 cuyos terminos son positivos es equivalente a la forma x2 + 2y2, etc. Cada forma del determinante —11 cuyos terminos extremos son positivos es equivalente a una de estas x2 + 11y2, 2x2 + 2xy + 6y2, 3x2 + 2xy + 4y2, 3x2 — 2xy + 4y2, etc.

177.

PROBLEMA. Se tiene una serie de formas de las cuales cada una es contigua a la parte posterior de la precedente y se desea una transformación propia de la primera en cualquier forma de la serie.

Solucion. Sean las formas (a, b, a') = F; (a',b',a'') = F'; (a'',b'',a''') = F'';

(a"'b"'a"") = F''' etc. Se denotan , b + , b + etc., respectivamente por h', h'', h''' etc. Sean x, y; x', y'; x'', y'' etc., las indeterminadas de las formas F, F', F''

etc. Se supone que F se transmuta

en F' poniendo x = o'x0 + β'y0, y = γ X + δ0 y0

F00 .... x = O'X' + β'Υ', y = 7'V + δ'Υ'

f'''. . . . x = o000 x00 + β00γ00, y = γ00 X00 + δ00γ00

etc.

Entonces, puesto que F se transforma en F' poniendo x = -y', y = x0 + h'y0

F' en F00 poniendo x0 = -y00, y0 = x00 + h00y00 F00 en F000 poniendo x00 = -y000, y00 = x000 + h000y0 etc. (art. 160)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| fácilmente se | encuentra el | | algoritmo | siguiente | (art. | 159): |  |  |
| o0 | = 0 | β0 | = -1 | γ0 | = 1 | δ0 = | h0 |  |
| o00 | = β0 | β00 | = h00y - o0 γ00 | | = δ0 | δ00 = | = h'V - | γ0 |
| o000 | = β00 | β000 | = h00y00 - | o00 γ000 | = δ00 | δ000 = | = h00V - | γ00 |
| o0000 | = β000 | β0000 | = h000y000 - | o000 γ0000 | = δ000 | δ0000 = | = h00V | - γ000 |

etc.,

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| o sea o0 = 0 | β0 | = -1 | γ0 | = 1 | δ0 | = h0 |
| o00 = β0 | β00 | = h00y | γ00 | = δ0 | δ00 | = hV - |
| o000 = β00 | β000 | = h00y00 - β0 | γ000 | = δ00 | δ000 | = h00v - |
| o0000 = β000 | β0000 | = h000y000 - β00 | γ0000 | = δ000 | δ0000 | = h00V |
|  |  |  | etc. |  |  |  |

Puede deducirse sin dificultad tanto de su formación como del art. 159 que todas estas transformaciones son propias.

Este algoritmo bien simple y preparado para los cálculos es analogo al algoritmo expuesto en el artículo 27, al cual tambien puede reducirse[[142]](#footnote-143)). Ademas, esta solucion no esta restringida a las formas de un determinante negativo, si no a todos los casos donde ninguno de los námeros a0, a00, a000, etc., = 0.

178.

4k + 0; 1; 2; 3; y

PROBLEMA. Dadas dos formas propiamente equivalentes a F y f del mismo determinante negativo, encontrar alguna transformación propia de la una en la otra.

Solución. Supongamos que la forma F es (A, B,A'), y que por el método del artículo 171 se ha encontrado la progresión de formas (A',B',A'') y (A",B",A"') etc. hasta la forma reducida (Am,Bm,Am+1). De manera similar supongamos que f es (a, b, a') y que por el mismo metodo se encuentra la serie (a',b',a") y (a",b",a'") hasta la forma reducida (an,bn,an+1). Entonces pueden tener lugar dos casos.

1. Si las formas (Am,Bm,Am+1) y (an,bn,an+1) o son identicas u opuestas y, a la vez, ambiguas, entonces, las formas (Am-1,Bm-1,Am) y (an, -bn-1,an-1) serón contiguas (donde Am-1 denota el penóltimo termino de la progresión A, A', A'', ...Am, y de manera semejante Bm-1, an-1, bn-1). Puesto que Am = an, Bm-1 ξ -Bm (mod. Am), bn-1 ξ- (mod. an osea Am), resulta Bm-1 - bn-1 ξ bn - Bm y, por tanto ξ 0, si las formas (Am,Bm,Am+1), (an,bn,an+1) son identicas, y ξ 2bn y por tanto ξ 0, si son opuestas y ambiguas. Por lo que, en las progresiones de las formas

*(a*

n

(A,B, A'), bn-1,an-1),

(A',B',A'), ... (Am-1,Bm-1,Am),

(an-1, -bn-2,an-2), ... (a', -b,a), (a,b,a')

cada forma seró contigua a la precedente; y de esto, por el artículo anterior podró encontrarse una transformacioón propia de la primera F en la segunda f.

1. Si las formas (Am,Bm,Am+1) y (an,bn,an+1) no son identicas, sino opuestas y, a la vez, Am = Am+1 = an = an+1; entonces, la progresion de las formas

(A,B,A'), (A',B',Afí), ... (Am,Bm,Am+1),

(an, -bn-1,an-1), (an-1, -bn-2,an-2), ... (a', -b,a), (a,b,a')

estarán provistas de la misma propiedad. Puesto que Am+1 = an, y Bm - bn-1 = -(bn + bn-1) seró divisible por an. De donde, por el artóculo anterior, se encontrara una transformacióon propia de la primera forma F en la segunda f.

Ejemplo. Para las formas (23,38,63) y (15, 20,27) se tiene la progresión (23, 38, 63), (63, 25,10), (10, 5, 3), (3,1, 2), (2,-7, 27), (27, -20,15), (15, 20, 27) por lo cual

h' = 1, h" = 3, h'" = 2, h"" = -3, h'"" = -1, h""" = 0

De esto se deduce que la transformación de la forma 23x2 + 76xy + 63y2 en

15t2 + 40tu + 27u2 es esta: x = — 13t - 18u, y = 8t + 11u.

De esta solucion, se deduce sin dificultad la solucion del problema: Si las formas F y f son impropiamente equivalentes, hallar una transformación impropia de la forma F en f. De hecho, sea f = at2 + 2btu + a'u2, entonces la forma opuesta ap2 - 2bpq + a'q2 sera propiamente equivalente a la forma F. Busquese una transformacion propia de la forma F en x = ap + βq y y = γρ + óq, entonces es claro que F se transforma en f dadas x = at - βu, y = qt - óu; por lo que esta transformacion sera impropia.

Si, por lo tanto, las formas F y f son equivalentes tanto propia como impropiamente, entonces podra encontrarse tanto una transformacion propia como una impropia. [[143]](#footnote-144)

1. m > 4, será D > m2; de donde en t2 + Du2 = m2, u deberá ser = 0, y por tanto t no puede tener otros valores más que +m y —m. De esto, si F y f son equivalentes de una sola manera, entonces no puede darse alguna transformacián más que

x = ax' + Py' , y = γx' + óy',

la cual resulta poniendo t = m (articulo 162), y otra

x = —ax — Py', y = —γχ0 — óy'.

Si por el otro lado F y f son equivalentes tanto propia como impropiamente, y si se tiene alguna transformacioán propia

x = ax' + Py', y = γx' + óy'

y una impropia

/ / I ni t

x = a x + p y ,

II I r/ /

y = γ x + ó y

entonces no se presentara otra transformación propia salvo aquellas (poniendo t y estas

m)

x = —ax' — Py', y = —γx' — óy'

(poniendo t = —m) y de modo semejante ninguna impropia salvo

i i , ni i i i . xi i *r r n! r i* I el *i*

x = ax + p y , y = γ x + óy ; y x = —a x — p y , y = —γ x — ó y .

x = ±ax' ± Py', y = ±γx' ± óy'

aB + γ^ . PB + óC , , aA + γΒ , PA + óB ,

x = ^ !— x' ^ y', y = ± !— x' ± y'

m

m

m

m

Por otro lado, si F y f son equivalentes de dos maneras, o sea, si ademas de esta transformacion dada se tiene otra no semejante a esta misma, ella tambien proporcionará cuatro no semejantes a ella de tal manera que se tengan ocho transformaciones. Ademas, en este caso puede demostrarse que F y f siempre son equivalentes de dos maneras. Como D = m2 = AC — B2, m tambien dividira a

1. El determinante de la forma (m, m, m) será = —1, por lo que sera equivalente a la forma (1, 0, 1) o a (—1, 0, — 1). Sin embargo, se percibe que, mediante la misma transformacián por la cual se transforma (m, m, m) en (±1, 0, ±1), se transformará la forma (A,B,C) en una ambigua (±m, 0, ±m). Por lo que, la forma (A,B,C), equivalente a una ambigua, equivaldraá tanto propia como impropiamente a cualquier forma a la cual sea equivalente.
2. Si 22 = 3, o sea 4D = 3m2, entonces m sera par y el total de soluciones de la ecuacián t2 + Du2 = m2 sera seis:
3. —1 1 —1

t,u = m 0; —m, 0; ^m 1 ~γm —1; 2m —1; m, 1

Por consiguiente, si se tienen dos transformaciones no semejantes de la forma F en

f,

x = αχ' + β^ y = γχ' + óy' x = α'χ' + β'ι/ y = γ'χ' + ó'y'

se tendraán doce transformaciones, a saber, seis semejantes a la primera  
x = ±αχ' ± β^, y = ±γχ' ± óy'

x = ±(1α — aB + ^)χ' ± (iβ — βΒ + óC)y'

χ ±(2" m )x ± (2β m )y

1 αΑ +γΒ ' ^ βΑ + óB '

y = ±bγ + )x ± bó + )y

1. m 2 m

χ = ±(1 α + αΒ±ΐ£)x' ± (1 β + )y'

1. m 2 m
2. αΑ + γΒ ' ^ βΑ + όΒ '

y = ±bγ )χ ± bó )y

1. m 2 m

y seis semejantes a la segunda, que se originan de áestas al sustituir α, β, γ, ó por α ,

β ,γ ,ó .

Para demostrar que en este caso F y f siempre son equivalentes de ambas maneras, consideremos lo siguiente. El determinante de la forma (, —, -A-) será = “~|2 = —3, y por tanto esta forma es equivalente (art. 176) o a la forma (±1, 0, ±3), o a la forma (±2, ±1, ±2). De donde se sabe que la forma (A, B,C) es equivalente

o a la forma (±2m, 0, ±|m) o a la forma (±m, 2m, ±m)[[144]](#footnote-145)), las cuales son ambas ambiguas, y, por tanto, de ambas maneras equivalente a una de ellas.

1. Si se supone ^ =2, sería (^)2 = 4^2 - 2, y, por tanto, = 2 (mod. 4). Pero, como ningún cuadrado puede ser = 2 (mod. 4), este caso no puede darse aquí.
2. Suponiendo que ^ = 1, sería (^ )2 = 4^2 — 1 = —1 (mod. 4). Pero como esto es imposible, este caso tampoco puede ocurrir aquí.

Ademas, como D no puede ser ni = 0 ni negativo, no pueden darse otros casos diferentes mías que los enumerados.

180.

PROBLEMA. Hallar todas las representaciones del número dado M por la forma ax2 + 2bxy + cy2 *...F,* del determinante negativo —D, en la cual x e y tengan valores primos entre sí.

Soluciún. Por el artículo 154, notamos que M no puede representarse tal como se necesita, a menos que —D sea residuo cuadratico de M. Así, primero búsquense todos los valores diferentes (i.e. incongruentes) de la expresión V—D (mod. M); sean estos valores N, —N,N', —N',N'', —N" etc. Para simplificar los calculos, se pueden determinar todos los N, N', etc., de tal manera que no sean > 2M. Puesto que cualquier representación debe pertenecer a alguno de estos valores, consideraremos cada uno separadamente.

Si las formas F, (M, N, ) no son propiamente equivalentes, no puede

existir ninguna representación de M perteneciente al valor N (artículo 168). Si al contrario existen, buscaremos una transformacion propia de la forma F en

Mx'2 + 2Nx y +

D + N2

M

2

y

la cual sea

x = ax + ey, y = jx' + óy

y x = a, y = γ sera una representaciín del nímero M por F perteneciente al valor N. Sea el míximo comín divisor de los numeros A, 2B, C = m, entonces distinguiremos tres casos (artículo anterior):

1. Si ^2 > 4 no se darán representaciones pertenecientes a N salvo estas dos x = a, y = γ y x = —a, y = —γ (artículos 169 y 179).
2. Si 42 = 4 se tendrán cuatro representaciones

aB + γ6\*

' m2 r

x = ±a, y = ±γ; x = ^

y = ±

m

aA + γΒ

m

1. Si 42 = 3 se tendran seis representaciones

/ m2 -1

y = ±γ

x = a

= ±( 1 a + AA) y = ±( 1 γ — -tos)

x

De la misma manera se deben buscar las representaciones pertenecientes a los valores —N, N', —N' etc.

181.

La investigación de las representaciones del número M por la forma F, en la cual x e y tienen valores no primos entre sí, puede reducirse facilmente al caso ya considerado. Suponga que se hace tal representación al poner x = μe e y = μf de manera que μ sea el maximo común divisor de μe y μf, o sea, e y f son primos entre sí. Entonces tendremos que M = μ2(Ae2 + 2Bef + Cf2) y, por lo tanto, sera divisible por μ2. Sin embargo, la sustitución x = e, y = f sera una representación del número por la forma F, en la cual x e y tienen valores primos entre sí. Si M no es divisible por ningún cuadrado (salvo 1), por ejemplo, si es un número primo, no se darón tales representaciones de M. Sin embargo, si M involucra divisores cuadrados, sean estas μ2, ν2, π2 etc. Se buscan primero todas las representaciones del número por la forma (A,B,C), en las cuales x e y tienen valores primos entre sí. Tales valores, si se multiplican por μ, suministraran todas las representaciones de M en las cuales el maximo comun divisor de los numeros x e y es μ. De modo semejante, todas las representaciones de Mf, en las cuales los valores de x e y son primos entre sí, producirán todas las representaciones de M en las que el maximo comun divisor de los valores x e y es ν etc.

Por lo tanto, es claro que por las reglas precedentes pueden encontrarse todas las representaciones de un numero dado por una forma dada de un determinante negativo.

Aplicaciones especiales a la descomposición de los números en dos cuadrados,  
en un cuadrado simple y uno doble, en un cuadrado simple y uno triple .

182.

Pasamos a ciertos casos especiales tanto por su elegancia notable como por el incesante trabajo empleado en ellos por el ilustre Euler, por lo que estan provistos de una belleza casi clásica.

1. Ningán numero puede representarse por la forma x2 + y2, de modo que x sea primo a y (o sea descompuesto en dos cuadrados primos entre sí) a no ser que —1 sea un residuo cuadratico de el. Sin embargo, tales námeros tomados positivamente sí pueden serlo. Sea M un numero tal, y todos los valores de la expresián y/—1 (mod. M) estos: N, — N, N', —N', N'', — N'' etc., entonces, por el artículo 176 la forma (M, N, ) será propiamente equivalente a la forma (1, 0, 1). Sea x = ay' + ^y', y = γx' + Sy' una transformacián propia de la segunda en la primera, y las representaciones del numero M por la forma x2 + y2 pertenecientes a N estas cuatro[[145]](#footnote-146)): x = ±a, y = ±γ; x = ^γ, y = ±a.

Puesto que la forma (1, 0, 1) es ambigua, de hecho sera propiamente equiva­lente a la forma (M, — N, Xjf1), y por ende aquella se transmutará en esta, poniendo x = ax' — ey, y = —γx' + Sy'. De esto se derivan cuatro representaciones de M pertenecientes a —N, x = ±a, y = ^γ; x = ±γ, y = ±a. Así pues, existen ocho representaciones de M, la mitad de los cuales pertenece a N, la otra mitad a —N; pero todas estas representan solo una descomposición del número M en dos cuadra­dos, M = α2 + γ2, si sálo consideramos a los cuadrados mismos, pero no al orden de las rames ni a sus signos.

Por tanto, si no existen otros valores de la expresion V — 1 (mod. M), salvo N y —N, lo cual e.g. resulta cuando M es un námero primo, M podrá resolverse en dos cuadrados primos entre sí de una sola manera. Puesto que —1 es un residuo cuadratico de cualquier numero primo de la forma 4n +1 (art. 108), entonces es evidente que un nuámero primo no puede descomponerse en dos cuadrados no primos entre sí. Así tendremos el teorema:

Cualquier numero primo de la forma 4n + 1 puede descomponerse como suma de dos cuadrados, y de una sola manera.

1. = 0 + 1, 5 = 1 + 4, 13 =4 + 9, 17 = 1 + 16, 29 = 4 + 25, 37 = 1 + 36,

41 = 16 + 25, 53 = 4 + 49, 61 = 25 + 36, 73 = 9 + 64, 89 = 25 + 64,

97 = 16 + 81 etc.

Este teorema elegantísimo ya fue conocido por Fermat, pero fue demostrado primero por el ilustre Euler, Comm. nov. Petr., V, 1754 y 1755, p. 3. En el cuarto volumen existe una disertación perteneciente al mismo argumento (p. 3) pero entonces aún no había encontrado una solución completa, vease especialmente artículo 27.

Por lo tanto, si algun numero de la forma 4n +1 puede resolverse en dos cuadrados o bien en varias maneras, o bien de ninguna manera, entonces no sería primo.

Al contrario, si la expresión y/ — 1 (mod. M) tiene otros valores, ademas de N y — N, se presentarón todavía otras representaciones de M, pertenecientes a estos. Así pues, en este caso M podró resolverse de varias maneras en dos cuadrados; e.g. 65 = 1 + 64 = 16 + 49, 221 = 25 + 196 = 100 + 121.

Las restantes representaciones, en las cuales x e y tienen valores no primos entre sí, pueden encontrarse con facilidad por nuestro metodo general. Sílo observamos que, si algín nímero que involucra factores de la forma 4n + 3 no puede liberarse de estos por ninguna division por un cuadrado (esto sucederí si uno o varios de tales factores tienen un exponente impar), entonces dicho nímero tampoco puede resolverse de manera alguna en dos cuadrados\*).

1. Ningín nímero del cual —2 es un no residuo podrí representarse por la forma x2 + 2y2, de tal modo que x sea primo a y, pero todos los restantes sí podrín. Sea —2 un residuo del nímero M, y N algín valor de la expresion y/—2 (mod. M). Entonces, por art. 176 las formas (1, 0, 2) y (M,N, ) serín propiamente

equivalentes. La primera se transforma en la segunda poniendo x = αχ' + β^, y = qx' + 6y', y x = α, y = q sera una representacion del nímero M perteneciente a

\*) Si el número M = 2VSaaCcγ ... de manera que a, b, c sean números primos diferentes de la forma 4n + 1 y si S es el producto de todos los factores primos de M de la forma 4n + 3 (a tal forma cualquier número positivo puede reducirse, haciendo μ = 0 cuando M es impar, y S =1, cuando M no involucra factores de la forma 4n + 3), entonces M de ninguna manera podrú resolverse en dos cuadrados si S no es un cuadrado, pero si S es un cuadrado, se presentarúan 2(α + 1)(β + 1)(γ + 1) etc. descomposiciones de M cuando alguno de los números α, β, γ, etc. es impar, pero 2 (α + 1)(β + 1)(γ + 1) etc. + 2 cuando todos α, β, γ, etc. son pares (puesto que se examinan solamente los cuadrados). Los que son versados en el calculo de combinaciones podran llevar a cabo la demostración de este teorema (en el que, como para otros casos particulares, no podemos detenernos) sin dificultad a partir de nuestra teoría general. Vea artículo 105.

N. Además de esta, tendremos x = —α e y = —7, y no existen otras pertenecientes a N (artículo 180).

De modo semejante, se percibe que las representaciones x = ±α, y = ^7 pertenecen al valor —N. Sin embargo estas cuatro representaciones presentan ánicamente una descomposicián de M en un cuadrado y el doble de un cuadrado, y si mas allá de N y —N no se dan otros valores de la expresión V— 2 (mod. M), tampoco existirán otras descomposiciones. De esto, con la ayuda de las proposiciones del artículo 116, se deduce fácilmente este teorema:

Cualquier número primo de la forma 8n +1 u 8n + 3 puede descomponerse en un cuadrado y un cuadrado duplicado de una sola manera.

1. = 1 + 0, 3 = 1 + 2, 11 = 9 + 2, 17 = 9 + 8, 19 = 1 + 18, 41 = 9 + 32,

43 = 25 + 18, 59 = 9 + 50, 67 = 49+ 18, 73 = 1 + 72, 83 = 81 + 2,

89 = 81 + 8, 97 = 25 + 72 etc.

Fermat tambien conocáa este teorema, como varios semejantes; pero el ilustre Lagrange dio la primera demostracián, Suite des recherches d’Arithmétique, Nouv. Mám. de l’Ac. de Berlán, 1775, p. 323. Ya el ilustre Euler habáa llevado a cabo mucho con relación al mismo argumento, Specimen de usu observationum in mathesi pura, Comm. nov. Petr., VI, p. 185. Pero nunca encontró una demostracion completa del teorema. Comparese tambien la disertacián en el Tomo VIII (para los años 1760 y 1761) Supplementum quorundam theorematum arithmeticorum, al final.

1. Se demuestra por un máetodo semejante que, cada nuámero del cual —3 es un residuo cuadrático, puede representarse o por la forma x2 + 3y2 o por 2x2 + 2xy + 2y2, de manera que el valor de x sea primo al valor de y. Por lo tanto, puesto que —3 es un residuo de todos los námeros primos de la forma 3n+1 (art. 119), y ya que ánicamente námeros pares pueden representarse por la forma 2x2 + 2xy+2y2. Tal como arriba se tiene este teorema:

Cualquier numero primo de la forma 3n + 1 puede descomponerse como suma de un cuadrado y un cuadrado triplicado y solo de una manera.

1. = 1 + 0, 7 = 4 + 3, 13 = 1 + 12, 19 = 16 + 3, 31 = 4 + 27, 37 = 25 + 12,

43 = 16 + 27, 61 = 49 + 12, 67 = 64 + 3, 73 = 25 + 48 etc.

El ilustre Euler presentáo la primera demostraciáon de este teorema en el comentario citado, Comm. nov. Petr., VIII, p. 105.

De modo semejante podremos adelantar y mostrar que todo número primo de la forma 20n + 1, o 20n + 3, o 20n + 7, o 20n + 9 (de los cuales —5 es un residuo) puede representarse por una de las dos formas x2+5y2, 2x2 + 2xy+3y2, y los números primos de la forma 20n + 1 y 20n + 9 pueden representarse por la primera forma, los números primos de la forma 20n + 3, 20n + 7 por la segunda, y ademas los dobles de los primos de la forma 20n + 1, 20n + 9 por la forma 2x2 + 2xy + 3y2 y los dobles de los primos de la forma 20n + 3, 20n + 7 por la forma x2 + 5y2. Pero esta proposiciún y otras infinitas particulares podrún derivarse de las precedentes y de lo que se discuta mas adelante. Pasamos ahora a las formas de un determinante positivo. Dado que la naturaleza de ellas es completamente diferente cuando el determinante es un cuadrado que cuando no es un cuadrado, excluiremos primero las formas de un determinante cuadrado y luego las consideraremos por separado.

Sobre las formas de un determinante positivo no cuadrado.

183.

PROBLEMA. Dada cualquier forma (a, b, a'), cuyo determinante positivo y no cuadrado es = D, se debe encontrar una forma *(A,B,C*) propiamente equivalente a ella, en la cual B sea positivo y < *\J~D* y donde A, si es positivo o —A, si A es negativo, estará situada entre \JD + B y \[D — B.

Resolución. Suponemos que en la forma propuesta las dos condiciones aún no tienen lugar; de lo contrario no sería necesario buscar otra forma. Ademas, observamos que en una forma de un determinante no cuadrado, el primer termino o el ultimo no puede ser = 0 (artículo 171, nota de pie). Sea b' = — b (mod. a') de modo que este situado entre los Emites \/D y y/D ^ a' (tomando el signo superior cuando a' es positivo, el inferior cuando es negativo), lo cual es posible por un

/2

razonamiento como el del art. 3. Sea b a,D = a'', que serú un entero ya que b'2 — D = b2 — D = aa' = 0 (mod. a'). Ahora, si a'' < a', se tomara b'' = — b' (mod. a'') y situado entre y[D y y/D ^ a'' (según a'' sea positivo o negativo) y = a'''. Si de nuevo a''' < a'', sea otra vez b''' = —b'' (mod. a''') y situado entre

b*"2-D*

/D y λ/D ^ a''' y b a-D = a''''. Se continuará este procedimiento para formar la progresión a', a'', a''', a''''etc. hasta un termino am+ no menor que el precedente am. Esto finalmente debe suceder, pues de lo contrario se tendrá una progresion infinita de números enteros continuamente decrecientes. Entonces, dadas am = A, bm = B y am+l = c, la forma (A,B, C) satisfará todas las condiciones.

Demostración. I. Puesto que en la progresión de formas (a, b, a'), (a/,b/,a//), (a",b",a'") etc. cualquiera es contigua a la precedente, la última (A,B,C) sera propiamente equivalente a la primera (a, b, a').

1. Puesto que B esta situado entre -^/D y \/~D T A (tomando siempre el signo superior cuando A es positivo, el inferior cuando A es negativo), es claro que, si se pone VD — b = p, B — (VD T A) = q, estos p y q serán positivos. Se confirma facilmente que q2 + 2pq + 2p\/D = D + A2 — B2; por lo que D + A2 — B2 sera un numero positivo, el cual pondremos = r. De esto, puesto que D = B2 — AC resulta r = A2 — AC y por tanto A2 — AC sera un numero positivo. Pero, ya que por hipotesis A no es mayor que C, es claro que esto no puede suceder a menos que AC sea negativo, y por lo tanto los signos de A y C deben ser opuestos. De esto, B2 = D + AC < D y por tanto B < \/D.
2. Ademús, ya que — AC = D — B2, tendremos AC < D, y de esto (puesto que A no es > C) A < \/D. Por lo que, \/D T A sera positivo, y por tanto tambien lo sera B, el cual esta situado entre los límites vD y \JD T A.
3. De esto, con mas razon \JD + B T A es positivo, y dado que \/D — B T A = —q, es negativo, ±A estará situado entre \/D + B y \JD — B. Q. E. D.

Ejemplo. Propuesta la forma (67, 97,140) cuyo determinante es = 29, se encontrara aquí la progresion de las formas (67, 97,140), (140, —97,67), (67, —37, 20), (20, —3, —1) y (—1,5,4). La ultima es la buscada.

Llamaremos formas reducidas a tales formas (A,B,C) de un determinante positivo no cuadrado D, en las cuales A, tomado positivamente, esta situado entre \/D + B y VD — B, siendo B positivo y < \/D. Así pues las formas reducidas de un determinante positivo no cuadrado difieren de las formas reducidas de un determinante negativo. Pero debido a la gran analogía entre estas y aquellas, no quisimos introducir diferentes denominaciones. [[146]](#footnote-147)

formas reducidas (de un determinante positivo no cuadrado, lo cual siempre está supuesto).

1. Si (a, b, c) es una forma reducida, a y c tendrán signos opuestos. Ya que puesto el determinante de la forma = D, sera ac = b2 — D, y por lo tanto, puesto que b < VD, sera negativo.
2. El námero c tomado positivamente estará situado, tal como a, entre \/D + b

y VD — b. Puesto que —c = ; entonces c, abstraído del signo, estará situado

entre —+b y —— , ^entre — b WD+b.

1. De esto es evidente que (c, b, a) tambien sera una forma reducida.
2. Tanto a como c serán < 2\[D. En efecto, ambos son < \JD + b, y así con mas razón < 2\JD.
3. El numero b estará situado entre \/D y VD T a (tomando el signo superior cuando a es positivo, el inferior cuando es negativo). Puesto que ±a cae entre \/D+b y VD — b, entonces ±a — (VD — b), o sea b — (VD T a) sera positivo; sin embargo b — VD es negativo, debido a que b estará situado entre \/D y VD T a. Del mismo modo se demuestra que b cae entre \/D y VD T c ( segun c sea positivo o negativo).
4. Cada forma reducida (a, b, c) es contigua por una u otra parte a una reducida y no a varias.

Sea a' = c, b0 ξ —b (mod. a0) tal que este situado entre \/D y VD T a0[[147]](#footnote-148)),

c0 = —ffV-, y la forma (a',b',c0) estará contigua a la forma (a, b, c) por su ultima parte. A la vez, es evidente que si existe alguna forma reducida contigua a la forma (a, b, c) por la ultima parte, ella misma no puede ser diferente a (a',b',c'). Sin embargo, demostramos que esta se ha reducido así:

A) Si se pone

VD + b T a0 = p, ±a0 — (λ/D — b) = q, VD — b = r

entonces por (2) arriba y la definicion de forma reducida, p, q y r serán positivos. Ademas, pongase

b0 — (λ/D T a0) = q0, VD — b0 = r0

y q' y r' serán positivos, puesto que b' está situado entre \/D y yfü ^ a'. Finalmente, sea b + b' = ±ma' entonces m será un entero. Es claro que sera p + q' = b + b', y por tanto b + b', o sea ±ma' es positivo, y por eso tambien lo es m; de donde resulta que m — 1 no será negativo. Ademas, tenemos

r + q' ± ma' = 2b' ± a', o sea 2b' = r + q' ± (m — 1)a'

de donde 2b' y b' serán necesariamente positivos. Y puesto que b' + r' = \/D,

tendremos b' < \/D.

B) Ademas tenemos

r ± ma' = VD + b', o sea r ± (m — 1)a' = λ/D + b' ^ a'

por lo cual \/D + b' ^ a' será positivo. Puesto que ±a' — (\/D — b') = q', y por lo

tanto positivo, ±a' estará situado entre \/D + b' y y/D — b'. Por esto, (a',b',c') sera

una forma reducida.

Del mismo modo se demuestra que si tenemos 'c = a, 'b ξ —b (mod. 'c) con 'b situado entre \/D y \/D ± 'c, y si 'a = b ,-D, entonces la forma ('a,'b,'c) sera reducida. Evidentemente, esta forma tambien es contigua a la forma (a,b,c) por la primera parte, y salvo ( a, b, c), otra forma reducida no podraá estar provista de esta propiedad.

Ejemplo. La forma reducida (—14, 3, 13) es contigua por la parte última a la reducida (5, 11, —14) cuyo determinante es = 191, y por la parte primera es contigua a (—22,9, 5).

1. Si la forma reducida (a',b,C) es contigua a la forma reducida (a, b, c) por la parte ultima, la forma (C,b,Y) sera contigua por la parte primera a la forma reducida (c, b, a). Si la forma ('a, 'b, 'c) es contigua por la parte primera a la reducida (a, b, c), la reducida ('c, 'b, 'a) sera contigua a la reducida (c, b, a) por la parte ultima. Tambien las formas (—'a,'b, — 'c), (—a, b, —c), (—a',b, —c') serán reducidas, y la segunda contigua a la primera, la tercera a la segunda por la parte ultima, o sea la primera a la segunda y la segunda a la tercera por la parte primera. De modo semejante, esto vale para las tres formas (—c',b, —a'), (—c, b, —a) y (—'c,'b, —'a). Esto es tan obvio que no es necesario explicarlo.

185.

El número de todas las formas reducidas de un determinante dado D siempre es finito, mas, ellas mismas pueden encontrarse de dos maneras. Denotaremos, de modo indefinido, por (a, b, c) todas las formas reducidas de un determinante D de manera que determinemos todos los valores de a, b, c.

Primer método. Se toma para a todos los números (tanto positiva como negativamente) menores que 2\fD, de los cuales D es un residuo cuadratico, y para cada a en particular se pone b igual a todos los valores positivos de la expresión \fD (mod. a) situados entre y/D y y/D ^ a. Pero para cada valor determinado de a y b

*b2- D*

. Si algunas formas provienen de este modo, en las

en particular se pone c =

cuales ±a esta situado afuera de y/D + b y y/D — b, deben rechazarse.

Segundo método. Se toma para b todos los números positivos menores que y/D, y para cada b en particular se resuelve b2 — D en dos factores de todas las maneras posibles, los cuales, desechado el signo, esten situados entre y/D+b y y/D—b y ponemos el uno = a, el otro = c. Evidentemente cada una de las resoluciones en factores en particular suministrarú dos formas; ya que uno u otro factor debe ponerse tanto = a, como = c.

Ejemplo. Sea D = 79, entonces tendremos veintidús valores de a: ^1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15. De donde se encuentran diecinueve formas:

(1, 8, —15), (2, 7, —15), (3, 8, —5), (3, 7, —10), (5, 8, —3), (5, 7, —6),

(6,7, —5), (6,5, —9), (7,4, —9), (7,3, —10), (9,5, —6), (9,4, —7),

(10, 7, —3), (10,3, —7), (13,1, —6), (14, 3, —5), (15,8, —1),

(15, 7, —2), (15, 2, —5)

y tantas otras resultan de úestas, si se cambian los signos de los túerminos extremos, por ejemplo (—1, 8, 15), (—2, 7, 15), etc., de tal suerte que todas son treinta y ocho. Pero rechazadas estas seis: (±13,1, ^6), (±14, 3, ^5) y (±15, 2, ^5), las restantes treinta y dos comprenderaún todas las reducidas.

Por el segundo metodo, tendremos las mismas formas en el orden siguiente[[148]](#footnote-149)):

(±7, 3, T10), (±10, 3, T7), (±7,4, T9), (±9,4, T7), (±6,5, T9),

(±9,5, ±6), (±2, 7, ±15), (±3, 7, ±10), (±5,7, ±6), (±6,7, ±5),

(±10, 7, ±3), (±15, 7, ±2), (±1, 8, ±15), (±3, 8, ±5),

(±5, 8, ±3), (±15, 8, ±1)

186.

Sea F una forma reducida del determinante D y la forma F0 contigua a ella misma por la parte última; entonces la reducida F00 sera contigua a esta por la parte última; la reducida F000 contigua a F00 por la parte última etc. Entonces, todas las formas F0, F00, F000 etc. estarún completamente determinadas, y serún propiamente equivalentes tanto entre si como a la forma F. Puesto que el numero de todas las formas reducidas de determinante dado es finito, todas las formas en la progresiún infinita F, F0, F00 etc. no podrún ser diferentes. Supongamos que Fm y Fm+n son identicas, entonces Fm-1 y Fm+n-1 seraún reducidas, contiguas a la misma forma reducida por la parte primera, y por lo tanto identicas. De la misma manera Fm-2 y Fm+n-2 serún identicas, etc., y finalmente F y Fn. De este modo, en la progresión F, F0, F00 etc., si se prosigue suficientemente, necesariamente vuelve a aparecer la primera forma F. Si suponemos que Fn es la primera identica a F, o sea todas F0, F00, ...Fn-1 son diferentes de la forma F, se percibe que todas las formas F, F0, F00, ...Fn-1 son diferentes. Llamaremos al conjunto de estas formas el periodo de la forma F. Por lo tanto, si la progresion se prolonga mas alla de la ultima forma del período, del mismo modo tendremos de nuevo las formas F, F0, F00 etc. y toda la progresiún infinita F, F0, F00 etc. estarú constituida por este período de la forma F repetido infinitas veces.

La progresiún F, F0, F00etc. tambien puede prolongarse al reves, con anteponer a la forma F la reducida 0F, la cual es contigua a F por la parte primera. Delante de esta pondremos la reducida 00F, la cual es contigua a ella por la primera parte etc. De esta manera se tiene una progresion de formas infinita por ambos lados:

...000 F, 00 F, 0F, F, F0, F00, F000 ...

Se ve que 0F sera identica con Fn-1, 00F con Fn-2 etc. y por lo tanto la progresion por el lado izquierdo tambien estará compuesta del período de la forma F repetida infinitas veces.

Si a las formas F, F0, F00 etc. 0F, 00F, etc. se les atribuyen los índices 0, 1, 2, etc. -1, -2, etc. y en general a la forma Fm el índice m, a la forma mF el índice

—m, entonces formas cualesquiera de la serie serán idénticas o diferentes, según los 'índices de ellas mismas sean congruentes o incongruentes según el modulo n.

Ejemplo. Para la forma (3, 8, —5), cuyo determinante es = 79, se encuentra este período: (3, 8, —5), (—5, 7, 6), (6, 5, —9), (—9,4, 7), (7, 3, —10), (—10, 7, 3). Despues de la última, de nuevo tenemos (3, 8, —5). Así pues n = 6.

187.

Tenemos aquí algunas observaciones generales sobre estos períodos

1. Si las formas F, F', F" etc.; 'F, "F, '''F etc. se presentan así:

(a, b, —a'), (—a',b',a"), (a",b", —a'") etc.

(—'a,' b, a), (''a,00 b, —'a), (—''''a,'0' b,'' a)

todos los a, a', a'', a'0' etc. y 'a, ''a, '''a etc. tendrún el mismo signo (artículo 184, proposición 1), y todos los b, b', b'' etc. 'b, ''b etc. serán positivos.

1. De esto es evidente que el nímero n (el nímero de formas de las cuales estí compuesto el período de la forma F) siempre es par. Pues el primer termino de la forma Fm de este período tendrá el mismo signo que el primer termino a de la forma F si m es par; el signo opuesto si m es impar. Puesto que Fn y F son identicas, n sería necesariamente par.
2. El algoritmo mediante el cual se encuentran los numeros b', b'', b''' etc., a'', a'0' etc., por la proposition 6 del artículo 184, es este:

b' = —b (mod. a') entre los límites \/D y λ/D T a';

D — b'2a'

D — b0'2

***a***

D — b'0'27w

//

a =

b'' = —b' (mod. a'') λ/D t a'';

///

a =

b''' = -b'' (mod. a'0') 4D T a''';

*lili*

a =

etc.

donde en la segunda columna, el signo superior o el inferior debe tomarse, segín a, a', a'' etc. sean positivos o negativos. En lugar de las formulas en la tercera columna,

b' + b"

a = (b' - b") + a

***a***

b'' + b'''

////

nn ,rri\ **, //**

(b — b ) + a

pueden darse las siguientes, las cuales llegan a ser más cómodas, cuando D es un número grande:

„ = b + b', a

*a*

*b+b*

= —~r(b- b) +

a

a =

etc.

1. Una forma cualquiera Fm, contenida en el período de la forma F, tiene el mismo período que F. A saber, este período serú Fm, Fm+1, . ..Fn-1, F, F', . . .Fm-1, en el cual aparecen las mismas formas y en el mismo orden que en el período de la forma F. Este discrepa de aquel únicamente respecto del inicio y del fin.
2. Es claro que todas las formas reducidas de un mismo determinante D pueden distribuirse en períodos. Tímese libremente alguna de estas formas F y busquese su período F, F', F'', ...Fn—1, el cual denotaremos por P. Si no se comprenden todas las formas reducidas del determinante D, sea G alguna no contenida en el, y sea Q el período de ella. Entonces, es claro que P y Q no podran tener ninguna forma común; de otra manera G tendría que estar contenida tambien en P y los períodos coincidiran totalmente. Si P y Q aín no agotan todas las formas reducidas, alguna de las faltantes, H, suministrara un tercer período, R, el cual no tendra una forma en comun con P y tampoco con Q. Podemos continuar en esta manera hasta agotar todas las formas reducidas. Por ejemplo, todas las formas reducidas del determinante 79 se distribuyen en seis períodos:
3. (1, 8, —15), (—15, 7, 2), (2, 7, —15), (—15, 8,1).
4. (—1, 8,15), (15, 7, —2), (—2, 7,15), (15,8, —1).
5. (3, 8, —5), (—5, 7, 6), (6, 5, —9), (—9,4, 7), (7, 3, —10), (—10, 7, 3).
6. (—3,8,5), (5, 7, —6), (—6,5,9), (9,4, —7), (—7,3,10), (10, 7, —3).
7. (5,8, —3), (—3, 7,10), (10,3, —7), (—7,4,9), (9,5, —6), (—6, 7,5).
8. (—5,8,3), (3, 7, —10), (—10,3, 7), (7,4, —9), (—9,5,6), (6, 7, —5).
9. Llamaremos formas asociadas a las que constan de los mismos terminos, pero puestos en orden inverso, como (a, b, —a'), (—a',b, a). Entonces, se percibe de la proposicion 7 del artículo 184 que si el período de la forma reducida F es F, F',

F00, ...Fn-1, y si la forma f es asociada a F y las formas f0, f00, . ..fn-2, fn-1 son asociadas a las formas Fn-1, Fn-2, ...F", F0, respectivamente, entonces el período de la forma f será f, f, f00, ...fn-2, fn-1, y por lo tanto constara de tantas formas como el período de la forma F. Llamaremos períodos asociados a aquellos de las formas asociadas. Así, en nuestro ejemplo, son asociados los períodos III y VI, IV y

V.

1. Pero puede ser que la forma f aparezca en el período de su asociado F, como en nuestro ejemplo de los períodos I y II y, por tanto, el período de la forma F concuerde con el período de la forma f, o sea que el período de la forma F sea asociado a sí mismo. Cada vez que esto suceda se encontraran dos formas ambiguas en este período. Supongamos que el período de la forma F consta de 2n formas, o sea F y F2n son identicas, y sea 2m + 1 el índice de la forma f en el período de la forma F [[149]](#footnote-150)), o sea F2m+1 y F son asociadas. Entonces es claro que tambien F0 y F2m serán asociadas, ademas de F00 y F2m-1 etc., y por tanto Fm y Fm+1. Sea Fm = (am,bm, -am+1), Fm+1 = (-am+1 ,bm+1,am+2). Entonces tendremos bm + bm+1 = 0 (mod. am+1); de la definiciín de las formas asociadas serí bm = bm+1 y de esto 2bm+1 = 0 (mod. am+1), o sea la forma Fm+1 es ambigua. Del mismo modo F2m+1 y F2n serán asociadas; de esto F2m+2 y F2n-1; F2m+3 y F2n-2 etc., finalmente Fm+n y Fm+n+1, de las cuales la segunda sera ambigua, como se prueba con facilidad por razonamiento semejante. Dado que m + 1 y m + n + 1 son incongruentes segín el modulo 2n, las formas Fm+1 y Fm+n+1 no serán identicas (artículo 186, donde n denota lo mismo que 2n aquí). Así en I, las formas ambiguas son (1, 8,-15), (2, 7, -15), en II son (-1, 8,15), (-2, 7,15).
2. Viceversa, cada período, en el cual aparece una forma ambigua, es asociado a sí mismo. En efecto, se ve que, si Fm es una forma reducida ambigua, a la vez la forma sera contigua a su asociada (que tambien es reducida) por la parte primera, i.e., Fm-1 y Fm son asociadas. Entonces todo el período serí asociado a sí mismo. Es claro que no puede ser que solo una forma ambigua estí contenida en algUn período.
3. Tampoco puede haber más de dos en un mismo período. Supongamos que en el período de la forma F, compuesta de 2n formas, se presentan tres formas ambiguas F\ Fμ y Fv, pertenecientes a los índices λ, μ y ν, respectivamente de tal manera que λ, μ y ν sean nímeros diferentes situados entre los límites 0 y 2n - 1

(inclusive). Entonces las formas Fλ-1 y Fλ serán asociadas; y al mismo tiempo Fλ-2 y Fetc., y finalmente F y F2^-1. Por el mismo razonamiento, F y F2^-1 serán asociadas, ademas de F y F2v-1; por lo cual F2^-1, F2^-1 y F2v-1 serán identicas, y los índices 2λ — 1, 2μ — 1, 2ν — 1 serán congruentes, segán el modulo 2n, y por eso tambien λ ξ μ ξ ν (mod. n), Q. E. A. , puesto que claramente no pueden caer entre los límites 0 y 2n — 1 tres numeros diferentes congruentes, segun el modulo n.

188.

Puesto que todas las formas del mismo período son propiamente equivalentes, la pregunta que surge es cuales formas de diferentes períodos pueden ser tambien equivalentes. Pero antes de mostrar que esto es imposible, debemos decir algo acerca de la transformacion de las formas reducidas.

Puesto que la transformación de formas frecuentemente sera tratada abajo, evitaremos la prolijidad tanto como sea posible y usaremos el siguiente metodo mas corto de escribir. Si la forma LX2 + 2MXY + NY2 es transformada en la forma lx2 + 2mxy + ny2 por la sustitucion X = αx + βy, Y = γx + óy, diremos simplemente que (L,M,N) es transformada en (l,m, n) por la sustitucion α, β, γ, ó. De esta manera no sera necesario denotar por caracteres propios las incognitas de cada una de las formas que esrán siendo tratadas. Es obvio que la primera incognita deberá distinguirse bien de la segunda en cualquier forma.

Sea (a, b, —a') ...f una forma reducida dada con determinante D. Como en el artículo 186, formamos una serie de formas reducidas infinita en ambas direcciones ...''f, 'f, f, f, f', ... y sea

f = (—a',tb,a"), f = (a'',b", —a''') etc. f = (—'a,'b, a), ''f = ("a,"b, — 'a) etc.

Pongase

*b±b[* = *h'*

-a' = h ,

0b±b = h

a h,

*b'+b*

, b-±T = h''' etc.

^ =' h, ='' h etc.

= h''

a'' = h ,

Entonces es claro que si (como en artículo 177) los námeros α', α'', α''', etc., β', β''β''', etc., etc., son formados según el siguiente algoritmo

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| α | = 0 | β | = —1 |  | γ | = 1 | δ | =h |
| α | = β' | β | = h β |  | γ | =δ | δ | = h δ — 1 |
| α | =β | β | = h β — | β | γ | =δ | δ | = h δ — δ |
| α | =β | β | = h β | —β | γ | =δ | δ | = h δ — δ |

etc.

f sera transformada

en f' por la sustitución α', β', γ', δ'

en f' α'', β'', γ'', δ''

en f''' α''', β''', γ''', δ'''

etc.

y todas estas transformaciones serán propias.

Puesto que 'f se transforma en f por la sustitución propia 0, -1, 1, h (art. 158), f sera transformada en 'f por la sustitucion propia h, 1, -1, 0. Por razonamiento similar, 'f seró transformada en ''f por la sustitución propia 'h, 1, —1, 0; ''f en '''f por la sustitución propia ''h, 1, —1, 0 etc. De esto, por el articulo 159, concluimos, de la misma forma como en el artículo 177, que si los nómeros 'α, ''α, '''α, etc., 'β, ''β, '''β, etc., etc., son formados segun el siguiente algoritmo

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| α = | h | β= | 1 | γ= | —1 | δ= | 0 |
| ''α = | 'h/α — 1 | β= | α | γ= | h γ | ''δ = | γ |
| '''α = | ''Λ"α — 'α | '''β = | ''α | '''γ = | ''Λ"γ — 'γ | '''δ = | γ |
| ''''α = | '''Λ"'α — ''α | ''''β = | '''α  etc. | ''''γ = | '''Λ"'γ — ''γ | ''''δ = | γ |

entonces f seróa transformada

en f por la sustitucioón α, β, γ, δ

en ''f ''α, ''β, ''γ, ''δ

en '''f '''α, '''β, '''γ, '''δ

etc.

y todas estas transformaciones serán propias.

Si se pone α = 1, β = 0, γ = 0, δ = 1, estos números tendrán la misma relacián con la forma f que α0, β0, γ0, δ0 tienen con f0; α00, β00, γ00, δ00 tiene con f00 etc.; 0α, 0β, 0γ, 0δ con 0f etc. Es decir, por la sustitución α, β, γ, δ la forma f será transformada en f. Entonces las series infinitas α0, α00, α000, etc., 0α, 00α, 000α etc. serón claramente puestas juntas por la insertion del termino α de modo que puedan ser concebidas como una serie infinita continua en ambas direcciones de acuerdo a la ley de progresián ... , 000α, 00α, 0α, α, α0, α00, α000, .... La ley de progresion es la siguiente

α + α — h α, α + α — h α, α + α — ύα, α + α

ύ0α0, α0 + α000

ύ00α00 etc.

o en general (si suponemos que un índice negativo indica la misma cosa escrito a la derecha que un índice positivo escrito en la izquierda)

α™-1 + αη+1 = ύ™α™

De una manera similar la serie ... , 00β, 0β, β, β0, β00, ... sera continua, y su ley es

β

η1

+ βη+1

hm+1 β™

Esta serie es identica a la precedente si cada termino es movido hacia arriba un lugar 00β = 0α, 0β = α, β = α0, etc. La ley para la serie continua ... , 00γ, 0γ, γ, γ0, γ00, ...

seráa

γη-1 + γ m+1 = ύ™γ™

y la ley para ... , 00δ, 0δ, δ, δ0, δ00, ... será

δ™-1 + δη+1 = ύη+1δη

y generalmente δ™ = γη+1.

Ejemplo. Sea f la forma (3, 8, -5) la cual se transformará

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| en la forma f | (—10, 7, 3) | por la sustituciáon — 805, | —152, | +143 | , +27 |
| ''''''f | (3, 8, —5) | — 152, | +45, | +27, | —8 |
| f | (—5, 7,6) | +45, | +17, | —8, | —3 |
| f | (6,5, —9) | +17, | —11, | —3, | +2 |
| f | (—9,4,7) | —11, | —6, | +2, | +1 |
| f | (7, 3, —10) | —6, | +5, | +1, | —1 |
| f | (—10, 7, 3) | +5, | +1, | —1, | 0 |
| f | (3,8, —5) | +1, | 0, | 0, | +1 |
| f | (—5, 7,6) | 0, | —1, | +1, | —3 |
| f | (6,5, —9) | —1, | —2, | —3, | —7 |
| f | (—9,4,7) | —2, | +3, | —7, | +10 |
| f | (7,3, —10) | +3, | +5, | +10, | +17 |
| f | (—10, 7, 3) | +5, | —8, | +17, | — 27 |
| f | (3,8, —5) | —8, | —45, | —27, | — 152 |
| f | (—5, 7,6) | —45, | +143, | — 152, | +483 |

etc.

negativo, por un razonamiento parecido encontramos o00 negativo, o000 positivo y > o = o00; o"" positivo > o000; o!"" negativo > o0000; etc., de modo que la serie o0, o00, o000, etc., crezca continuamente, y el signo del termino om será +, —, —, +, segun sea m = 0, 1, 2, 3 (mod. 4)

1. De esta forma encontramos que las cuatro progresiones o0, o00, o000, etc., γ, γ0, γ00, etc., o0, o, 0o, 00o, etc., γ, 0γ, 00γ, etc., crecen continuamente y entonces todas las siguientes, que son identicas a ellas: β, β0, β00, etc., 0δ, δ, δ0, δ00, etc., β, 0β, 00β, etc., 0δ, 00δ, etc., y segun sea m = 0, 1, 2, 3 (mod. 4), el signo

de om, + ± — ψ de γ™, ± + ψ —; de mo, + ± — ψ de , ψ — ± +;

de β™, ± — ψ + de δ™, + ψ — ± de ™β, ψ + ± — de ™δ, + ψ — ±

con el signo superior usado cuando a es positivo, el inferior cuando a es negativo. Tengase en cuenta esta propiedad: si designamos cualquier índice positivo por m, om y γ™ tendrán el mismo signo cuando a es positivo, signos opuestos cuando a es negativo, y similarmente para βm y δ™; por el otro lado mo y ™γ o ™β y ™δ tendrán el mismo signo cuando a es negativo, opuesto cuando a es positivo.

1. Usando la notación del artículo 27 podemos mostrar el tamaño de los námeros om etc., poniendo

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Th0 = | = k0, ±h00 | = k00, ψδ000 = | k000 | etc. | ± h | = k, ψ0δ = 0k, | ±00h |
| tal que | todos los námeros k0, k00, | | etc.; | k, 0k, | etc., | sean positivos: |  |
|  | o™ = | ±[k00,k000,k0000, | ...k™-1]; | | β™ | = ±[k00,k000,k0000, | ...k™] |
|  | γ™ = | ±[k0,k00,k000,. . | .. k™-1]; | | δ™ | = ±[k0,k00,k000,. | ... k™] |
|  | ™o = | ±[k,0k,00k, ... |  | -1k]; | ™β | = ±[k,0k,00k, ... | ™-2k] |
|  | ™γ = | ±[ 0k, 00k, |  | -1k]; | ™δ | = ±[ 0k, 00k, | ™-2k] |

00k etc.

Los signos deberán ser determinados por lo que acabamos de decir arriba. A traves de estas formulas, cuya demostracion omitiremos por ser muy facil, el computo involucrado puede hacerse muy rápidamente.

190.

LEMA: Designemos enteros cualesquiera por las letras m, μ, m', n, v, n' de tal forma que ninguno de los Ultimos tres sea = 0. Afirmo que si μ está estrictamente entre los lámites f y fr y si mn*'* — nm' = ^1, entonces el denominador v sera mayor que n y n'.

Demostración. Manifiestamente μnn' estará entre vmn' y vnm', y entonces la diferencia entre este námero y cada límite sera menor que la diferencia entre un límite y el otro; i.e., tenemos vmn' — vnm' > μnn' — vmn' y > μnn' — vnm', o ν > n'^n — vm) y > n^n' — vm'). Entonces se sigue que, puesto que μn — vm no es = 0 (puesto que de otra manera tendríamos μ = f contrariamente a la hipótesis) y tampoco μ^ — vm' = 0 (por una razán similar), pero cada uno será al menos = 1, por lo tanto v > n' y > n. Q. E. D.

Es por lo tanto claro que v no puede ser = 1; i.e., si mn' — nm' = ±1 ningun entero puede estar entre las fracciones f y fr. Tampoco cero puede estar entre ellas, i.e., las fracciones no pueden tener signos contrarios.

191.

TEOREMA. Si la forma reducida (a,b, —a') con determinante D es transfor­mada por la sustitucián a, β, γ, δ en la forma reducida (A, B, —A') con el mismo determinante: Primero, estará entre α y μ (siempre y cuando ni γ ni δ = 0,

*i.e.,* si cada limite es finito). El signo superior debe ser usado cuando ninguno de estos limites tiene un signo contrario al de a (o más claro, cuando ambos tienen el mismo signo o uno tiene el mismo signo, el otro =0). El signo inferior debe ser usado cuando ninguno tiene el mismo signo de a. Segundo, *±^ +* estará entre α y β (siempre y cuando ni α ni β = 0). El signo superior debe ser usado cuando ningún

límite tiene un signo contrario al signo de a' (o a), el signo inferior cuando ninguno

tiene el mismo signo de a' [[150]](#footnote-151)).

Demostraciáon. Tenemos las ecuaciones

aa2 + 2baY — a'Y2 = A [1]

aβ2 + 2bβδ — a^2 = — A' [2]

De esto deducimos

α *μ .* .

|  |  |  |  |
| --- | --- | --- | --- |
| ±f | + | aA  Ψ | -b |
|  | a |  |  |
|  | - | aA' | -b |
|  | a |  |  |
| ±qD | - | a'A  O2 | +b |
| a | | | |
| ± d | + | a'A | " + b |

α

[3]

γ ~

± *Id* — aA" - b

[4]

[5]

β a [6]

Las ecuaciones [3], [4], [5], [6] deben descartarse si γ, δ, α, β son respectivamente = 0. Pero todavía queda la duda acerca de cuales signos deben darse a las cantidades en radicales. Vamos a decidir esto de la siguiente manera.

Es claro inmediatamente que con [3] y [4] el signo de arriba debe ser usado cuando ni ° ni f tengan un signo contrario al de a, porque si el signo inferior fuera usado, y serían cantidades negativas. Ahora, puesto que A y A0 tienen el

mismo signo, vD cae entre D + y \JD — ^2" y así en este caso caera

entre α y f. Entonces la primera parte del teorema ha sido demostrada para el caso anterior.

De la misma manera vemos que en [5] y [6] los signos inferiores deben tomarse cuando ni O ni f tenga el mismo signo de a0 o a, porque si tomamos el signo superior,

y η^· serían necesariamente cantidades positivas. Entonces sucedería en este caso

que ~+b estaría entre O y f. Por lo tanto la segunda parte del teorema queda mostrada para el último caso. Ahora, si hubiera sido igualmente facil mostrar que en [3] y [4] los signos inferiores deberían ser tomados cuando ninguna de las cantidades α y f tiene el mismo signo de a, y los signos superiores en [5] y [6] cuando ni O ni f

tienen signo opuesto, entonces se seguiría para el primer caso que —estí entre O y f y para el ultimo caso que estí entre O y f; es decir, la primera parte del

teorema quedaría demostrada para el ultimo caso y la segunda parte para el primer caso. Pero aunque esto no es difícil, no se puede hacer sin algunas ambigüedades y preferimos entonces el siguiente míetodo.

Cuando ninguno de los nímeros α, β, γ, δ = 0, entonces α y f tendrán los mismos signos que O y f. Cuando, por lo tanto, ninguna de estas cantidades tiene el

signo que a' o a, y entonces está entre α y β, ninguna de las cantidades

α y δ tendra el mismo signo de a y VD+ = —^a~b (puesto que aa' = D — b2)

mismo

α \_ γ y δ

estaran entre α y βδ. Por lo tanto para el caso en que ni α ni β = 0, la primera parte del teorema cubre el segundo caso (pues la condición que ni γ ni δ = 0 ha sido considerada en el mismo teorema). De una forma similar cuando ninguno de los námeros α, β, γ, δ = 0 y ni α ni δ tiene el signo opuesto a a o a', y por eso esta

entre α y δ, entonces ni α ni ^ tendrán un signo opuesto al de a', y - = ^Hái+L· estará entre α y ^. Por lo tanto, donde ni γ ni δ = 0 la segunda parte del teorema demuestra el segundo caso.

Queda entonces por mostrar que la primera parte del teorema tambien se aplica al segundo caso si ninguno de los numeros α y β = 0, y que la segunda parte se aplica al primer caso si γ o δ = 0. Pero todos estos casos son imposibles. Supongase, pues, para la primera parte del teorema que ni γ ni δ = 0; que α y δ no tienen el mismo signo que a y que (1) α = 0. Entonces, de la ecuacion αδ — βγ = ±1 tenemos β = ±1, γ = ±1. Y de [1] A = —a', por lo tanto A y a' y entonces tambien a y A' tendrán signos opuestos y yjD — aA > \/D > b. De esto es claro que en [4] se toma necesariamente el signo inferior porque, si tomamos el signo superior, δ tendría el mismo signo que a. Tenemos entonces δ > > 1 (puesto que a < \JD + b

por la definition de una forma reducida), Q. E. A. , pues β = ±1, y δ no es = 0. (2) Sea β = 0, entonces, por la ecuacion αδ — βγ = ±1 tenemos α = ±1, δ = ±1.

De [2] —A' = —a', así a', a y A tendrán el mismo signo y yjD + > λ/D > b. Por

lo tanto claramente en [3] tenemos que tomar el signo inferior porque si tomamos el signo superior, α tendría el mismo signo de a. Obtenemos entonces α > —> 1, Q. E. A. , por la misma razon de antes. Para la segunda parte, si suponemos que ni α ni β = 0; que α y β no tienen signos opuestos al de a' y que (1) γ = 0: de la ecuacion αδ — βγ = ±1 obtenemos α = ±1, δ = ±1. Entonces por [1] A = a y a' y A'

tendrán el mismo signo y entonces D + > y/D > b. Por lo tanto en [6] se tiene

que tomar el signo superior porque si tomamos el signo de abajo, ^ tendría un signo

opuesto al de a'. Obtenemos entonces δ > > 1, Q. E. A. , porque δ = ±1 y

β no es = 0. Finalmente (2), si fuera δ = 0, de αδ — βγ = ±1 tendríamos β = ±1, γ = ±1 y así de [2] —A' = a. Por lo tanto yjD — DA > VD > b, y se debe tomar el

signo superior en [5]; α > > 1, Q. E. A. Y el teorema está demostrado en

toda su generalidad.

Puesto que la diferencia entre α y β es = γδ, la diferencia entre b y γ

o β sera < γδ; entonces, entre y γ o entre esa cantidad y β no puede haber

fracciones cuyo denominador no sea mayor que y o δ (lema precedente). De la misma manera, la diferencia entre la cantidad y la fracción β o β sera menor que

γβ, y ninguna fracción puede estar entre esa cantidad y alguna de estas fracciones a no ser que el denominador sea mayor que a y β.

192.

Con la aplicacion del teorema precedente al algoritmo del artículo 188 se sigue que la cantidad , la cual designaremos con L, estará entre SLT y °r; entre y

o" /// *offf*

βπ; entre γτ^ y , etc. (puesto que es facil de ver por el artículo 189.3, hacia el final, que ninguno de estos límites tiene un signo opuesto al de a, así, se debe dar un signo positivo a la cantidad radical \/D); o entre γ, y βττ; entre γ,, y αm, etc. Por

/ α 777 α77777

lo tanto todas las fracciones γ, γ,, γ"" , etc. estaran en un lado de L, y todas las fracciones γ,, γ,,, γ,,,,,,, etc. en el otro lado. Pero, puesto que y < y , γ estaró fuera de γ, y L, y por una razón analoga γ estará fuera de L y γ,,; γ, fuera de L

γ00000

./// \*

y γ™,; etc. Entonces estas cantidades esrán en el siguiente orden:

α0

y’

α

.///

γ

*a'"" ynn* ’

...L’

|  |  |  |
| --- | --- | --- |
| a'''''' | a'''' | a' |
| y'''''' ’ | y'''' ’ | y'' |

La diferencia entre γ, y L sera menor que la diferencia entre γ, y γ; i.e. < γτγπ, y por una razón anóloga la diferencia entre γ y L seró < γ,,γ,,, etc. Por lo tanto, las

fracciones ψ, ^, y-, etc. se aproximarón continuamente al límite L y, puesto que y', y'', y00' crecen indefinidamente, la diferencia entre las fracciones y el Emite puede hacerse menor que cualquier cantidad dada.

Por el artóculo 189, ninguna de las cantidades y, γγ, , etc. tendró el mismo

signo que a; entonces, por el razonamiento de arriba, estos numeros y la cantidad ~, que designaremos por L', estaran en el siguiente orden:

|  |  |
| --- | --- |
| 1 | ''y |
| ’  a | ''a |

*'"y . '""y*

''''a’ ... ’ ... *'''''a’*

*m\_y\_*

*'''a’*

*'y*

*'a*

La diferencia entre γ y L0 será menor que t1-, la diferencia entre -A y L0 menor que

α J ^ / 'αα 'α J n

1. etc. Por lo tanto, las fracciones α, 70., etc. se aproximarán continuamente a L0

''α'α ’

y la diferencia puede hacerse menor que cualquier cantidad dada.

En el ejemplo del artículo 188 tenemos L = = 0,2960648, y las

143

fracciones aproximantes son 1, ^, 2, 10, 17, 27, 152, iÜ, etc., y 183 = 0, 2960662. En

el mismo ejemplo L0 = ~v^9+8 = -0,1776388, y las fracciones aproximantes son 0,

\_i \_ 1 \_A \_A \_A —AL \_ 143 etc "

5, 6, 11, 17, 45, 152, 805 , etc.

De hecho 843 = 0,1776397.

193.

TEOREMA. Si las formas reducidas f y F son propiamente equivalentes, cada una de ellas estará contenida en el período de la otra.

Sea f = (a, b, — a0) y F = (A, B, — A!) y el determinante de estas formas D, y transfármese la primera en la segunda por la sustitucián propia A, B, C, D. Si se busca el período de la forma f y se calcula la serie infinita de dos sentidos de las formas reducidas y las transformaciones de la forma f en áestas, como hicimos en el artículo 188, entonces o bien +A sera igual a algán termino de la serie ..." α, 0α, α, α0, α00, ... (y si lo ponemos = am, +B sera = β™, +C = qm, +D = ám); o bien —A sera igual a algán termino α™ y — B, —C, —D, respectivamente, serán = β™, qm, óm (donde m puede designar tambien un ándice negativo). En cualquier caso F sera identico a fm.

Demostración. I. Tenemos las cuatro ecuaciones

aA2 + 2bAC — a0C2 = A [1]

aAB + b(AD + BC) — a0CD = B [2]

aB2 + 2bBD — a0D2 = — A0 [3]

AD — BC =1 [4]

Consideremos primero el caso donde uno de los numeros A, B, C, D =0.

1o Si A = 0 resulta por [4] BC = —1, y así B = ±1, C = ^1. Entonces por [1], —a0 = A; por [2], —b±a0D = B o B = —b (mod. a0 o A); por lo tanto, se deduce que la forma (A, B, — A0) es contigua por la parte ultima a la forma (a, b, —a0). Puesto que la primera de estas es reducida, sera necesariamente identica a f0. Por lo tanto B = b0, y entonces de [2] b + b0 = —a0CD = ±a0D; de esto, puesto que = h0,tenemos que D = ^h'. De esto se colige que ^A, ^B, ^C, ^D son respectivamente = 0, -1, +1, h', o = α', β', τ', δ'.

2o Si B = 0 tenemos de [4] A = ±1, D = ±1; de [3] a' = A'; de [2] b^a'C = B,

1. b = B (mod. a'). Pero, como f y F son formas reducidas, ambas b y B estarán entre \/D y \/D ^ a' (según a' sea positivo o negativo, por el art. 184.5). Así, sera necesariamente, b = B y C = 0. Entonces las formas f y F son identicas y ±A, ±B, ±C, ±D = 1, 0, 0, 1 = α, β, τ, δ respectivamente.

3o Si C = 0 tenemos de [4] A = ±1, D = ±1; de [1] a = A; de [2] ±aB+b = B o b = B (mod. a). Dado que tanto b como B estan entre \/D y λ/D^a, necesariamente se tendrú que B = b y B = 0. Así, este caso no difiere del precedente.

4o Si D = 0, tenemos de [4] B = ±1, C = ^1; de [3] a = -A'; de [2] ±aA — b = B o B ξ —b (mod. a). Entonces la forma F sera contigua por la primera parte a la forma f y así identica a la forma 'f. Por lo tanto, puesto que = h y B = 'b tenemos ±A = h. De aquí se colige ±A, ±B, ±C, ±D respectivamente = h,

1. —1 0 = 'α 'β 'τ> 'δ.

Solo queda el caso donde ninguno de los números A, B, C, D = 0. Por el lema del artículo 190, las cantidades C, Djy, A, B tendrán el mismo signo y resultaran dos casos según este signo sea el mismo o el opuesto al signo de a y a'.

II. Si C y B tienen el mismo signo que a, la cantidad b (la cual designaremos por L) estarú entre estas fracciones (art. 191). Ahora demostraremos

A // /// //// b

que c es igual a una de las fracciones O', οτττ, O"", etc. y -y a la siguiente; esto es, si

C *III y*

A fuera =

*α*

m

I

m

B

entonces seria

am+T ym+T.

En el artículo precedente mostramos que

las cantidades αψ, αψΤ, yv, etc. (a las que por brevedad denotaremos por (1), (2), (3), etc.) y L sigue este orden (I): (1), (3), (5), ...L, ... (6), (4), (2). La primera de estas cantidades es = 0 (puesto que α' = 0); el resto tiene el mismo signo de L o a. Pero, puesto que por hipútesis y y (para los cuales escribimos M y N) tienen el mismo signo, es claro que estas cantidades estan a la derecha de (1) (o si se prefiere en el mismo lado que L) y, de hecho, puesto que L esta entre ellas, una esta a la derecha de L, la otra a la izquierda. Con facilidad, puede mostrarse que M no puede estar a la derecha de (2), pues de otra manera N estaría entre (1) y L, de donde resultaría primero que (2) esta entre M y N, y el denominador de la fracciún (2) sería mayor que el denominador de la fracción N (art. 190); segundo que N estaría entre (1) y (2) y el denominador de la fraccion N sería mayor que el denominador de la fracciún

(2), *Q.E.A.*

Supongamos que M no es igual a ninguna de las fracciones (2), (3), (4), etc. Veamos lo que sucede. Si la fracción M está a la izquierda de L, estará necesariamente entre (1) y (3), o entre (3) y (5), o entre (5) y (7), etc. (porque L es irracional, y entonces ciertamente no igual a M, las fracciones (1), (3), (5), etc. pueden aproximarse mas a L que a cualquier cantidad dada diferente a L). Ahora, si M está a la derecha de L, estará necesariamente entre (2) y (4), o entre (4) y (6), o entre (6) y (8), etc. Supongamos entonces que M esta entre (m) y (m + 2); es obvio que las cantidades M, (m), (m + 1), (m + 2), L están en el siguiente orden

(II)[[151]](#footnote-152)): (m), M, (m + 2), L, (m + 1).

Entonces, necesariamente, N = (m +1). Ahora N estará a la derecha de L; pero si tambien esta a la derecha de (m +1), (m +1) estará entre M y N, de donde γ™+1 > C, y M estará entre (m) y (m + 1), y por tanto C > ym+1 (art. 190), Q. E. A. Pero si N estuviera a la izquierda de (m + 1), es decir entre (m + 2) y (m + 1), tendríamos D > γm+2, y puesto que (m + 2) está entre M y N, tendríamos γ™+2 > D, Q. E. A. Tenemos, por lo tanto , N = (m +1); es decir ^ = β™.

Puesto que AD — BC = 1, B será primo con D, y por razán similar β™ sera primo con ám. Entonces, se ve que la ecuacián d = no puede ser consistente a menos que B = βm, D = óm o B = —β™, D = —ám. Ahora, puesto que la forma f se transforma por la sustitucion propia am, βm, ym, óm en la forma fm, que es (±am,bm, ^am+1), tendremos las ecuaciones

+ 2bamYm — α'γ2™ = ±am

aa2m

[5]

[6]

[7]

[8]

αα™β™ + b(amám + β™γ™) — α0γ™δ™ = bm

αβ2m + 2bβmδm — a'á2m = ^am+1 amám — β™γ™ = 1

De aquí resulta (de las ecuaciones [7] y [3]): ^am+1 = —A0. Adicionalmente, al multiplicar la ecuacián [2] por amám — β™γ™, la ecuacion [6] por AD — BC y al restar obtenemos por un cáalculo fáacil que:

B — bm = (Cam — Αγ™)^βm + b(Dβm + Bám) — a'Dám)

+ (Bám — Dβm)(αAαm + b(Cam + Αγ™) — a,Cγm) [9]

o puesto que βm = B, δ™ = D o βm = -B, δ™ = -D

B - bm = ±(Ca™ - Αγm)(aB2 + 2bBD - a'D2) = *t(Co™ -* Ay™)A'

Entonces B = bm (mod. A'); y puesto que tanto B como bm están entre -\/D y VD ψ A' tendremos B = b™, y asl Ca™ - Ay™ = 0 o A = «m; i.e., M = (m).

De esta forma, entonces, dedujimos de la suposición que M no es igual a ninguna de las cantidades (2), (3), (4), etc., que de hecho es igual a alguna de ellas. Pero, si suponemos desde el principio que M = (m), tendremos claramente A = a™, C = γ™ o -A = a™, -C = γm. En cualquier caso, resulta de [1] y [5] A = ±am y de [9] B - bm = ±(Bhm - Dem)A o B = bm (mod. A). De esto concluimos de la misma forma como arriba que B = bm, y entonces Bhm = Dem; por lo tanto, puesto que B es primo con D y β™ con óm, sera entonces B = β™, D = óm o -B = β™, -D = óm, y de [7] -A' = ^am+1. Entonces las formas F y fm serán identicas. Con la ayuda de la ecuacion AD - BC = Cimóm - β™γ™ no es difícil mostrar que, cuando +A = am, +C = γ™ debe ponerse +B = β™, +D = óm; y por el otro lado, cuando -A = α™, -C = γ™ debe ponerse -B = β™, -D = δ™. Q. E. D.

1. Si el signo de las cantidades A etc. es opuesto al de a, la demostracion es tan similar a la precedente que es suficiente anadir solamente los puntos principales. La cantidad -estará entre A y D. La fraccion BB sera igual a una de las fracciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 'δ | ''δ | '''δ | (I) |
|  |  |  | , etc |
|  | 'β' | ''β' | '''β' |
| ™δ  y si se pone esta = —-,  J r mo 1 |  |  | C ™γ — sera =  A ™α | (II) |

Se demuestra (I) como sigue: si suponemos que B no es igual a ninguna de estas

D B

m+2 g

fracciones, deberá caer entre dos de ellas y m+Τβ. De donde, de la misma manera como se deduce arriba, mostramos que

C ™+1δ ™γ

A = ™+Τβ =

y, o bien A = ™α, C = ™γ o bien -A = ™α, -C = ™γ. Pero puesto que por la sustitucion propia ™α, ™β, ™γ, ™δ se transforma f en la forma

™f = (±™a, ™b, T™-1a)

podemos derivar tres ecuaciones. De estas y de las ecuaciones [1], [2], [3], [4] y la ecuación ηαηδ — ιηβιηγ = 1 deducimos de la misma manera que arriba que el primer termino A de la forma F es igual al primer termino de la forma mf y que el termino del medio de la anterior es congruente (segón el modulo A) al termino del medio del óltimo. Puesto que ambas formas son reducidas, el termino del medio de cada una esta entre vD y y/D ^ A, y entonces estos terminos del medio serán iguales. De esto concluimos que = —■ . La veracidad de la afirmación (I) es derivada suponiendo que esto es falso.

Supongase que m^ = —-. De la misma forma y usando las mismas ecuaciones, podemos mostrar que ma = C, que era la segunda afirmacion (II). Ahora, con la ayuda de las ecuaciones AD — BC = 1, ηαηδ — ιηβιηγ = 1 deducimos que o bien

A = ma, B = ηβ, C = ηγ, D = mó

o bien

—A = ma, —B = ηβ, —C = m7, —D = ηδ y las formas F y mf son identicas. Q. E. D.

194.

Puesto que las formas que arriba hemos llamado asociadas (art. 187.6) son siempre impropiamente equivalentes (art. 159), es claro que si las formas reducidas F y f son impropiamente equivalentes, y si la forma G es la asociada de la forma F, entonces las formas f y G serán propiamente equivalentes y la forma G estará contenida en el período de la forma f. Y si las formas F y f son equivalentes tanto propiamente como impropiamente, es claro que ambas F y G deberan ser encontradas en el período de la forma f. Por lo tanto, este período seró un asociado de el mismo y contendrá dos formas ambiguas (art. 187.7). Entonces, se confirma perfectamente el teorema del artículo 165, ya garantizado, que podemos encontrar una forma ambigua equivalente a las formas F y f. [[152]](#footnote-153)

Solución. Búsquense dos formas reducidas F y f propiamente equivalentes a las formas dadas Φ y φ (art. 183). Ahora, segun que estos sean solo propiamente equivalentes o súlo impropiamente equivalentes o ambas o ninguna, entonces las formas dadas serún solo propiamente equivalentes, o solo impropiamente, o ambas o ninguna. Se calcula el período de una de las formas reducidas, e.g., el período de la forma f. Si la forma F aparece en este período aunque no la forma de su asociada, entonces tendrá lugar el primer caso; por otro lado, si la asociada aparece aquí pero F no, ocurre el segundo caso; si ambas aparecen, se da el tercer caso; si ninguna aparece, se da el cuarto caso.

Ejemplo. Sean las formas dadas (129,92, 65) y (42, 59, 81) con determinante 79. Para estas tenemos las formas reducidas propiamente equivalentes (10, 7, -3) y (5, 8, -3). El período de la primera de estas es : (10, 7, -3), (-3, 8, 5), (5, 7, -6), (-6, 5, 9), (9, 4, -7), (-7, 3, 10). Puesto que la forma (5, 8, -3) no aparece aquí sino solo su asociada (-3, 8, 5), concluimos que las formas dadas son solo impropiamente equivalentes.

Si todas las formas reducidas de un determinante dado son distribuidas de la misma forma que arriba (art. 187.5) en períodos P, Q, R, etc., y si se selecciona una forma de cada período al azar, F de P; G de Q; H de R, etc., entonces ningun par de las formas F, G, H, etc. podran ser propiamente equivalentes. Y cualquier otra forma del mismo determinante sera propiamente equivalente a una y solo una de estas. Entonces, todas las formas de este determinante pueden ser distribuidas en tantas clases como períodos tenga, esto es: poniendo las formas que son propiamente equivalentes a la forma F en la primera clase, aquellas que son propiamente equivalentes a G en la segunda clase, etc. De esta manera, todas las formas contenidas en la misma clase seran propiamente equivalentes, y las formas contenidas en clases diferentes no pueden ser propiamente equivalentes. Pero no nos detendremos aquí en este tema que sera tratado en detalle mas adelante. [[153]](#footnote-154)

tales que cada forma equivalga propiamente a su predecesora y las últimas Φη y φν sean formas reducidas. Y, puesto que supusimos que Φ y φ eran propiamente equivalentes, Φη estarú necesariamente contenida en el período de la forma φν. Sea φν = f y sea su período hasta la forma Φη :

f, f, f", ...f"-1, Φη

tal que en este período el índice de la forma Φη sea m; y se designaran las formas que son opuestas a las asociadas de las formas

Φ, Φ0, Φ00, ... Φη por Φ, Φ0, Φ00, . . . Φη respectivamente[[154]](#footnote-155))

Entonces en la sucesión

*φ, φ, φ*

,f, f, f0, *...f*

"1

Φ

η1

Φη-2, ... φ, Φ

cada forma serú contigua a la precedente por la última parte, y por el artículo 177 podemos obtener una transformacion propia de la primera φ en la última Φ. Esto es fúcil de ver para los otros terminos de la sucesion; para los terminos fm-1 y ψη-1 lo probamos como sigue: sea

fm-1 = (g,h,i); f" o Φη = (g,h',i'); Φη-1 = (g",h",i")

La forma (g ,h' ,i') sera contigua por la última parte de cada una de las formas (g, h, i) y (g0,h",i"); por lo tanto, i = g = i0/ y —h ξ h0 ξ —h0/ (mod. i o g o i0/). De esto, es manifiesto que la forma (i00, — h00,g0), i.e., la forma Ψη-1 es contigua por la ultima parte de la forma (g, h, i), i.e., de la forma fm—1.

Si las formas Φ y φ son impropiamente equivalentes, la forma φ equivaldrúa propiamente a la forma opuesta a Φ. Podemos, entonces, encontrar la transformacion propia de la forma φ en la forma opuesta a Φ; si suponemos que esto puede darse por la sustitucion α, β, γ, δ, es facil ver que φ se transformara impropiamente en Φ por la sustitución α, —β, γ, —δ.

De aquú es claro que si las formas Φ y φ son propia e impropiamente equivalentes, podemos encontrar dos transformaciones, una propia y la otra impropia.

Ejemplo. Se busca una transformación impropia de la forma (129, 92, 65) en la forma (42, 59, 81), ya que observamos en el artículo anterior que las dos formas son impropiamente equivalentes. Se deberá primero encontrar una transformación propia de la forma (129, 92, 65) en la forma (42, -59, 81). Para este fin, calculamos la sucesión de formas (129, 92, 65), (65,-27,10), (10, 7, -3), (-3, 8,5), (5, 22,81), (81, 59,42), (42, -59, 81). De esta se deduce la transformación propia -47, 56, 73, -87, a traves de la cual (129, 92,65) se transforma en (42, -59, 81); por lo tanto se transformaró en (42, 59, 81) por la transformación impropia -47, -56, 73, 87.

197.

Si tenemos una transformación de una forma (a, b, c) . ..φ en una forma equivalente Φ, de esto podran deducirse todas las transformaciones similares de la forma φ en Φ, si solamente podemos determinar todas las soluciones de la ecuación indeterminada t2 - Du2 = m2, donde D indica el determinante de las formas Φ y φ, m es el maximo común divisor de los números a, 2b, c (art. 162). Solucionamos este problema arriba para un valor negativo de D, y ahora consideraremos un valor positivo. Pero, puesto que obviamente cualquier valor de t o u que satisfaga la ecuacion tambien la satisfará si cambiamos el signo, sera suficiente asignar valores positivos a t ya u. De hecho, cualquier solucion por valores positivos proporcionara cuatro soluciones efectivas. Para resolver este asunto, encontraremos primero los valores mínimos de t y u (excepto aquellos obvios donde t = m y u = 0) y entonces de estos veremos como derivar los otros. [[155]](#footnote-156)

188, fn será (+an,bn, —an+1) porque n es par y f será transformada en esta forma por la sustitución propia on, βn, qn, ón. Pero, puesto que f y fn son identicas, f se transformará en fn tambien por la sustitución propia 1, 0, 0, 1. De estas dos trans­formaciones similares de la forma f en fn, por el artículo 162 podra deducirse una solucion integral de la ecuación t2 — Du2 = m2, a saber t = 2 (on + ón)m (ecuación 18, art. 162), u = YY (ecuación 19).[[156]](#footnote-157)) Tómense estos valores positivamente si no lo son ya y desógnense por T y U. Estos valores T y U serán los valores menores de t y u excepto t = m y u = 0 (ellos deben ser diferentes de estos, puesto que claramente qn no podría ser = 0).

Supongase en efecto que hay valores menores de t y u, llamados t y u, los cuales son positivos y u no es =0. Entonces por el artículo 162 la forma f se transformaró en una forma que es identica a ella misma por la transformación propia m (t — bu), m a'u, m au, m (t+bu). Ahora, por el artículo 193, II resulta que o m (t—bu) o bien — m(t — bu) debe ser igual a uno de los numeros α’’, o!", o!’", etc., por ejemplo a αμ (puesto que t2 = Du2 + m2 = b2u2 + aa’u2 + m2 tenemos t2 > b2u2 y por lo tanto t — bu es positivo; de aqui la fracción que corresponde a la fraccion

C en el artículo 193 tendrá el mismo signo que a o a’); y en el primer caso ma’u, m au, m (t + bu) serán iguales a βμ, γμ, respectivamente, y en el ultimo caso serón iguales a las mismas cantidades pero con cambio de signo. Puesto que u < U, i.e. u < YY y > 0, obtenemos γμ < yn y > 0; y puesto que la sucesión γ, γ’, γ’’, etc., es continuamente creciente, μ estará necesariamente entre 0 y n exclusivamente. Asó la forma correspondiente fμ sera identica a la forma f, Q. E. A. puesto que todas las formas f, f’, f’’, etc., hasta fn-1 se suponen diferentes. De esto concluimos que los valores menores de t y u (excepto los valores m y 0) serán T y U.

Ejemplo. Si D = 79 y m =1 podemos usar la forma (3, 8, —5) para la cual n = 6, y on = —8, γ”- = —27, δη = —152 (art. 188). Entonces T = 80 y U = 9, que son los valores menores de los nómeros t y u, que satisfacen la ecuacion t2 — 79u2 = 1.

199.

En la practica, pueden desarrollarse formulas aón mós cómodas. Tenemos 2bγn = —a(on — hn), que es facil de deducir del artículo 162, multiplicando la ecuación [19] por 2b, [20] por a, y cambiando los súmbolos usados alló por los que

donde podemos tambien escribir m[k00,k000,...kn, a] para el valor de T.

estamos usando aquí. De esto obtenemos αη + δη

2δη - f γη y entonces

b

±T = m^n - -γn), a

±U

n

γ m  
a

Por un metodo similar obtendremos los valores siguientes

— β nm

±T = m(an + --βη), ±U = Ιβ-β

*a a*0

Estos dos conjuntos de fórmulas son muy convenientes porque γn = δn-1 y an = βη-1, de modo que si usamos el segundo conjunto, es suficiente calcular la sucesión β0, β00, β0/0, ... , β”-; y si usamos el primer conjunto, la sucesión δ0, δ00, δ000, etc., seró suficiente. Mas aón, del artículo 189.3 podemos facilmente deducir que, puesto que n es par, αη y aβn tienen el mismo signo. Esto es tambien cierto para δn y aγη, de modo que en la primera fórmula deba tomarse para T la diferencia absoluta, y en la segunda la suma absoluta sin que sea necesario prestar atencion al signo. Usando los símbolos del artículo 189.4 obtenemos de la primera formula lo siguiente:

T = *m[k0,k00,k000,...kn] - — [k0,k00,k000,...k*n-1],

*a*

y de la segunda fórmula resulta:

*m*

U = -[k0,k00,k000,...kn-1] a

T = m[k00,k000,...kn-1] + m— [k00,k000,...kn],

a0

m

U = ^[k00,k000,...kn] a0

Ejemplo. Para D = 61, m = 2, puede usarse la forma (2, 7, -6). De esto encontramos n = 6; k0, k00, k000, k0000, k00000, k000000 respectivamente = 2, 2, 7, 2, 2, 7. Entonces

T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2] = 2888 - 1365 = 1523

de la primera formula; lo mismo resulta de la segunda formula

7

T = 2[2, 7, 2, 2] + -[2, 7, 2, 2, 7]

y U = [2, 2, 7, 2, 2] = ±[2, 7, 2, 2, 7] = 195.

Existen otros artificios mediante los cuales puede simplificarse el cólculo, pero la brevedad no nos permite tratarlos en detalle aquó.

200.

Para obtener todos los valores de t y u de los valores menores, presentaremos la ecuación T2 — DU2 = m2 de la siguiente forma

(T + - VD)(T — - VD) = 1

m m m m

De esto tenemos tambien que

(T + - VD)e(T — - VD)e = 1

[1]

m m m m

donde e puede ser cualquier numero. Ahora por brevedad designaremos los valores de las cantidades

m

"2

T

m

*m T U ^-,e m T*

—u= ( 1 vD) == (—

*2yD m m 2yD* m

* vD)e

*m*

* - VD)

*m*

e

en general por te y ue, respectivamente; i.e., para e = 0 serán t0 y u0 (estos valores son m y 0); para e = 1 sera t0 y u0 (estos valores son T y U); para e = 2 serán t00 y u00; para e = 3 serán t000 y u000, etc. Ademas mostraremos que, si para e se toman todos los enteros no negativos, i.e., 0 y todos los enteros positivos de 1 a to, estas expresiones producirán todos los valores positivos de t y u; es decir, (I) todos los valores de estas expresiones son, en efecto, valores de t y u; (II) todos estos valores son enteros; (III) no existen valores positivos de t y u que no esten contenidos en estas formulas.

1. Si sustituimos te y ue por sus valores y usamos la ecuación [1] es facil encontrar que

(te + uVD)(te — ueVD) = m2, i.e. t2e — Du2e = m2

1. De la misma forma es facil confirmar que en general

e + „ 1 2T e+1 e\_ 1 2T e

te+i + te 1 = — te, ue+1 + u 1 = — u

mm [[157]](#footnote-158)

Entonces, es claro que las dos sucesiones t0, t0, t00, t000, etc., u0, u0, u00, u000, etc. son recurrentes y que los factores correspondientes para cada una son — y — 1, es decir

2T

.. 2T , 0

t00 = — t0 — t0, m

2T

u = — u etc.  
m

t000 = —t00 — t0 etc., m

Ahora, puesto que por hipótesis tenemos una forma (M, N, P) con determi­nante D en la cual M, 2N, P son divisibles por m, tendremos

T2 = (N2 — MP)U2 +

m

q ^ q 2T

y manifiestamente 4T2 seró divisible por m2. Entonces 2y sera un entero positivo. Y puesto que t0 = m, t0 = T, u0 = 0, u0 = U, y son entonces enteros, todos los numeros t00, t000, etc., u00, u000, etc., seran tambien enteros. Mós aón, puesto que T2 > m2, todos los numeros t0, t0, t00, t000, etc. seran positivos y continuamente crecientes al infinito; lo mismo es cierto para los nómeros u0, u0, u00, u000, etc.

1. Supongamos que existen otros valores positivos de t y u, no contenidos en la serie t0, t0, t00, etc. u0, u0, u00, etc., llamados T y U. Puesto que la serie u0, u0, etc. crece de 0 a infinito, U estara necesariamente entre dos terminos vecinos un y un+1 tal que U > un y U < un+1. Para mostrar lo absurdo de esta suposición, observamos que

1o La ecuación t2 — Du2 = m2 se satisface si se ponen

t = — (Ttn — DUun), m

u = — (Utn — Tun) m

Esto puede confirmarse sin dificultad por sustitución. Así mostraremos que estos valores, que por brevedad escribimos τ y v, son siempre enteros. Si (M, N, P) es una forma con determinante D y m es el móximo común divisor de los números M, 2N, P, ambos T + NU y tn + Nun seran divisibles por m y por lo tanto tambien U(tn + Nun) — un(T + NU) o Utn — Tun. Por esto v sera un entero y tambien lo sera τ porque τ2 = Dv2 + m2.

2o Claramente v no puede ser = 0; puesto que de esto resultaría que

U2t2n = T2u2n o

U2(Du2n + m2) = u2n(DU2 + m2)

o U2 = u2n en contra de la hipótesis de que U > un. Puesto que excepto para el valor 0, el valor menor de u es U, ν ciertamente no seró menor que U.

3o De los valores de tn, tn+1, un, un+1 es fócil confirmar que

Y así Utn — Tun ciertamente no seró menor que un+7n — tn+1ur‘

DU[[158]](#footnote-159) =

*=\l°+*

4o Ahora, de la ecuación T2 — DU2 = m2 tenemos

T

*u2n+2*

mU = un+1tn- tn+1un

y similarmente

U

tn+1

u

n+1

m2

U

*= {d +*

m

t ^ o

U un

Si se multiplican y en lugar de T2, t2n, t2n+2 se sustituyen sus valores DU2 + m2, Du2n + m2, Du2n+2 + m2, resultaró que

1

^(U2 — u2n

) >-n+r (u2n+2 — u2n)

De esto es facil de ver que u > n+T. Esto, a la par de la conclusión en 3o, nos da

T

(Utn — Tun)(tn + unT) > (un+1 tn — tn+1un)(tn + un

tn+1

un+1

2n

u

n+1

Ademaós se encuentra que

t0 = 2, t0 = 1523, t00 = 1523t0 — t0 = 2319527, t000 = 1523t00 — t0 = 3532638098, etc. u0 = 0, u0 = 195, u00 = 1523u0 — u0 = 296985, u000 = 1523u00 — u0 = 452307960, etc.

De esto, puesto que cada cantidad es positiva, resultaró trasponiendo U + un+T > n+1 +

u

, 1523 195

‘ “ΥΤ + ΊΓ^

,1523 195

+r — ίγ^

195

u = \_^((1523 + 195^ \_ (1523

76! 2

2

2

2

761)6)

201.

Añadimos las siguientes observaciones acerca del problema tratado en los artículos precedentes.

1) Puesto que hemos mostrado cómo resolver la ecuación t2 — Du2 = m2 para todos los casos cuando m es el maximo comón divisor de los tres nómeros M, 2N, P, tal que N2 — MP = D, es útil especificar todos los nómeros que pueden ser esos divisores, es decir, todos los valores de m para un valor dado de D. Sea D = n2D0 de modo que D0 este enteramente libre de factores cuadrados. Esto puede obtenerse poniendo n2 como el cuadrado mayor que divide D y, si D no tiene un factor cuadrado, poniendo n = 1. Entonces:

Primero, si D0 es de la forma 4k +1, cualquier divisor de 2n será un valor de m y viceversa. En efecto, si g es un divisor de 2n, tendremos la forma (g, n, n D ^), cuyo determinante es D y en la cual el móximo comón divisor de los nómeros g, 2n, —H seró obviamente g (puesto que es claro que n ~ 4 ^ es un

entero). Si, por el otro lado, suponemos que g es un valor de m, es decir, el maximo comón divisor de los nómeros M, 2N, P, y que N2 — MP = D, manifiestamente 4D o 4n2D0 seró divisible por g2. Se sigue que 2n es divisible por g. Pues, si g no dividiera a 2n, g y 2n tendrían un maximo comun divisor menor que g. Supóngase que fuera = δ, y 2n = ñn0, g = ñg0; n0 D0 seró divisible por g0 . Asó, n0 y g0 al igual que n02 y g02 seróan primos relativos y D0 seróa divisible por g02, en contra de la hipotesis segón la cual D0 esta libre de factores cuadrados.

Segundo, si D0 es de la forma 4k + 2 o 4k + 3, cualquier divisor de n sera un valor de m e, inversamente, cualquier valor de m dividira n. En efecto, si g es un

divisor de n se tendró una forma (g, 0.

*-n2D'*

*a*

) cuyo determinante es = D. Claramente n2D0

el maximo comón divisor de los nómeros g, 0, n g seró g. Ahora, si suponemos que g es un valor de m, es decir, el móximo comón divisor de los nómeros M, 2N, P y que N2 — MP = D, de la misma forma que arriba, g dividira 2n y 2n seró un entero.

Si este cociente es impar, el cuadrado 4^ sera = 1 (mod. 4), y entonces 4ngP sería = 2, o = 3 (mod. 4). Pero

4n2D0

a

4D

4 N 2

*H*2

4MP 4N2

, , , , -^ = —^ (mod. 4) y entonces

4pr seróa = 2 o = 3 (mod. 4), Q.E.A, porque todo cuadrado debe ser congruente a cero o a la unidad segón el modulo 4. Por lo tanto, el cociente seró necesariamente

par, y asó es un entero, es decir, g un divisor de n.

Entonces es claro que 1 es siempre un valor de m, es decir, que la ecuacioón t2 — Du2 = 1 es resoluble de la manera precedente para cualquier valor no cuadrado

positivo de D; 2 será un valor de m solo si D es de la forma 4k o 4k +1.

1. Si m es mayor que 2 pero es todavía un número idóneo, la solución de la ecuación t2 — Du2 = m2 puede reducirse a la solucion de una ecuacion similar en la cual m es 1 o 2. Así, poniendo D = n2D0, si m divide a n, m2 dividiró a D. Entonces si suponemos que los valores menores de p y q en la ecuación p2 — y q2 = 1 son p = P y q = Q, los valores menores de t y u en la ecuacion t2 — Du2 = m2 serón t = mP y u = Q. Pero si m no divide a n, al menos dividira a 2n y sera ciertamente par, y 4D/m2 sera un entero. Entonces, si se encuentra que los valores menores de p y q en la ecuacion p2 — y q2 = 4 son p = P y q = Q, los valores menores de t y u en la ecuación t2 — Du2 = m2 serón t = yP y u = Q. En cualquier caso, sin embargo, podran deducirse no solo los valores menores de t y u por el conocimiento de los valores menores de p y q, sino que, por este metodo podrón deducirse todos los valores del anterior de todos los valores del ultimo.
2. Designemos por t0, u0; t0, u0; t00, u00, etc. a todos los valores positivos de t y u, en la ecuacion t2 — Du2 = m2 (como en el artículo precedente). Si resulta que cualesquiera valores en la serie son congruentes a los primeros valores seguón un modulo dado r, por ejemplo si tp ξ t0 (o ξ m), up ξ u0 o ξ 0 (mod. r), y si al

mismo tiempo los valores siguientes son congruentes a los segundos valores, i.e.,

tP+1 ξ t0, uP+1 ξ u0 (mod. r)

se tendró tambien que

tP+2 ξ t00, uP+2 ξ u00; tP+3 ξ t000, uP+3 ξ u000; etc.

Esto puede deducirse facilmente porque cada serie t0, t0, t00, etc., u0, u0, u00, etc. es una serie recurrente; esto es asó puesto que

t00 = —t0 — t0, tP+2 = —tP+1 — tp

mm

seróa

t00 ξ tP-2

y similarmente para el resto. Entonces se sigue que en general

th+P ξ th, uh+P ξ uh (mod. r)

donde h es cualquier número; e incluso, más generalmente, si

μ = ν (mod. ρ), entonces t = tv, up = uv (mod. r)

1. Podemos siempre satisfacer las condiciones requeridas por la observaciún precedente; esto es, siempre puede encontrarse un índice ρ (para cualquier modulo dado r) para el cual sean

tp = t0, tp+1 = t0, up = u0, up+1 = u

Para mostrar esto, observamos:

Primero, que la tercera condición siempre puede satisfacerse. Pues por los criterios dados en 1) es claro que la ecuacion p2 — r2Dq2 = m2 es resoluble, y si se supone que los valores positivos menores de p y q (excepto m y 0) son P y Q, manifiestamente t = P y u = rQ estará entre los valores de t y u. Por lo tanto P y rQ estarán contenidos en las sucesiones t0, t0, etc., u0, u0, etc., y si P = tA y rQ = uA tendremos uA = 0 = u0 (mod. r). Mas aun, se ve que entre u0 y uA no existirá ningun termino que sea congruente a u0 segun el modulo r.

Segundo, si las otras tres condiciones se cumplen, es decir, si uA+1 = u0, tA = t0, t^+1 = t0, entonces se debe poner ρ = λ. Pero, si una u otra de estas condiciones no se cumple, podemos con certeza poner ρ = 2λ. En efecto, de la ecuacion [1] y las formulas generales para te y ue del artículo precedente se deduce

y entonces

t2A = — (t2A + Du2A) = — (m2 + 2Du2A)

m

m

t2A \_ t0 2Du'

2A

r mr

Esta cantidad sera un entero porque por hipotesis r divide a uA y m2 divide a 4D y, así, m divide a 2D. Mas aun u2A = ^tAuA, y puesto que

4t2A = 4Du2A + 4m2

es entonces divisible por m2, 2tA sera divisible por m y entonces u2A por r o

u

2A 0

= u0 (mod. r)

En el tercer lugar se encuentra

(2A+1 = t, + 2D“2>+1

m

y puesto que, por una razón similar, 2^ es un entero, se tendrá

t2>+1 = t' (mod. r)

Finalmente se encuentra que

,2>+1 , 2t>+1u>

u + = u +

m

y puesto que 2t>+1 es divisible por m y u> por r, tenemos que

u2>+1 = u' (mod. r). Q. E. D.

La utilidad de las óltimas dos observaciones apareceró en lo siguiente.

202.

Un caso particular del problema de resolver la ecuación t2 — Du2 = 1 ya ha sido tratado por geometras del óltimo siglo. El extremadamente agudo geometra Fermat propuso el problema a los analistas ingleses, y Wallis atribuyó el descubrimiento de la solución a Brounker, y reportó este en el capítulo 98 de su Algebra, Opera T. II, p. 418 y siguientes. Ozanam afirma que fue Fermat; y Euler, que trato de el en Comm. Petr. VI p. 175, Comm. nov. XI, p. 28 [[159]](#footnote-160)), Algebra P. 2, p. 226, Opuse. An. I, p. 310, afirma que Pell fue el descubridor, y por esa razon se llama el problema de Pell por algunos autores. Todas estas soluciones coinciden esencialmente con lo que obtenemos si en el artículo 198 usamos la forma reducida con a = 1; pero nadie antes de Lagrange mostróo que la operacioón necesariamente termina, es decir que el

problema es realmente resoluble[[160]](#footnote-161)). Consúltese Mélanges de la Soc. de Turin,T. 4, p. 19; y para una presentación mús elegante Hist. de l’Ac. de Berlin, 1767, p. 237. Tambien hay una investigaciún de esta cuestión en el apendice del Algebra de Euler, que hemos frecuentemente recomendado. Ademas nuestro metodo (partiendo de principios totalmente diferentes y no estando restringidos al caso de m = 1) nos da muchas formas de obtener una soluciún porque en el artículo 198 podemos empezar de cualquier forma reducida (a, b, -a').

203.

PROBLEMA. Si las formas Φ y φ son equivalentes, exhibir todas las trans­formaciones de una en la otra.

Solución. Cuando estas formas son equivalentes de una sola manera (i.e., ya sea solo propiamente o solo impropiamente), por el artículo 196 se busca una transformation α, β, γ, δ de la forma φ en Φ, y es claro que todas las otras son similares a esta. Pero cuando φ y Φ son equivalentes propia e impropiamente se buscan dos transformaciones disímiles (i.e., una propia, y la otra impropia) α, β, γ, δ; y α', β', γ', δ'; y cualquier otra transformation sera similar a una de estas. Si la forma φ es (a,b,c), su determinante es = D, m es el maximo comun divisor de los numeros a, 2b, c (como siempre fue el caso arriba), y t y u representan numeros indeterminados que satisfacen la ecuacion t2 — Du2 = m2, entonces en el primer caso todas las transformaciones de la forma φ en Φ estaran contenidas en la primera de las formulas, y en el ultimo caso en la I o en la II.

1. . . . . mm (at — (ab + γ^) , ^ ^t — ^b + δ^)

m ^t + (aa + γ^^ , ^ ^t + (βα + δ^^

1. . . . . m (a't — (a'b + γ'c)u) , ^ (β't — (β'b + δ'c)u)

(γ't + (a'a + γ'b)u) , (δ't + (β'a + δ'b)u)

Ejemplo. Se desean todas las transformaciones de la forma (129, 92, 65) en la forma (42, 59, 81). Encontramos, en el artículo 195, que estas son solo impropiamente

equivalentes y, en el artículo siguiente, que la transformación impropia de la primera en la ultima es -47, -56, 73, 87. Por lo tanto todas las transformaciones de la forma (129,92, 65) en (42, 59,81) serán expresadas por la fórmula

— (47t + 421u), — (56t + 503u), 73t +653u, 87t + 780u

donde t y u son todos los nómeros que satisfacen la ecuación t2 estan expresados por la formula

79u2

1; y estos

2((80 + 9^79)e + (80 — 9^79)e) 2

±t

u

1

((80 + ^/79)e — (80 — ^/79)e)

2λ/79 donde e representa a todos los enteros no negativos.

204.

Es claro que una formula general que represente a todas las transformaciones sería más simple si la transformación inicial de la cual se deduce la formula es mas simple. Ahora, puesto que no importa desde cual transformación empecemos, muy frecuentemente la fórmula general puede simplificarse si desde la primera formula encontrada deducimos una transformación menos compleja dando valores específicos a t y u, y usando esto para producir otra formula. Entonces, e.g., en la fórmula encontrada en el artículo precedente, al poner t = 80, u = —9, resulta una transformation que es mas simple que la que encontramos. De esta forma obtenemos la transformation 29, 47, —37, —60 y la fórmula general 29t — 263u, 47t — 424u, —37t + 337u, —60t + 543u. Cuando, entonces, por medio de los preceptos precedentes la fórmula general es encontrada, podra probarse si la transformación obtenida es mas simple o no que aquella de la que la fórmula fue deducida, dóndole a t y u los valores específicos ±t', ±u'; ±t'', ±u'', etc., y en este caso podra derivarse una formula mós simple de esa transformation. Pero que constituye simpleza es todavóa un principio arbitrario. Si fuera útil, podríamos encontrar una norma fija y asignar límites en las series t!, u'; t'', u", etc., mós alló de las cuales las transformaciones lleguen a ser continuamente menos simples. Entonces no habría necesidad de buscar mós y bastaría confinar nuestra bósqueda dentro de estos Emites; no obstante, por brevedad suspendimos esta investigation porque muy frecuentemente mediante los metodos prescritos por nosotros surge la transformación mós simple, ya sea inmediatamente o usando los valores ±t' y ±u' para t y u.

205.

PROBLEMA. Encontrar todas las representaciones de un número dado M por una formula dada ax2 + 2bxy + cy2 cuyo determinante no cuadrado positivo es = D.

Solución. Primero observamos que la investigación de representaciones por valores de x e y que no son primos relativos se puede reducir al caso (art. 181) de formas con determinante negativo donde se buscaron las representaciones por valores relativamente primos de las incógnitas. No hay necesidad de repetir aquí el argumento. Ahora, para representar M por valores primos relativos de x e y se requiere que D sea un residuo cuadrático de M, y si todos los valores de la expresión \f~D (mod. M) son N, — N, N', — N', N'', —N'', etc. (podemos escogerlos tal que ninguno sea > ^M), entonces cualquier representación del nómero M por la forma dada perteneceraó a uno de estos valores. Antes de todo, se debe buscar estos valores y despues investigar las representaciones que pertenecen a cada uno de ellos. No habrá ninguna representacion que pertenezca al valor de N a no ser que las formas (a, b, c) y (M,N, N-2) sean propiamente equivalentes; si lo son, se busca una transformación propia α, β, γ, δ de la primera en la segunda. Entonces tendremos una representacion del nómero M por la forma (a, b, c) perteneciente al valor N, poniendo x = α e y = γ, y todas las representaciones pertenecientes a este valor estarón expresadas por la fórmula

1

1

= —(at — (ab + jc)u), y = —(jt + (αα + γ^)η)

x

donde m es el maximo común divisor de los números a, 2b, c y t, u representan en general a todos los nómeros que satisfacen la ecuación t2 — Du2 = m2. Pero, manifiestamente esta fórmula general seró mas simple si la transformación α, β, γ, δ de la que fue deducida es mas simple. Entonces seró ótil encontrar, segón el artículo precedente, la transformacion mós simple de la forma (a, b, c) en (M, N, KwD) y deducir la formula de esta. Exactamente de la misma manera podemos producir fóormulas generales para representaciones pertenecientes a los valores restantes — N, N', —N' etc. (si efectivamente existe alguno).

Ejemplo. Se buscan todas las representaciones del nómero 585 por la formula 42x2 + 62xy + 21y2. En relacion con las representaciones por valores de x e y que no son primos relativos, es inmediatamente evidente que no puede haber otros de este tipo excepto aquellos en los cuales el móximo común divisor de x e y sea 3, porque 585 es divisible solo por un cuadrado, 9. Cuando encontramos, entonces, todas las representaciones del numero -g-, i.e. 65 por la forma 42x' + 62x'y' + 21y' con x' e y' primos relativos, podemos derivar todas las representaciones del nuómero 585 por

la forma 42x2 + 62xy + 21 y2 no siendo x e y primos relativos, poniendo x = 3x0 e y = 3y0. Los valores de la expresión -\/79 (mod. 65) son ±12 y ±27. Se encuentra que la representación del nómero 65 perteneciente al valor -12 es x0 = 2 e y0 = -1. Por lo tanto todas las representaciones de 65 pertenecientes a este valor estaróan expresadas por la fórmula x0 = 2t — 41u, y0 = —t + 53u y de esto todas las representaciones de 585 por la fórmula x = 6t — 123u, y = —3t + 159u. De manera similar encontramos que la fórmula general para todas las representaciones del número 65 pertenecientes al valor 12 es x0 = 22t — 199u, y0 = — 23t + 211u; y la fórmula para todas las representaciones del nómero 585 derivadas de esto sera x = 66t — 597u, y = —69t + 633u. Pero, no existe una representación del nómero 65 perteneciente a los valores +27 y —27. Para encontrar representaciones del nómero 585 por valores x e y primos entre si, debemos primero calcular los valores de la expresión ^/79 (mod. 585), los cuales son ±77, ±103, ±157, ±248. No existe ninguna representación perteneciente a los valores ±77, ±103 y ±248, pero la representación x = 3, y = 1 pertenece al valor —157, y podemos deducir la formula general para todas las representaciones pertenecientes a este valor: x = 3t — 114u, y = t + 157u. Similarmente encontramos la representación x = 83, y = —87 perteneciente a +157, y la formula en la que todas las respresentaciones similares estan contenidas es x = 83t — 746u, y = —87t + 789u. Tenemos entonces cuatro fórmulas generales en las que estan contenidas todas las representaciones del nómero 585 por la forma 42x2 + 62xy + 21y2:

x = 6t — 123u x = 66t — 597u x = 3t — 114u x = 83t — 746u

y = —3t + 159u y = —69t + 633u y = t + 157u

y = —87t + 789u

donde t y u representan en general todos los enteros que satisfacen la ecuacioón t2 — 79u2 = 1.

Por brevedad no nos detendremos en aplicaciones especiales del anóalisis precedente sobre formas con determinante no cuadrado positivo. Cualquiera podró tener su propia lucha con estas imitando el metodo de los artículos 176 y 182. Nos vamos a apresurar inmediatamente a considerar formas con determinante cuadrado positivo, que es el ónico caso que falta.

Formas de determinante cuadrado.

206.

PROBLEMA. Dada la forma (a,b,c) con el determinante cuadrado h2, donde h es la raíz positiva, encontrar una forma (A,B,C) que sea propiamente equivalente a ella, en la que A esté entre los límites 0 y 2h — 1 inclusive, B sea = h, C = 0.

Solución. I. Puesto que h2 = b2 — ac, tenemos (h — b) : a = c : — (h + b). Sea β : δ igual a esta razón de modo que β sea primo a δ, y determínense α y γ tal que αδ — βγ = 1, lo cual puede hacerse. Por la sustitución α, β, γ, δ, la forma (a, b, c) seró transformada en (a',b',c'), la cual sera propiamente equivalente. Entonces se tendraó

tí = ααβ + b(αδ + βγ) + cγδ

= (h — b)αδ + ^αδ + βγ) — (h + ^βγ = Λ,(αδ — βγ) = h c0 = aβ2 + 2bβδ + cδ2 = (h — ^βδ + 2bβδ — (h + ^βδ = 0

Mas aón, si a0 estó entre los límites 0 y 2h — 1, la forma (a0,b0,c0) satisfaró todas las condiciones.

1. Pero si a0 estó fuera de los límites 0 y 2h — 1, sea A el residuo positivo mínimo de a0 relativo al modulo 2h que manifiestamente estaró entre esos Emites y sea A — a0 = 2hk. Entonces la forma (a0,b0,c0), i.e. (a0,h,0) seró transformada por la sustitucion 1, 0, k, 1 en la forma (A, h, 0) que seró propiamente equivalente a las formas (a0,b0,c0) y (a, b, c) y satisfará todas las condiciones. Por otra parte es claro que la forma (a, b, c) sera transformada en la forma (A, h, 0) por la sustitución α + β^ β, γ + δ^ δ.

Ejemplo. Considere la forma (27,15,8) cuyo determinante es = 9. Aquó h = 3 y 4 : —9 es la razon con los terminos menores que es igual a las razones — 12 : 27 = 8 : —18. Por lo tanto, con β = 4, γ = —9, α = —1, γ = 2, la forma (a0,b0,c0) se convierte en (—1, 3, 0), que va a la forma (5, 3, 0) por la sustitucion 1, 0, 1, 1. Esta es entonces la forma buscada, y la forma dada se transforma en ella por la sustitucion propia 3, 4, —7, —9.

A tales formas (A, B, C), en las que C = 0, B = h, y A estó entre los limites 0 y 2h — 1, las llamaremos formas reducidas, que deben distinguirse de las formas reducidas que tienen un determinante negativo o no cuadrado positivo.

207.

TEOREMA. Dos formas reducidas (a, h, 0) y (a',h, 0) no idénticas no pueden ser propiamente equivalentes.

Demostración. Si fueran propiamente equivalentes, la primera se transformaría en la segunda por una sustitución propia α, β, γ, δ y tendríamos las cuatro ecuaciones:

aa2 + 2haj = a' [1]

ααβ + h(αδ + βγ) = h [2]

αβ2 + 2Λ,βδ = 0 [3]

αδ — βγ = 1 [4]

Multiplicando la segunda ecuación por β, la tercera por a y restando, tenemos —h(aδ — βγ)β = βΛ, o, de [4], — βΛ, = βΛ,; de donde necesariamente β es = 0, por lo cual, usando [4], αδ = 1 y a = ±1. Entonces de [1], a ± 2γΛ = a', y esta ecuación no puede ser consistente a menos que γ = 0 (porque tanto a como a' por hipótesis estón entre 0 y 2h — 1), i.e. a menos que a = a' o que las formas (a, h, 0), (a',h, 0) sean identicas, lo que esta en contra de la hipótesis .

Entonces los siguientes problemas, que ofrecóan una mayor dificultad para los determinantes no cuadrados, pueden ser resueltos con muy poco esfuerzo.

1. Dadas dos formas F y F' con el mismo determinante cuadrado investigar si son propiamente equivalentes o no. Busquemos dos formas reducidas que sean propiamente equivalentes a las formas F y F' respectivamente. Si son idóenticas, las formas dadas seróan equivalentes; de otra manera, no lo seróan.
2. Dadas las mismas formas, F y F', investigar si son impropiamente equivalentes o no. Sea G la forma opuesta a una de las formas dadas, e.g. la forma F. Si G es propiamente equivalente a la forma F', F y F' serón propiamente equivalentes; de otra manera no lo seróan. [[161]](#footnote-162)

y una transformación propia α', β', γ0, δ' de la forma F' en Φ. Entonces Φ será transformada en F' por la transformación propia δ', —β', — γ', α' y entonces F en F' por la sustitucion propia

αδ' — βγ', βα' — αβ', γδ' — δγ', δα' — γβ'

Sera ótil desarrollar otra fórmula para la transformación de la forma F en F' para la cual no sea necesario conocer la forma reducida Φ. Supongamos que la forma

F = (a, b, c), F' = (a ,b',c ), Φ = (A, h, 0)

Puesto que β : γ es la razón con nómeros menores igual a las razones h — b : a o c : — (h + b), es fócil ver que h-· = a seró un entero, que llamaremos f, y que f = ~h~b seró tambien un entero, que llamaremos g. Tenemos, sin embargo:

A = αα2 + 2bαγ + σγ2 y por lo tanto βΑ = αα2β + 2bαβγ + cβγ2 o (sustituyendo αβ por δ(Λ, — b) y c por βg)

βΑ = α2δΛ, + ^2βγ — αδ)α + β2γ2g o sea (puesto que b = —h — δg)

βΑ = 2α(αδ — βγ)Λ, + (αδ — βγ)^ = 2αh + g

δΑ = αα2δ + 2bαγδ + cy^

Similarmente

= α2δ2f + ^2αδ — βγ)γ — βγ2h = (αδ — βγ)^ + 2γ (αδ — βγ)h = 2γΛ, + f

Por lo tanto

βΑ — g δΑ — f

α = —~—, γ =

2h

2h

De exactamente la misma forma, poniendo

h — b' a' , c' —h — b' ,

ιτ = τ,= f , τι = —— = g

β δ

β δ

tenemos

0 \_ *βΆ - g* 0 \_ *δ A - f*

α 2h ’ γ 2 h

Si los valores α,γ,α0,γ0 son sustituidos en la fórmula que acabamos de dar para la transformación de la forma F en F0, obtenemos

βί0 - S0g β7 - β9' Sf0 - S0f β7 - Sg0

2h , 2h ’ 2h ’ 2h

en donde A ha desaparecido completamente.

Si se dan formas impropiamente equivalentes F y F0 y se busca una transformación impropia de una en la otra, sea G la forma opuesta a la forma F y sea α, β, γ, δ la transformación propia de la forma G en F0. Entonces, manifiestamente α, β, -γ, -δ seró la transformation impropia de al forma F en F0.

Finalmente, si las formas dadas son propia e impropiamente equivalentes, este metodo nos puede dar dos transformaciones, una propia y la otra impropia.

209.

Ahora sólo resta mostrar como deducimos de una transformación todas las otras transformaciones similares. Esto depende de la solucióon de la ecuacioón indeterminada t2 - h2u2 \_ m2, donde m es el maximo comun divisor de los números a, 2b, c y (a, b, c) es una de las formas equivalentes. Pero esta ecuación puede resolverse en solo dos maneras, esto es, poniendo ya sea t \_ m, u \_ 0, o t \_ -m, u \_ 0. En efecto, supongamos que existe otra solution t \_ T, u \_ U, donde U no es \_ 0.

<-) c\ λ/τι2 λ~τ2ττ2

Entonces, puesto que m2 divide a 4h2, ciertamente obtendremos \_ 2—+ 4

5 ^ 1 7 m2 m2

4T 2 Ah2jj 2 s s

y tanto como 22 serán enteros cuadrados. Pero claramente el nómero 4 no puede ser la diferencia de dos enteros cuadrados, a no ser que el menor cuadrado sea 0, i.e., U \_ 0, en contra de la hipotesis. Por lo tanto, si la forma F se transforma en la forma F0 por la sustitución α, β, γ, δ, no habrá otra transformation similar a esta excepto -α, -β, -γ, -δ. Por lo tanto, si dos formas son solo propiamente o solo impropiamente equivalentes, habrá solo dos transformaciones; pero si son propiamente e impropiamente equivalentes, habra cuatro, a saber, dos propias y dos impropias. [[162]](#footnote-163)

de los números a, 2h o a', 2h; y reciprocamente si a, 2h o a!, 2h tienen el mismo

máximo común divisor m y aa' = m2 (mod. 2mh), las formas (a, h, 0), (a',h, 0) seran impropiamente equivalentes.

Demostracián. I. Transfórmese la forma (a, h, 0) en la forma (a',h, 0) por la sustitución impropia a, β, γ, δ tal que tengamos cuatro ecuaciones

aa2 + 2haj = a' [1]

aaβ + h(αδ + βγ) = h [2]

aβ2 + 2Λ,βδ = 0 [3]

αδ — βγ = — 1 [4]

Si multiplicamos [4] por h y restamos de [2], lo cual escribimos como [2] — h[4], se sigue que

(aa + 2Λ,γ )β = 2h [5]

Similarmente de γδ[2] — γ2[3] — (a + αβγ + hγδ)[4], al borrar los terminos que se cancelan, tenemos

—ααγ = a + 2Λ,γδ o — (aa + 2Λ,γ )δ = a

[6]

[7]

y finalmente de a[1] ...aa(aa + 2Λ,γ) = aa' o

2

(aa + 2Λ,γ) — aa = 2h^(aa + 2Λ,γ)

o

(aa + 2Λ,γ)2 = aa' (mod. 2h(aa + 2hγ))

= m2 (mod. 2mh), entonces m, m, mi, Q<2rñmT serón enteros. Es facil confirmar que la forma (a, h, 0) sera transformada en la forma (a',h, 0) por la sustitución —y, ——, α<α~m , —, y que esta transformacion es impropia. Por lo tanto las dos formas seran impropiamente equivalentes. Q. E. S.

Ahora de [5] y [6] se sigue que aa + 2Λ,γ divide a 2h ya a, de donde tambien a m, que es el maximo comón divisor de a y 2h; sin embargo manifiestamente m tambien divide a aa + 2Λ,γ; por lo tanto necesariamente aa + 2Λ,γ seró = +m o = —m. Y se sigue inmediatamente de [7] que m2 = aa' (mod. 2mh) Q. E. P.

II. Si a y 2h, a' y 2h tienen el mismo móximo comun divisor m y ademas

aa

De esto puede juzgarse inmediatamente si alguna forma reducida dada (a, h, 0) es impropiamente equivalente a sí misma. Esto es, si m es el maximo comón divisor de los números a y 2h, deberemos tener a2 = m2 (mod. 2mh).

211.

Todas las formas reducidas de un determinante dado h2 son obtenidas si en la forma indefinida (A, h, 0) se sustituye A por todos los 2h números de 0 hasta 2h — 1 inclusive. Claramente todas las formas del determinante h2 pueden ser distribuidas en este número de clases y tendrán las mismas propiedades mencionadas arriba (art. 175, 195) para las clases de formas con determinantes negativos y positivos no cuadrados. Entonces todas las formas con determinante 25 serán distribuidas en diez clases, que podrún distinguirse por las formas reducidas contenidas en cada una de ellas. Las formas reducidas serún: (0, 5, 0), (1,5,0), (2, 5, 0), (5, 5, 0), (8,5, 0), y (9, 5, 0), cada uno de los cuales es impropiamente equivalente a si misma; (3, 5, 0) que es impropiamente equivalente a (7, 5, 0), y (4, 5, 0) que es impropiamente equivalente a (6,5,0).

212.

PROBLEMA. Encontrar todas las representaciones de un número dado M por una forma dada ax2 + 2bxy + cy2 con determinante h2.

La solucioún de este problema puede buscarse a partir de los principios del articulo 168 exactamente de la misma manera que enseñamos arriba (art. 180, 181, 205) para formas con determinantes negativos y positivos no cuadrados. Sería superfluo repetirla aquí, puesto que no ofrece dificultad alguna. Por otro lado, no estarúa fuera de lugar deducir la solucioún de otro principio que es propio para el caso presente.

Como en los artúculos 206 y 208:

h — b : a = c : — (h + b)= β : δ h — b a c —h — b

β = δ =f; β = δ = g

y se muestra sin dificultad que la forma dada es un producto de los factores δχ — βγ y fx — gy. Entonces es evidente que cualquier representaciún del numero M por la forma dada debe proveer una resoluciúon del nuúmero M en dos factores. Si, por lo tanto, todos los divisores del número M son d, d0, d00, etc., (incluyendo tambien a 1 y M, y cada uno tomado dos veces, o sea positivamente y negativamente), es claro que todas las representaciones del nuúmero M serúan obtenidas si se pone sucesivamente

que

δx - βy = d, fx - gy = —

δχ - βy = d0, fx - gy = — etc.

Los valores de x e y se derivarán de aquí, y aquellas representaciones que producen valores fraccionales de x e y deberán ser descontadas. Pero, manifiestamente, de las dos primeras ecuaciones resulta

β— - gd2 δ— - fd2

^f - δg)d e y = W-W

Estos valores serán siempre determinados porque βf - δg = 2h y entonces el denominador con certeza no será = 0. Por lo demas, por el mismo principio podríamos haber resuelto los otros problemas respecto a la resolubilidad de cualquier forma con un determinante cuadrado en dos factores; pero preferimos usar un metodo analogo a aquel presentado arriba para formas con determinante no cuadrado.

Ejemplo. Buscaremos todas las representaciones del námero 12 por la forma 3x2 + 4xy - 7y2. Esto es resuelto en los factores x - y y 3x + 7y. Todos los divisores del námero 12 son ±1, 2, 3, 4, 6, 12. Poniendo x - y = 1 y 3x + 7y = 12 obtenemos x = 10 e y = 10, lo que debe ser rechazado porque son fracciones. De la misma manera obtenemos valores inátiles de los divisores -1, ±3, ±4, ±6, ±12; pero del divisor +2 se obtienen los valores x = 2, y = 0 y del divisor -2, x = -2, y = 0. No existen, por lo tanto, otras representaciones excepto estas dos.

Este metodo no se puede usar si — = 0. En este caso, manifiestamente, todos los valores de x e y deben satisfacer ya sea la ecuacián δx—βy = 0 o fx-gy = 0. Todas las soluciones de la primera ecuación están contenidas en la fármula x = βζ, y = δζ, donde z es cualquier entero (mientras β y δ sean primos relativos, como supusimos); similarmente, si ponemos m como el maximo comun divisor de los números f y g, todas las soluciones de la segunda ecuacián estarán representadas por la fármula x = m, y = m. Entonces estas dos formulas generales incluyen en este caso a todas las representaciones del nuámero —.

En la discusion precedente todo lo concerniente a la equivalencia, al descubri­miento de todas las transformaciones de formas, y a la representacioán de nuámeros dados por formas dadas ha sido explicado satisfactoriamente. Solo resta, por consiguiente, mostrar cámo juzgar si una de dos formas dadas, que no pueden ser equivalentes porque tienen determinantes no iguales, esta contenida en la otra o no, y, en este caso, encontrar las transformaciones de la una en la otra.

Formas contenidas en otras a las cuales no son equivalentes.

213.

En los artículos 157 y 158 arriba mostramos que, si la forma f con determinante D implica a la forma F con determinante E y es transformada en ella por la sustitución α, β, γ, δ, entonces E = (αδ — βγ)2D; y que si αδ — βγ = ±1, la forma f no sólo implica a la forma F sino que es equivalente a ella. Por consiguiente, si la forma f implica a F pero no es equivalente a esta, el cociente D es un entero mayor que 1. Este es el problema que por lo tanto deberá resolverse: juzgar cuando una forma dada f con determinante D implica a una forma dada F con determinante De2 donde se supone que e es un numero positivo mayor que 1. Para resolver esto, mostremos como asignar un numero finito de formas contenidas en f, escogidas tal que si F esta contenida en f, deba ser equivalente necesariamente a una de estas.

1. Supongamos que todos los divisores positivos de un numero e (incluyendo 1

y e) son m, m',m" etc. y que e = mn = m'n' = m"n" etc. Por brevedad, indicaremos por (m; 0) la forma en la cual f es transformada por la sustitución propia m, 0, 0, n; por (m; 1) la forma en la cual f es transformada por la sustitucion propia m, 1, 0, n, etc.; y en general por (m; k) la forma en la que f es cambiada por la sustitucion propia m, k, 0, n. Similarmente, f sera transformada por la transformacion propia m', 0, 0, n' en (m';0); por m', 0, 1, n' en (m';1) etc.; por m'', 0, 0, n'' en (m'';0)

etc.; etc. Todas estas formas estarón contenidas propiamente en f y el determinante de cada una seró = De2. Designaremos por Ω el conjunto de todas las formas (m;0), (m;1), (m;2), ... (m; m — 1), (m';0), (m';1), ... (m'; m' — 1), (m'';0), etc. Habró m + m' + m'' + etc. de ellas y es facil ver que todas serán diferentes la una de la otra.

Si, e.g., la forma f es (2, 5, 7) y e = 5, Ω incluirá las siguientes formas (1;0), (5;0); (5;1), (5; 2), (5; 3), (5; 4), y si son expandidas serón (2, 25,175), (50, 25, 7), (50,35,19), (50,45,35), (50,55,55), (50,65, 79).

1. Ahora, afirmo que si la forma F con determinante De2 esta propiamente contenida en la forma f, sera necesariamente propiamente equivalente a una de las formas Ω. Supongamos que la forma f es transformada en F por la sustitución propia α, β, γ, δ; tendremos αδ — βγ = e. Sea n el móximo comun divisor de los números γ, δ (que no pueden ser 0 al mismo tiempo) y sea n = m, lo que sera, manifiestamente, un entero. Tomense g y h tal que γg + δύ = n, y finalmente sea k el residuo positivo mínimo del nómero αg + βύ segón el modulo m. Entonces la forma (m; k), que esta manifiestamente entre las formas Ω, sera propiamente equivalente a la forma F y sera

transformada en ella por la sustitución propia

δ ag + βΚ — k γ

γ \_ ag + βΚ — k + ^ n m

δ

*n*

g,

n m n

Primeramente, es claro que estos cuatro nómeros son enteros; en segundo lugar, es fócil confirmar que la sustitución es propia; en tercer lugar, es claro que la forma en la cual (m; k) se transforma por esta sustitución es la misma en la que f [[163]](#footnote-164)) se transforma por la sustitucióon

γ ag + βΚ — k ,. γ ,δ ag + βΚ — k

, kδ

g) + —, Y, δ

m(

— · + Κ) + k—, m(— ·

n m n n m n

o puesto que mn = e = αδ — βγ y entonces βγ + mn = αδ, αδ — mn = βγ, esta es

la sustitución 1 1

-(ajg + αδΚ), -(βγg + βδΚ), γ, δ

nn

Pero γ g + δΚ = n, así que esta es la sustitución α, β, γ, δ, i.e. por hipotesis esta transforma f en F. Así (m; k) y F serán propiamente equivalentes. Q. E. D.

De esto, por consiguiente, podemos siempre juzgar cuando una forma dada f con determinante D implica propiamente a la forma F con determinante De2. Si queremos encontrar cuando f implica impropiamente a F, solo necesitamos investigar cuando la forma opuesta a F esta contenida en f (art. 159).

214.

PROBLEMA. Dadas dos formas, f con determinante D y F con determinante De2, donde la primera implica propiamente a la segunda: encontrar todas las

transformaciones propias de la forma f en F.

Solución. Designando por Ω el mismo conjunto de formas como en el artículo precedente, extraiga de este conjunto todas las formas Φ, Φ0, Φ00, etc. a las cuales F es propiamente equivalente. Cada una de estas formas proporcionara transformaciones propias de la forma f en F y cada una de ellas dara una transformacion diferente, pero en total las proporcionaran todas (i.e., no habrá ninguna transformacion propia de la forma f en F que no surja de una de las formas Φ, Φ0, etc.). Puesto que el metodo es el mismo para todas las formas Φ, Φ0, etc., hablamos de solo una de ellas.

Supongamos que Φ es (M; K) y e = MN de manera que f se transforme en Φ por la sustitución propia M, K, 0, N. Además desígnense todas las transformaciones propias de la forma Φ en F en general por a, b, c, d. Entonces claramente f se transformará en Φ por la substitución propia Ma + Kc, Mb + Kd, Nc, Nd y de esta manera cualquier transformacioón propia de la forma Φ en F daróa una transformacioón propia de la forma f en F. Las otras formas Φ0, Φ00, etc. se tratan del mismo modo, y cada transformación propia de una de estas en F dará lugar a una transformación propia de la forma f en F.

Para mostrar que esta solution es completa en todo aspecto, se mostrara

1. Que todas las transformaciones propias posibles de la forma f en F se obtienen de este modo. Sea α, β, γ, δ cualquier transformation propia de la forma f en F y como en el artículo anterior, parte II, sea n el maximo comón divisor de los nómeros γ y δ; y sean los numeros m, g, h, k determinados tal como lo fueron allí. Entonces la forma (m; k) estaró entre las formas Φ, Φ0, etc. y

7

n

ag + βΛ — k  
m

+ h,

δ ag + βΛ — k γ

*g, -,*

n m n

*δ*

n

sera una de las transformaciones propias de esta forma en F; a partir de esta, por la regla que acabamos de dar, se obtiene la transformation α, β, γ, δ; todo esto fue demostrado en el artículo precedente.

1. Que todas las transformaciones obtenidas de esta manera son diferentes entre sí; esto es, ninguna de ellas se obtiene dos veces. Es facil ver que

transformaciones diferentes de la misma forma Φ o Φ0, etc. en F no pueden producir la misma transformacion de f en F; se muestra de la siguiente manera que formas diferentes, por ejemplo Φ y Φ0, no pueden producir la misma transformation. Supongamos que la transformacion propia α, β, γ, δ de la forma f en F se obtiene tanto de la transformación propia a, b, c, d de la forma Φ en F como de la transformation propia a0, b0, c0, d0 de la forma Φ0 en F. Sean Φ = (M; K),

Φ0 = (M0; K0) y e = MN = M0N0. Habra estas ecuaciones:

α = M a + K c = M0a0 + K0c0 [1]

β = M b + Kd = M 'b' + K0d0 [2]

γ = N c = N0c0 [3]

δ = Nd = N0d0 [4]

ad — bc = a0d0 — b0c0 = 1 [5]

De a[4] — b[3] y usando ecuación [5] se sigue que N = N'(ad' — bc'), y de este modo N' divide a N; de manera análoga, de a'[4] — b'[3] resulta N' = N(a'd — b'c) y N divide a N', de donde, dado que ambos N y N' se suponen positivos, tenemos necesariamente N = N' y M = M' y así de [3] y [4], c = c' y d = d'. Ademas, de a[2] — b[1],

K = M'(ab' — ba') + K'(ad' — bc') = M (ab' — ba') + K'

de aquí K ξ K' (mod. M), lo que no puede ser cierto a menos que K = K', porque ambos K y K' se encuentran entre los límites 0 y M — 1. Por lo tanto las formas Φ y Φ' no son diferentes, contrariamente a la hipotesis.

Es claro que si D es negativo o un cuadrado positivo, este metodo nos dará todas las transformaciones propias de la forma f en F; y si D es positivo no cuadrado, pueden darse ciertas fáormulas generales que contendraán todas las transformaciones propias (su námero es infinito).

Finalmente, si la forma F esta impropiamente contenida en la forma f, todas las transformaciones impropias de la primera en la uáltima pueden encontrarse fácilmente por el metodo dado. A saber, si α, β, γ, δ designan en general todas las transformaciones propias de la forma f en la forma opuesta a la forma F, todas las transformaciones impropias de la forma f en F serán representadas por α, —β, γ, δ.

Ejemplo. Se desean todas las transformaciones de la forma (2,5,7) en (275, 0, —1), la cual esta contenida en ella tanto propia como impropiamente. En el artículo precedente dimos el conjunto de las formas Ω para este caso. Despues de unos calculos, se encuentra que tanto (5; 1) como (5; 4) son propiamente equivalentes a la forma (275, 0, — 1). Todas las transformaciones propias de la forma (5; 1), i.e., (50, 35, 19) en (275, 0, — 1), se pueden hallar por nuestra teoría arriba dentro de la fármula general

16t — 275u, —t + 16u, — 15t + 275u, t — 15u

donde t y u son representaciones indeterminadas de todos los enteros que satisfacen la ecuacián t2 — 275u2 = 1; por lo tanto todas las transformaciones propias de la forma (2, 5, 7) en (275, 0, —1) estarán contenidas en la formula general

65t — 1100u

4t + 65u,

15t + 275u, t — 15u.

De manera análoga, todas las transformaciones propias de la forma (5; 4), i.e., (50, 65, 79) en (275, 0, -1), estan contenidas en la formula general

14t + 275u, t + 14u, — 15t — 275u, —t — 15u

y así todas las transformaciones propias de la forma (2, 5, 7) en (275, 0, —1) estarán contenidas en

10t + 275u, t + 10u, — 15t — 275u, —t — 15u

Por lo tanto, estas dos formulas incluyen todas las transformaciones propias que buscamos[[164]](#footnote-165)). De la misma manera se encuentra que todas las transformaciones impropias de la forma (2, 5, 7) en (275, 0, —1) estan contenidas en las dos formulas siguientes:

1. ... 65t — 1100u, 4t — 65u, —15t +275u, —t + 15u

y (II) ... 10t + 275u, —t — 10u, — 15t — 275u, t + 15u

Formas con determinante 0.

215.

Hasta ahora hemos excluido de todas las investigaciones las formas con determinante 0; ahora agreguemos algo acerca de estas formas para que nuestra teoría sea completa en todos los sentidos. Dado que se mostró en general que, si una forma con determinante D implica a una forma con determinante D0, D0 es un multiplo de D, es inmediatamente claro que una forma cuyo determinante es igual a cero no puede implicar a otra forma a menos que su determinante tambien sea igual a cero. Así solamente dos problemas quedan por resolver, a saber: (1) dadas dos formas f y F, donde F tiene determinante 0, juzgar si f implica a F o no, y,

en ese caso, exhibir todas las transformaciones involucradas; (2), encontrar todas las representaciones de un número dado por una forma dada con determinante 0. El primer problema requiere de un método cuando el determinante de la forma f es también 0, otro cuando no es 0. Ahora explicamos todo esto.

1. Antes de todo observamos que cualquier forma ax2 + 2bxy + cy2 cuyo determinante es b2 — ac = 0 puede ser expresada como m(gx + hy)2 donde g y h son primos relativos y m un entero. Pues, sea m el maximo común divisor de a y c con el mismo signo que ellos (es fúcil ver que ellos no pueden poseer signos opuestos), entonces f y ff serán enteros primos relativos no negativos, y su producto serú igual

b2 ^ , , .

a , i.e., un cuadrado, y así cada uno de ellos sera tambien un cuadrado (art. 21). Sean ff = g2 y ff = h2 con g y h tambien primos relativos, y tenemos g2h2 = f y gh = ± -f. Así es claro que

m(gx ± hy)2 sera

22 = ax + 2bxy + cy

Sean ahora f y F dos formas dadas, cada una con determinante 0 y con

f = m(gx + hy)2, F = M (GX + HY )2

donde g y h, G y H son primos relativos. Afirmo ahora que si la forma f implica a la forma F, m es igual a M o al menos divide a M, y el cociente es un cuadrado; y, recíprocamente, si f es un entero cuadrado, F esta contenida en f. Pues si se asume que f se transforma en F, por la substitucion

x = aX + βΥ, y = 7X + δΥ

M2 m (GX + HY )2 = ((ag + 7h)X + (eg + úh)Y )2

resultara

y se sigue facilmente que f es un cuadrado. Iguarándole a e2, tenemos

e(GX + HY) = ± ((ag + 7h)X + (£g + úh)Y), i.e. ±eG = ag + 7h, ±eH = eg + δΛ,

Por lo tanto si G y H se determinan de modo que GG + HH = 1 obtenemos

±e = G(ag + 7h) + H(eg + δύ,)

y por ende un *entero. Q. E. P.*

Si, recíprocamente, se supone que M es un entero cuadrado igual a e2, la forma f implicará a la forma F. Esto es, los enteros α, β, γ, δ pueden determinarse de modo que

ag + γh = ±eG, β^ + δh = ±eH

Pues si se encuentran enteros 0 y h de modo que gg + hh = 1, podemos satisfacer estas ecuaciones poniendo:

a = ±eGg + hz, γ = ±eGh — gz

β = ±eH 0 + hz0, δ = ±eH h — gz0

donde z y z0 pueden tomar valores enteros cualesquiera. Así F estará contenida en f. Q. E. S. Al mismo tiempo no es difícil ver que estas formulas dan todos los valores que α, β, γ, δ pueden asumir, i.e., todas las transformaciones de la forma f en F, a condición que z y z0 asuman todos los valores enteros.

1. Propuestas las dos formas f = ax2 + 2bxy + cy2 cuyo determinante no es igual a 0, y F = M(GX + HY)2 cuyo determinante es igual a 0 (aquí como antes G y H son primos entre si), afirmo primero que si f implica a F, el numero M puede representarse por la forma f; segundo, si M puede representarse por f, F estará contenida en f; tercero, si en este caso todas las representaciones del námero M por la forma f pueden ser exhibidas en terminos generales por x = ξ e y = ν, todas las transformaciones de la forma f en F pueden exhibirse por Gξ, Hξ, Gv , Hv. Mostramos todo esto de la siguiente manera.

1o Suponga que f se transforma en F por la substitution α, β, γ, δ y tomense námeros G, H de modo que GG + HH = 1. Entonces si hacemos x = aG + βΗ, y = γ G + δΗ, el valor de la forma f se hará M y así M es representable por la forma

f.

2o Si se supone que αξ2 + 26ξν + cv2 = M, por la substitucián Gξ, Hξ, Gv, Hv la forma f se transformará en F.

3o En este caso la substitution Gξ, Hξ, Gv, Hv presentará todas las transformaciones de la forma f en F si se supone que ξ y ν recorren todos los valores de x e y que hacen f = M; se muestra esto del siguiente modo. Sea α, β, γ, δ cualquier transformacián de la forma f en F y sea como antes GG + HH = 1. Entonces entre los valores de x e y estarán tambien estos:

x = α0 + β Η

y = γG + δΗ

de los cuales se obtiene la substitución

G(aG + βΗ), H (α0 + β H), G(70 + δΗ), H (γ 0 + δΗ)

o

α + H(eG — αΗ), β + 0(αΗ — eG), γ + H^G — γΗ), δ + Η(γΗ — γG).

Pero ya que

α(αΧ + βΥ )2 + 2δ(αΧ + βΥ )(γΧ + δΥ) + φΧ + δΥ )2 = M (GX + HY )2 resultaraó

α(αδ — βγ)2 = M ^G — γΗ)2 c(βγ — αδ)2 = M (βG — αΗ )2

y así (ya que el determinante de la forma f multiplicado por (αδ determinante de la forma F, i.e., igual a 0, y así tambien αδ — βγ

— βγ)2 es igual al = 0),

δG — γΗ = 0, βG — αΗ = 0

Por consiguiente la substitución en cuestión se reduce a α, β, γ, δ, y la fórmula que estamos considerando produce todas las transformaciones de la forma f en F.

1. Queda por mostrar como podemos exhibir todas las representaciones de un nómero dado por una forma dada con determinante 0. Sea esta forma m(gx+hy)2, y es claro inmediatamente que el nómero debe ser divisible por m y que su cociente es un cuadrado. Si por lo tanto representamos al nómero dado por me2, los valores de x e y que hacen m(gx + hy)2 = me2 serán aquellos valores para los cuales gx + hy sea igual a +e o a —e. Así se tendrán todas las representaciones si se encuentran todas las soluciones enteras de las ecuaciones lineales gx + hy = e y gx + hy = — e. Es claro que estas son resolubles (si verdaderamente g y h son primos relativos como se supone). Esto es, si 0 y h son determinados de modo que gg + hh = 1, la primera ecuacion se satisfará poniendo x = 0e + hz, y = he — gz; la segunda tomando x = —0e + hz, y = —he — gz con z cualquier entero. Al mismo tiempo estas formulas darán todos los valores enteros de x e y si z representa en general a cualquier entero.

Solución general de toda ecuación indeterminada de segundo grado  
con dos incognitas por numeros enteros.

Habiendo concluido exitosamente estas investigaciones, proseguimos.

216.

PROBLEMA. Encontrar todas las soluciones enteras para la ecuación gen­eral [[165]](#footnote-166)) indeterminada de segundo grado con dos incógnitas

ax2 + 2bxy + cy2 + 2dx + 2ey + f = 0

(donde a, b, c, etc. son cualesquiera enteros dados).

Solución. En lugar de las incognitas x e y introducimos otras

p = (b2 — ac)x + be — cd y q = (b2 — ac)y + bd — ae

que siempre serán enteros cuando x e y son enteros. Ahora resulta la ecuacion

ap2 + 2bpq + cq2 + f (b2 — ac)2 + (b2 — ac)(ae2 — 2bde + cd2) = 0

o si por brevedad escribimos

f (b2 — ac)2 + (b2 — ac)(ae2 — 2bde + cd2) = — M

se da

ap2 + 2bpq + cq2 = M

Mostramos en la seccion precedente como encontrar todas las soluciones de esta ecuacion, i.e., todas las representaciones del número M por la forma (a, b, c). Ahora si para cada valor de p y q determinamos los valores correspondientes de x e y con la ayuda de las ecuaciones

p + cd — be q + ae — bd

x = —?¡ , y = —?¡

b2 — ac b2 — ac

es facil ver que todos estos valores satisfacen la ecuaciún dada y que no existen valores enteros de x e y que no se incluyen. Si por lo tanto eliminamos las fracciones entre todos los valores de x e y así obtenidos, todas las soluciones que deseamos permaneceraún.

Con respecto a estas soluciones se observa lo siguiente.

1o Si M no puede representarse por la forma (a, b, c) o si no se obtienen valores enteros de x e y de ninguna representación, la ecuación no puede resolverse por enteros del todo.

2o Cuando el determinante de la forma (a, b,c), i.e. el número b2 — ac, es negativo o un cuadrado positivo y al mismo tiempo M no es igual a 0, el numero de representaciones del número M sera finito y así tambien el número de soluciones de la ecuaciún dada (si es que existe alguna) sera finito.

3o Cuando b2 — ac es positivo no cuadrado, o cuadrado con M igual a 0, el numero M podrú representarse en infinitamente distintas maneras por la forma (a, b, c) si es que puede representarse de alguna manera. Pero dado que es imposible encontrar todas estas representaciones individualmente y examinar si ellas dan valores enteros o fraccionarios de x e y, es necesario establecer una regla bajo la cual podamos tener certeza de cuando ninguna representacion en absoluto produce valores enteros de x e y (puesto que no importa cuaúntas representaciones se intenten, sin una regla tal nunca estaremos seguros). Y cuando algunas representaciones dan valores enteros de x e y y otras dan fracciones, debe determinarse coúmo distinguir en general una de la otra.

4o Cuando b2 — ac = 0, los valores de x e y no pueden determinarse del todo por las fúrmulas precedentes; por lo tanto para este caso necesitaremos recurrir a un método especial.

217.

Para el caso donde b2 — ac es un nuúmero positivo no cuadrado, mostramos arriba que todas las representaciones del número M por la forma ap2 + 2bpq + cq2 (si es que existe alguna) pueden exhibirse por una o por varias fórmulas como la siguiente:

11

p = —(At + Bu), q = —(Ct + Du)

m m

donde A, B, C, D son enteros dados, m es el maximo común divisor de los numeros a, 2b y c, finalmente t y u son en general todos los enteros que satisfacen la ecuaciún t2 — (b2 — ac)u2 = m2. Como todos los valores de t y u pueden tomarse tanto positiva como negativamente, para cada una de estas formas podemos substituir otras cuatro:

p = (At + Bu), q = (Ct + Du)

mm

de modo que el número de fórmulas es ahora cuatro veces lo que era antes, y t y u ya no son todos los numeros que satisfacen la ecuación t2 — (b2 — ac)a2 = m2 sino solamente los valores positivos. Por lo tanto cada una de estas formas sera considerada separadamente, y debe investigarse cuóles valores de t y u dan valores enteros de x e y.

De la fórmula

p = —(At + Bu), q = —(Ct + Du)

[1]

p = —(At + Bu), m

*p = — (At — Bu), m*

*p = — (—At* + Bu), *m*

q = —(Ct + Du) m

q = — (Ct — Du) m

*q = —(—Ct* + Du) *m*

mm

los valores de x e y serán estos:

At + Bu + mcd — mbe Ct + Du + mae — mbd

m(b2 — ac) , y m(b2 — ac)

Demostramos antes que todos los valores (positivos) de t forman una serie recurrente t0, t0, t", etc. y similarmente, que los valores correspondientes de u tambien forman una serie recurrente u0, u0, u00, etc.; y que ademas puede asignarse un nómero ρ tal que segun cualquier modulo dado tengamos

tp = t0, tp+1 = t0, tp+2 = t00 etc., up = u0, up+1 = u0, etc.

Tomaremos para este modulo el nómero m(b2 — ac) y por brevedad designaremos por x0 e y0 los valores de x e y que se obtienen haciendo t = t0, u = u0; de la misma manera x0 e y0 designaran los valores que se obtienen haciendo t = t0 y u = u0, etc. Entonces no es difícil notar que si xh e yh son enteros y ρ apropiadamente escogido, xh+p e yh+p, xh+2p e yh+2p y, en general, xh+kp e yh+kp tambien serán enteros; y recíprocamente, si xh o yh es una fraccion, xh+kp o yh+kp seró tambien una fracción. Se concluye que si uno revisa los valores de x e y correspondientes a los óndices 0, 1,2, ...ρ — 1 y encuentra que no hay uno de ellos para el cual tanto x como y sea

entero, entonces no existen en absoluto índices, para los cuales ambos x e y posean valores enteros, y así de la formula [1] no se pueden deducir valores enteros de x e y. Pero si existen algunos índices, digamos μ, μ', μ", etc., para los cuales x e y poseen valores enteros, entonces todos los valores de x e y que pueden obtenerse a partir de la fórmula [1] serán aquellos cuyos índices esten contenidos en una de las formulas μ + kp, μ' + kp, μ1' + kp, etc., donde k es cualquier entero positivo incluyendo al cero.

Las otras fórmulas que contienen los valores de p y q pueden tratarse exactamente de la misma manera. Si se diera el caso que de ninguna de estas se obtienen valores enteros de x e y, entonces la ecuación propuesta no puede ser resuelta por enteros. Pero cuando esta puede ser resuelta, todas las soluciones enteras se pueden mostrar por medio de las reglas precedentes.

218.

Cuando b2 — ac es un cuadrado y M es igual a cero, todos los valores de p y q estón incluidos en dos fórmulas de la forma p = Az, q = Bz o p = A'z, q = B'z, donde z indica de modo indefinido a cualquier entero, A, B, A', B' son enteros dados, y el primero y el segundo no han de poseer un divisor comón, ni tampoco el tercero y el cuarto (art. 212). Todos los valores enteros de x e y que surgen de la primera formula estarán contenidos en la fórmula [1]:

Az + cd — be Bz + ae — bd

x T2 , y

b2 — ac b2 — ac

y todos los otros que surjan de la segunda formula estarán contenidos en [2]:

A'z + cd — be B'z + ae — bd

b2 — ac b2 — ac

Pero dado que cada formula puede producir valores fraccionarios (a menos que b2 — ac = 1), es necesario separar de los otros, en cada formula, aquellos valores de z que hacen a ambos x e y enteros. Sin embargo, es suficiente considerar la primera formula solamente, dado que exactamente el mismo metodo puede usarse para la otra.

Como A y B son primos relativos, se pueden determinar dos números a y b tales que aA + bB = 1. De esto se obtiene

(ax + by)(b2 — ac) = z + a(cd — be) + b(ae — bd)

De esto es inmediatamente claro que todos los valores de z que producen valores enteros de x e y deben ser congruentes al número a(be — cd) + b(bd — ae) segun el modulo b2—ac, o deben estar contenidos en la fúrmula (b2—ac)z0+a(be—cd)+b(bd—ae) donde z0 designa cualquier entero. Entonces en lugar de la fúrmula [1] obtenemos facilmente la siguiente:

x =

y =

0 *A(bd — ae) — B(be — cd)*

b2 — ac

*A(bd — ae) — B(be — cd)*

*Bz -* a

b2

*ac*

Queda de manifiesto que esta da valores enteros para x e y ambos para todos los valores de z0 o para ninguno. Lo primero serú cierto cuando A(bd — ae) y B(be — cd) sean congruentes según el modulo b2 — ac, el ultimo cuando ellos no sean congruentes. Podemos tratar la fúrmula [2] exactamente de la misma manera y separar las soluciones enteras (si existe alguna) del resto.

219.

Cuando b2 — ac = 0, la forma ax'2 + 2bxy + cy2 puede expresarse como m(ax + ey)2 donde m, a, β son enteros (art. 215). Si se pone ax + ey = z, la ecuaciún se convertirá en:

mz2 + 2dx + 2ey + f = 0

De esto y del hecho que z = ax + ey deducimos que

emz2 + 2ez + ef

x=

*2ae— 2ed*

y =

*amz2* + *2dz* + *af  
2ed— 2ae*

Ahora es claro que si no fuera ae = ed (consideraremos este caso por separado de inmediato), los valores de x e y obtenidos a medida que z toma cualquier valor en estas fúrmulas, satisfarán la ecuaciún dada; por lo tanto, solo queda por demostrar como determinar los valores de z que darán valores enteros de x e y.

Dado que ax + ey = z, puede escogerse súlo valores enteros para z. Ademas es claro que si cualquier valor de z da valores enteros tanto para x como para y, todos los valores congruentes con z según el múdulo 2ae — 2ed producirán de la

misma manera valores enteros. Por esto si se substituyen en z todos los enteros de 0 a 2ae — 2βd — 1 (cuando ae — βd es positivo) o inclusive a 2βd — 2ae — 1 (cuando ae — βd es negativo), y si para ninguno de estos valores se hacen x e y enteros, entonces ningún valor de z producirá valores enteros para x e y, y la ecuación dada no podrá resolverse por enteros. Pero si x e y poseen valores enteros para alguno de esos valores de z, digamos ζ, ζ0, ζ", etc., (ellos tambien pueden hallarse resolviendo la congruencia de segundo grado de acuerdo con los principios de la sección IV), se encuentran todas las soluciones poniendo z = (2ae — 2βd)ν + ζ, z = (2ae — 2βd)ν + ζ0, etc., con ν tomando todos los valores enteros.

220.

Es conveniente indagar un metodo especial para el caso que hemos excluido, donde ae = βd. Supongamos que a y β son primos entre sí, lo cual es posible por el artículo 215.I; así ^ e sera un entero (art. 19), que llamamos h. Entonces, la ecuación dada tomara esta forma:

c\ c\

(max + mβy + h)2 — h + mf = 0

y claramente esta no puede resolverse racionalmente, a menos que h2 — mf sea un cuadrado. Sea h2 — mf = k2, y la ecuación dada será equivalente a las siguientes dos:

max + mβy + h + k = 0, max + mβy + h — k = 0

i.e., cualquier solución de la ecuación dada satisfará una u otra de estas ecuaciones y viceversa. Obviamente la primera ecuación no puede resolverse por enteros a menos que h + k sea divisible por m, y, similarmente, la segunda ecuacion no admitiró solución por enteros a no ser que h — k sea divisible por m. Estas condiciones son suficientes para resolver todas las ecuaciones (porque nosotros asumimos que a y β son primos entre só) y puede encontrarse todas las soluciones usando reglas bien conocidas. [[166]](#footnote-167)

Todas las soluciones por enteros de esta ecuación se encuentran por consiguiente contenidas en las siguientes cuatro fórmulas:

p = 6t, q = — 24t — 90u

p = 6t, q = —24t + 90u

p = —6t, q = 24t — 90u

p = —6t, q = 24t + 90u

donde t y u denotan todos los enteros positivos que satisfacen la ecuacion t2 — 15u2 = 1, y ellos se expresan por la fórmula:

t = 1 ((4 + 75)" + (4 — 75)")

u = 575 ((4+ ^5)" — (4 —G5)")

donde n designa a todos los enteros positivos (incluido el cero). Por esto todos los valores de x e y estarán contenidos en estas formulas

*x*

*x*

*x*

*x*

1

5

1

5

1

5

1

5

(2t + 3) y

(2t + 3) y

(—2t + 3) y

(—2t + 3) y

* y (8t + 30u + 2) 5

1

* - (8t — 30u + 2) 5

1

-(8t — 30u — 2)

5

1. (8t + 30u — 2)

5

Si aplicamos correctamente lo que hemos dicho arriba, descubrimos que para producir enteros debemos usar en la primera y segunda formulas valores de t y u que vienen de tomar n par; en la tercera y cuarta de tomar n impar. Las soluciones mas simples son: x = 1, —1, — 1 e y = —2, 0, 12 respectivamente.

Por otra parte, observamos que la solución del problema en los artículos precedentes puede a menudo acortarse por varios artificios especialmente ideados para excluir soluciones inutiles, i.e., fracciones; pero debemos omitir esta discusion a fin de no prolongar nuestra discusion mas alla de los límites.

Anotaciones Históricas.

222.

Dado que mucho de lo que hemos explicado también ha sido tratado por otros geómetras, no podemos pasar sobre sus trabajos en silencio. El ilustre Lagrange emprendió investigaciones generales concernientes a la equivalencia de las formas en Nouv. Móm. de l’Ac. de Berlin, 1773, p. 263 y 1775, p. 323 y siguientes, donde el mostro, que para un determinante dado, puede encontrarse un número finito de formas tales que cada forma de ese determinante sea equivalente a una de estas, y así que todas las formas de un determinante dado pueden distribuirse en clases. Mas tarde el distinguido Legendre descubrio, en gran parte por induction, muchas propiedades elegantes de esta clasificacion, cuyas demostraciones presentaremos mas abajo. Hasta aquí nadie ha usado la distincion entre equivalencia propia e impropia, pero este es un instrumento muy efectivo para investigaciones mas sutiles.

Lagrange fue el primero en resolver completamente el famoso problema del artículo 216 y siguientes, Hist. de l’Ac. de Berlin, 1767, p. 165 y 1768 p. 181 y siguientes. Tambien existe una solucion (pero menos completa) en el suplemento al Algebra de Euler, el cual hemos nombrado regularmente. El mismo Euler ataco este problema en Comm. Petr., T. VI, p. 175, Comm. Nov., T. IX, p. 3; Ibid., T. 18, p. 185 y siguientes, pero el siempre restringio su investigation a derivar otras soluciones de una que el asumía ya conocida; ademas, sus metodos pueden dar todas las soluciones en solamente unos cuantos casos (vease Lagrange Hist. de l’Ac. de Berlin, 1767, p. 237). Ya que el ultimo de estos tres comentarios es de fecha mas reciente que la solucion de Lagrange, que trata el problema con toda generalidad y no deja nada que desear en este aspecto, parece que Euler no sabía entonces de esa solucion (el Vol. 18 de los Commentarii corresponde al año 1773 y fue publicado en 1774). Por lo demas, nuestra solucion (al igual que todas las cosas discutidas en esta seccion) es construida sobre principios totalmente diferentes.

Lo que Diofanto, Fermat, etc., entre otros, han tratado en relation con este tema pertenece solamente a casos especiales; por esto, ya que arriba hemos mencionado lo mas digno de notar, no lo discutiremos separadamente.

Lo que ha sido dicho hasta aquí acerca de las formas de segundo grado debe ser considerado solamente como los primeros principios de esta teoría. El campo dejado para investigacion posterior parece muy vasto, y en lo que sigue notaremos cualquier cosa que parezca especialmente digna de atencion. Pero esta línea del argumento es tan fertil que deberemos pasar sobre muchos otros resultados que hemos descubierto, y sin duda muchos mas permaneceran ocultos, esperando una

más amplia investigación. Finalmente, conviene notar que formas con determinante 0 estan excluidas de los límites de nuestra investigacion, a menos que específicamente mencionemos lo contrario.

Distribución de formas de un determinante dado en clases.

223.

Ya hemos mostrado (arts. 175, 195, 211) que, dado cualquier entero D (positivo o negativo) se puede asignar un número finito de formas F, F', F", etc. con determinante D, tal que cada forma de determinante D sea propiamente equivalente a una, y súlo una, de estas. Así todas las formas con determinante D (su número es infinito) pueden clasificarse según estas formas para componer una primera clase del conjunto de todas las formas propiamente equivalentes a la forma F; una segunda clase de formas que son propiamente equivalentes a la forma F0, etc.

Una forma puede seleccionarse de cada una de las clases de formas con determinante dado D, y esta sera considerada como la forma representante de toda la clase. De por sí es enteramente arbitrario cual forma es tomada de una clase dada, pero se debe preferir siempre la que parezca ser mas simple que las demás. La simplicidad de una forma (a, b, c) ciertamente debe ser juzgada por el tamaño de los números a, b, c, y así la forma (a',b',c0) se dice menos simple que (a,b,c) si a0 > a, b0 > b, c0 > c. Pero esto no nos concede una determinaciún completa porque estaría ligeramente indefinido si e.g., escogemos (17, 0, -45) o (5, 0, -153) como la forma mas simple. Sin embargo, muy a menudo sería ventajoso observar las siguientes normas.

1. Cuando el determinante D es negativo, se toman las formas reducidas en cada clase como las formas representantes; cuando dos formas en la misma clase son formas reducidas (ellas serán opuestas, art. 172), se toma aquella cuyo termino medio sea positivo.
2. Cuando el determinante D es positivo no cuadrado, se calcula el período de toda forma reducida contenida en la clase. Existirún o bien dos formas ambiguas o ninguna (art. 187).

1) En el primer caso sean (A,B,C) y (A0,B0,C0) las formas ambiguas; y sean M y M0 los residuos múnimos de los numeros B y B0 según los módulos A y A0 respectivamente (que se pueden tomar positivamente a menos que sean iguales a cero); finalmente, sean = N, = N0. Habiendo hecho esto, de las

formas (A,M, —N) y (A0,M0, — N0), tomese como forma representante aquella que parezca ser la múas simple. Para juzgar esto, la forma cuyo túermino medio es igual a

cero es la preferida; cuando el término medio es cero o es distinto de cero en ambas, la forma que posee el menor primer termino se prefiere sobre la otra, y cuando los primeros terminos sean iguales en tamaño pero con signos opuestos, aquella con el signo positivo será la preferida.

2) Cuando no hay formas ambiguas en todo el período, se elige la forma cuyo primer termino sea menor, sin importar el signo. Si ocurren dos formas en el mismo período, una con signo positivo y la otra con el mismo termino con signo negativo, se deberá tomar la de signo positivo. Sea (A,B, C) la forma escogida y como en el caso anterior deducimos otra forma (A, M, — N) a partir de esta (esto es, tomando M como el menor residuo absoluto de B relativo al modulo A, y haciendo N = );

esta sera la forma representante.

Si sucediera que el mismo menor primer termino A fuera comun a varias formas del período, trátense todas estas formas de la manera que ya hemos delineado, y de las formas resultantes escójase como la forma representante aquella que posea el menor termino medio.

Así, e.g., para D = 305 uno de los períodos es: (17,4, —17), (—17,13, 8), (8,11, —23), (—23,12, 7), (7,16, —7), (—7,12, 23), (23,11, —8), (—8,13,17), del cual se escoje la forma (7, 16, —7), y entonces se deduce la forma representante (7, 2, —43).

1. Cuando el determinante es un cuadrado positivo igual a k2, se busca una forma reducida (A, k, 0) en la clase bajo consideration y, si A < k o = k, esta es tomada como forma representante. Pero si A > k, tomese en su lugar la forma (A — 2k, k, 0). El primer termino sera negativo, pero menor que k.

Ejemplo. De esta manera todas las formas del determinante -235 se dis- tribuiran en dieciseis clases con los siguientes representantes: (1,0, 235), (2, 1, 118), (4,1, 59), (4, —1,59), (5, 0,47), (10, 5, 26), (13, 5, 20), (13, —5, 20) y otras ocho que son diferentes de las anteriores solamente en que poseen terminos exteriores con signos opuestos: (-1, 0, -235), (—2,1, —118), etc.

Las formas con determinante 79 caen en seis clases con los siguientes repre­sentantes: (1, 0, —79), (3,1, —26), (3, —1, —26), (—1, 0, 79), (—3,1, 26), (—3, —1, 26). [[167]](#footnote-168)

que sea representable por una de ellas será también representable por la otra; y si un námero cualquiera M puede representarse por la primera forma de tal manera que los valores indeterminados sean primos entre sí, el mismo numero podrá ser representado por la otra forma de la misma manera y, claro esta, de manera que cada representación pertenezca al mismo valor de la expresión \J~D (mod. M). Si, no obstante, dos formas pertenecen a diferentes clases, ellas no seraán propiamente equivalentes; y si un nuámero dado es representado por una de las formas, nada puede decirse con respecto a si este es representable por la otra. Por otro lado, si el námero M puede ser representado por una de estas de tal manera que los valores de los indeterminados sean primos entre sí, podemos estar seguros inmediatamente que no existe representacioán similar del mismo nuámero por otra forma que pertenezca al mismo valor de la expresion \[D (mod. M) (veanse arts. 167, 168).

Puede suceder, sin embargo, que dos formas F y F' que provienen de clases diferentes, K y K', sean impropiamente equivalentes, en este caso toda forma de una de las clases sera impropiamente equivalente a todas las formas de la otra clase. Toda forma de K poseerá una forma opuesta en K' y las clases se llamarán opuestas. Así, en el primer ejemplo del articulo precedente, la tercera clase de formas con determinante -235 es opuesta a la cuarta, la setima a la octava; en el segundo ejemplo, la segunda clase es opuesta a la tercera y la quinta a la sexta. Por esto, dadas dos formas cualesquiera de dos clases opuestas, cualquier nuámero M que pueda representarse por una, tambien puede ser representado por la otra. Si en una esto sucede por valores primos entre sí de las indeterminadas, esto podra suceder tambien en la otra pero de tal manera que estas dos representaciones correspondan a valores opuestos de la expresion \J~D (mod. M). Ademas, las reglas dadas arriba para la eleccián de formas representantes estan fundadas de modo que clases opuestas siempre dan origen a formas representantes opuestas.

Finalmente, existen clases que son opuestas a si mismas. A saber, si alguna forma y su opuesta están contenidas en la misma clase, es fácil ver que todas las formas de esta clase son tanto propia como impropiamente equivalentes a alguna otra y que ellas tendrán todas sus opuestas en la clase. Cualquier clase tendrá esta propiedad si contiene una forma ambigua y, recáprocamente, una forma ambigua se encuentra en cualquier clase que es opuesta a sí misma (art. 163, 165). Por esto le llamaremos clase ambigua. Así, entre las clases con determinante -235 se encuentran ocho clases ambiguas. Sus formas representantes son (1, 0, 235), (2, 1, 118), (5, 0,47), (10, 5, 26), (-1,0, -235), (-2,1,-118), (-5, 0, -47), (-10, 5,-26); entre las clases de formas con determinante 79 se encuentran dos con representantes: (1, 0,-79) y (—1, 0, 79). Pero si las formas representadas han sido determinadas de acuerdo con nuestras reglas, las clases ambiguas se pueden determinar a partir de ellas sin ningún problema. Esto es, para un determinante positivo no cuadrado una clase ambigua ciertamente corresponde a una forma representante ambigua (art. 194); para un determinante negativo la forma representante de una clase ambigua será ella misma ambigua o bien sus terminos exteriores serán iguales (art. 172); finalmente, para un determinante positivo cuadrado, por el artículo 210 es fácil deducir si la forma representante es impropiamente equivalente a sí misma y así si la clase a la cual representa es ambigua.

225.

Nosotros demostramos arriba (art. 175) que para una forma (a, b, c) con determinante negativo los terminos exteriores deben poseer el mismo signo y que este será el mismo signo que el de los terminos exteriores de cualquier otra forma equivalente a esta. Si a y c son positivos, podremos llamar positiva a la forma (a,b,c), y diremos que la clase entera en la cual (a,b,c) esta contenida, y la cual esta compuesta solo por formas positivas, es una clase positiva. Al contrario (a,b,c) sera una forma negativa contenida en una clase negativa si a y c son negativos. Un numero negativo no puede representarse por una forma positiva, ni un numero positivo lo puede ser por una forma negativa. Si (a, b, c) es la forma representante de una clase positiva, (-a, b, —c) sera la forma representante de una clase negativa. Así se sigue que el numero de clases positivas es igual al numero de clases negativas, y tan pronto como conozcamos una conoceremos la otra. Por lo tanto, al investigar formas con determinante negativo es muy a menudo suficiente considerar clases positivas, ya que sus propiedades pueden ser facilmente transferidas a clases negativas.

Pero esta distincion se cumple solo para formas con determinante negativo; námeros positivos y negativos pueden representarse igualmente por formas con determinante positivo, así no es raro encontrar en este caso las dos formas (a, b, c) y (—a, b, —c) en la misma clase.

Distribución de clases en órdenes.

226.

Llamamos primitiva a la forma (a, b, c) si los numeros a, b, c no poseen divisores en común; en otro caso la llamaremos derivada y, claro esta, si el maximo

común divisor de a, b, c es igual a m, la forma (a, b, c) será la forma derivada de la forma primitiva (—, —, —). A partir de esta definiciún es obvio que cualquier forma cuyo determinante no es divisible por ningún cuadrado (excepto 1) es necesariamente primitiva. Ademas, por el artículo 161, si tenemos una forma primitiva en una clase arbitraria dada de formas con determinante D, todas las formas de esa clase serán primitivas; en este caso se dice que la clase misma es primitiva. Y es claro que, si cualquier forma F con determinante D se deriva de una forma primitiva f con determinante m2, y si las clases en las cuales las formas F y f respectivamente esrán contenidas son K y k, todas las formas de la clase K serán formas derivadas de la clase primitiva k; en este caso diremos que la clase K es asimismo derivada de la clase primitiva k.

Si (a, b, c) es una forma primitiva y a y c no son ambos pares (i.e. o uno es impar o bien ambos son impares), entonces evidentemente no solo a, b y c sino tambien a, 2b y c no poseen divisores comunes. En este caso la forma (a, b, c) se dice propiamente primitiva o simplemente una forma propia. Pero si (a, b, c) es una forma primitiva y los números a y c son ambos pares, obviamente los números a, 2b y c tendrán el divisor común 2 (este sera tambien el maximo divisor) y (a, b, c) se llamará una forma impropiamente primitiva o simplemente una forma impropia[[168]](#footnote-169)). En este caso b sera necesariamente impar (en otro caso (a,b,c) no sería una forma primitiva); por lo tanto tendremos b2 ξ 1 (mod. 4) y, como ac es divisible por 4, el determinante b2 — ac ξ 1 (mod. 4). Por lo que formas impropias corresponderán solamente a determinantes de la forma 4n + 1 si son positivos o de la forma — (4n+3) si son negativos. A partir del artúculo 161 es obvio que si encontramos una forma propiamente primitiva en una clase dada, todas las formas de esta clase serúan propiamente primitivas y que una clase que incluya una forma impropiamente primitiva estarúa compuesta solamente por formas impropiamente primitivas. Por ende, en el primer caso la clase se llamarúa propiamente primitiva o simplemente propia; y en el último caso impropiamente primitiva o impropia. Asú, p. ej., entre las clases positivas de formas con determinante —235 existen seis propias con formas representantes (1, 0, 235), (4,1, 59), (4, —1,59), (5, 0,47), (13, 5, 20) y (13, —5, 20) y el mismo número de negativas; y se encuentran dos clases impropias en cada una. Todas las clases de formas con determinante 79 (dado que ellas son de la forma 4n+3) son propias.

Si la forma (a, b, c) se deriva de la forma primitiva (ff, ^, mC) esta última puede ser o propiamente o bien impropiamente primitiva. En el primer caso m sera tambien el máximo común divisor de los números a, 2b, c; en el último el maximo común divisor será 2m. A partir de esto podemos hacer una clara distinción entre una forma derivada de una forma propiamente primitiva y una forma derivada de una forma impropiamente primitiva; y ademas (ya que por el art. 161 todas las formas de una misma clase son las mismas en ese sentido) entre una clase derivada de una clase propiamente primitiva y una clase derivada de una clase impropiamente primitiva.

Por medio de estas distinciones hemos obtenido el primer principio funda­mental sobre el cual podemos construir la nocion de distribucion de todas las clases de formas con un determinante dado en varios órdenes. Dadas dos representaciones (a,b,c) y (a',b',c'), las agruparemos en el mismo orden siempre que los números a, b y c tengan el mismo maximo común divisor que a', b' y c', y, a, 2b y c posean el mismo maximo común divisor que a', 2b' y c'; si una u otra de esas condiciones falla, las clases serún asignadas a órdenes diferentes. Es claro de inmediato que todas las clases propiamente primitivas constituiraún un orden; y todas las clases impropia­mente primitivas otro. Si m2 es un cuadrado que divide al determinante D, las clases derivadas de las clases propiamente primitivas del determinante ^“2 formarún un orden especial, y las clases derivadas de clases impropiamente primitivas del deter­minante ^“2 formarún otro, etc. Si D es divisible por un no cuadrado (excepto 1), no habrá úrdenes de clases derivadas, y así habrá o solamente un orden (cuando D ξ 2 o 3 según modulo 4) que es un orden de clases propiamente primitivas, o dos ordenes (cuando D ξ 1 (mod. 4)), esto es, un orden de clases propiamente primitivas y un orden de clases impropiamente primitivas. No es difícil establecer la siguiente regla general con la ayuda de los principios del cúalculo de combinaciones. Suponemos que D = D'22^a2ab2/3c2y ... donde D' denota un factor no cuadrado y a, b, c, etc. son diferentes números primos impares (cualquier número puede reducirse a esta forma tomando μ = 0 cuando D no es divisible por 4; y cuando D no es divisible por un cuadrado impar tomamos α, β, γ, etc. iguales a 0 o, lo que es la misma cosa, omitimos los factores a2a, b2^, c2y, etc.) ; así habrá o

(μ +1)(α + 1)(β + 1)(γ + 1)...

ordenes cuando D' ξ 2 ú 3 (mod. 4); o

(μ +2)(α +1)(β + 1)(γ +1)...

órdenes cuando D' = 1 (mod. 4). Pero no demostraremos esta regla, dado que no es difícil ni es necesaria aquí.

Ejemplo. 1. Para D = 45 = 5 · 32 tenemos seis clases con representantes (1, 0, -45), (-1, 0,45), (2,1,-22), (-2,1, 22), (3, 0,-15), (6, 3, -6). Estas se

distribuyen en cuatro ordenes. El orden I incluye dos clases propias cuyas representantes son (1,0, 45) y (-1, 0,45); el orden II contendrá dos clases impropias cuyas representantes son (2, 1,-22) y (-2, 1, 22); el orden III contendrá una clase derivada de la clase propia del determinante 5, con representante (3, 0, -15); el orden IV estará conformado por una clase derivada de una clase impropia del determinante 5 con representante (6, 3, -6).

Ejemplo. 2. Las clases positivas del determinante -99 = -11 · 3 se distribuirá en cuatro ordenes: el orden I incluirá las siguientes clases propiamente primitivas:[[169]](#footnote-170)) (1, 0, 99), (4,1, 25), (4,-1, 25), (5,1, 20), (5,-1, 20), (9, 0,11); el orden II contendrá las clases impropias (2, 1, 50), (10, 1, 10); el orden III contendrá las clases derivadas de las clases propias del determinante -11, a saber (3,0,33), (9,3,12), (9, -3, 12); el orden IV, la clase derivada de las clases impropias del determinante -11, i.e., (6, 3,18). Clases negativas de este determinante pueden distribuirse en ordenes de exactamente la misma manera.

Observaremos que clases opuestas son siempre asignadas al mismo orden.

227.

De todos estos diferentes ordenes el orden de las clases propiamente primitivas merece especial atencioán. Para cada clase derivada obtenemos su origen de ciertas clases primitivas (con un determinante mínimo) y, considerando estas, las propiedades de las clases se harán claras de inmediato. Mostraremos despues que cualquier clase impropiamente primitiva se asocia o con una clase propiamente primitiva o con tres (con el mismo determinante). Ademas, para determinantes negativos, se puede omitir la consideraciáon de clases negativas, dado que ellas siempre corresponderáan a ciertas clases positivas. A fin de entender mas plenamente la naturaleza de las clases propiamente primitivas, debemos primero explicar una cierta diferencia esencial seguán la cual el orden completo de clases propias puede subdividirse en varios géneros. Dado que todavía no hemos alcanzado este muy importante tema, lo trataremos desde el principio.

La partición de ordenes en géneros.

228.

TEOREMA. Existe una infinidad de numeros no divisibles por un numero primo p dado, que pueden representarse por una forma propiamente primitiva.

Demostracion. Si la forma F = ax2 + 2bxy + cy2, es claro que p no puede ser divisor de los tres numeros a, 2b, c. Ahora si a no es divisible por p, es claro que si elegimos un numero no divisible por p para x , y para y un número que sea divisible por p, el valor de la forma F no sera divisible por p; cuando c no es divisible por p ocurrirú lo mismo si damos a x un valor divisible por p ya y un valor que no sea divisible por p; finalmente, cuando ambos a y c son divisibles por p, y 2b no lo es, la forma F tendrá un valor no divisible por p si damos a ambos x y y valores que no sean divisibles por p. Q. E. D.

Es obvio que el teorema tambien es valido para formas que sean impropiamente primitivas mientras que no se tenga p = 2.

Dado que muchas condiciones de este tipo se pueden dar simultúneamente, tal como que el mismo numero es divisible por ciertos numeros primos pero no por otros (vease art. 32), es fúcil notar que los numeros x e y se pueden determinar de infinitas maneras, resultando que la forma primitiva ax2 + 2bxy + cy2 adquiera un valor que no es divisible por cualquier cantidad de numeros primos, excluyendo, sin embargo, el número 2 cuando la forma sea impropiamente primitiva. Así podemos proponer el teorema mas generalmente: Siempre se puede representar por medio de cualquier forma primitiva una infinidad de números que sean primos relativos a un número dado (el cual es impar cuando la forma es impropiamente primitiva). [[170]](#footnote-171) y mm' será congruente a un cuadrado según el modulo D y así también según p; i.e., mm' sera un residuo cuadrútico de p. Se sigue por lo tanto que ambos m y m' son residuos cuadráticos de p, o que ambos no lo son. Q. E. D.

De la misma manera podemos demostrar que cuando el determinante D es divisible por 4, todos los numeros primos representables por F son o congruentes a 1 o congruentes a 3 (mod. 4). Esto es, el producto de dos de esos números siempre sera un residuo cuadrático de 4 y por ende congruente a 1 (mod. 4); así ambos deben ser congruentes a 1 o ambos a 3.

Finalmente, cuando D es divisible por 8, el producto de dos números impares cualesquiera que pueden representarse por F sera un residuo cuadratico de 8 y por tanto congruente a 1 (mod. 8). Así, en este caso los números impares representables por F serún todos congruentes a 1, o todos congruentes a 3, o todos congruentes a 5, o todos congruentes a 7 (mod. 8).

De este modo, p. ej., ya que el número 10 que es un no residuo de 7 se puede representar por la forma (10, 3, 17), todos los números no divisibles por 7 que se pueden representar por esa forma serán no residuos de 7. Como —3 es representable por la forma (—3, 1, 49) y es congruente a 1 (mod. 4), todos los números impares representables por esta forma serán congruentes a 1 (mod. 4).

Si fuese necesario para nuestros propósitos, podríamos demostrar facilmente que los nuúmeros representables por la forma F no guardan tal relacioún con nuúmeros primos que no dividan a D. Ambos residuos y no residuos de un nuúmero primo que no divide a D se pueden representar igualmente por la forma F. Por el contrario, con respecto a los numeros 4 y 8 existe una cierta analogía, en otros casos tambien, que no podemos atrasar.

1. Cuando el determinante D de la forma primitiva F es congruente a 3 (mod. 4), todos los números impares representables por la forma F seran congruentes a 1 o todos congruentes a 3 (mod. 4). En efecto, si m y m' son dos números representables por F, el producto mm' podrú reducirse a la forma p2 — Dq2 tal y como hicimos arriba. Cuando cada uno de los números m y m' es impar, uno de los nuúmeros p o q es necesariamente par, y el otro impar, y por ende uno de los cuadrados p2 o q2 serú congruente a 0 y el otro a 1 (mod. 4). Asú p2 — Dq2 debe ser ciertamente congruente a 1 (mod. 4), y ambos m y m' deben ser congruentes a
2. o a 3 (mod. 4). Luego, p. ej., ningun número impar, mas que aquellos de la forma 4n + 1, puede representarse por la forma (10, 3,17).
3. Cuando el determinante D de la forma primitiva F es congruente a
4. (mod. 8): todos los números impares representables por la forma F seran o congruentes en parte a 1 *y en parte a 7, o bien en parte a* 3 *y en parte a* 5 (mod. 8). En efecto, supongamos que m y m' son dos números impares representables por F cuyo producto mm' puede reducirse a la forma p2 — Dq2. Por lo que cuando ambos m y m' son impares, p debe ser impar (porque D es par) y así p2 ξ 1 (mod. 8); q2 por lo tanto será congruente a 0, 1 o 4 y Dq2 a 0 o a 2. Así mm' = p2 — Dq2 sera congruente a 1 o a 7 (mod. 8); por eso, si m es congruente a 1 o a 7, m' será tambien congruente a 1 o a 7; y si m es congruente a 3 o a 5, m' sera tambien congruente a 3 o a 5. Por ejemplo, todos los námeros impares representables por la forma (3, 1,5) son congruentes a 3 o a 5 (mod. 8), y ningán námero de la forma 8n + 1 u 8n + 7 puede representarse por esta forma.
5. Cuando el determinante D de una forma primitiva F es congruente a 6 (mod. 8): los números impares que pueden representarse por esta forma son o todos congruentes a 1 ya 3, o todos congruentes a 5 ya 7 (mod. 8). El lector puede desarrollar el argumento sin ningán problema. Es exactamente como el argumento anterior (II). Así, p. ej., para la forma (5, 1, 7), solamente aquellos numeros impares que son congruentes a 5 o a 7 (mod. 8) pueden representarse.

230.

Por lo tanto todos los námeros que pueden representarse por una forma primitiva F dada con determinante D guardaran una estrecha relación con cada uno de los divisores primos de D (por el cual ellos no son divisibles). Y námeros impares que pueden representarse por la forma F guardaran tambien una estrecha relación con los numeros 4 y 8 en ciertos casos: a saber, con 4 siempre que D sea congruente a 0 o a 3 (mod. 4) y con 8 siempre que D sea congruente a 0, a 2 o a 6 (mod. 8)[[171]](#footnote-172)). Llamaremos a este tipo de relacion con cada uno de estos námeros el caracter o el caracter particular de la forma F, y expresaremos este de la siguiente manera. Cuando solamente residuos cuadraticos de un numero primo p pueden representarse por la forma F, asignaremos a ella el carácter Rp, en caso contrario asignaremos el caracter Np; similarmente escribiremos 1, 4 cuando ningán otro námero puede representarse por la forma F excepto aquellos que son congruentes a 1 (mod. 4). Es claro de inmediato cuaáles caracteres se denotan por 3, 4; 1, 8; 3, 8; 5, 8 y 7, 8. Finalmente, si tenemos formas a traves de las cuales solamente pueden representarse aquellos námeros impares que son congruentes a 1 o a 7 (mod. 8), les asignaremos a

ellos el carácter 1 y 7,8. Es obvio de inmediato que representamos por los caracteres 3 y 5, 8; 1 y 3, 8 ; 5 y 7, 8.

Los diferentes caracteres de una forma primitiva dada (a, b, c) con determi­nante D siempre se pueden conocer a partir de al menos uno de los numeros a o c (partiendo de que ambos son representables por tal forma). En efecto, siempre y cuando p sea un divisor primo de D, ciertamente uno de los námeros a o c, no sera di­visible por p; pues si ambos fueran divisibles por p, p dividiría tambien a b2 (= D + ac) y por lo tanto tambien a b; i.e. la forma (a, b, c) no sería primitiva. Similarmente, en aquellos casos en que la forma (a, b, c) posee una relación fija con el námero 4 o el 8, al menos uno de los námeros a o c sera impar, y podra conocerse la relacion de ese námero. Así, p. ej., el carácter de la forma (7, 0, 23) con respecto al námero 23 puede inferirse a partir del námero 7 como N23, y el carácter de la misma forma con respecto al numero 7 puede deducirse a partir del námero 23, a saber R7; finalmente, el carácter de esta forma con respecto al námero 4, a saber 3, 4, puede hallarse a partir del numero 7 o a partir del námero 23.

Dado que todos los námeros que pueden representarse por una forma F contenida en una clase K son tambien representables por cualquier otra forma de la clase, queda manifiesto que los diferentes caracteres de la forma F se aplicaráan a todas las demáas formas de esta clase y por ende podemos considerar estos caracteres como representativos de toda la clase. Los caracteres individuales de una clase primitiva dada pueden entonces conocerse a partir de sus formas representantes. Clases opuestas poseerán siempre los mismos caracteres. [[172]](#footnote-173)

p. ej., para el determinante -161 tenemos 16 clases positivas propiamente primitivas que estan distribuidas en 4 generos de la siguiente manera:

Formas representantes de las clases  
(1, 0,161), (2,1, 81), (9,1,18), (9,-1,18)

Carácter 1, 4; R7; R23 1, 4; N7; N23 3, 4; R7; N23 3, 4; N7; R23

(5, 2, 33), (5, -2, 33), (10, 3,17), (10, -3,17) (7, 0, 23), (11, 2,15), (11, -2,15), (14, 7,15) (3,1, 54), (3,-1, 54), (6,1, 27), (6,-1, 27).

Se puede decir unas cuantas palabras con respecto a la cantidad de diferentes caracteres completos que son posibles a priori.

1. Cuando el determinante D es divisible por 8, con respecto al numero 8 cuatro caracteres particulares son posibles; el námero 4 no aportara ningán carácter en especial (vease el artículo precedente). Ademas, con respecto a cada divisor primo impar de D existirán dos caracteres; por lo tanto, si hay m de esos divisores, existirán en total 2m+2 diferentes caracteres completos (siendo m = 0 siempre que D sea potencia de 2).
2. Cuando el determinante D no es divisible por 8 pero sá es divisible por 4 y por m námeros primos impares, habrá en total 2m+ caracteres completos diferentes.
3. Cuando el determinante es par y no divisible por 4, este seráa congruente a 2 o a 6 (mod. 8). En el primer caso existirán dos caracteres particulares con respecto al námero 8, a saber 1 y 7, 8 y 3 y 5, 8; y el mismo numero en el ultimo caso. Por lo tanto, tomando el námero de divisores primos impares de D igual a m, habrá en total 2m+1 caracteres completos diferentes.
4. Cuando D es impar, sera congruente a 1 o a 3 (mod. 4). En el segundo caso existirán dos diferentes caracteres con respecto al námero 4, pero en el primer caso esta relación no formara parte del carácter completo. Así si definimos m como antes, en el primer caso existirán 2m diferentes caracteres completos, en el ultimo caso 2m+1.

Pero hay que señalar bien que no se sigue a priori que siempre existirán tantos generos como diferentes posibles caracteres. En nuestro ejemplo el námero de clases o generos es solamente la mitad de la cantidad posible. No existen clases positivas para los caracteres 1, 4; R7; N23 o 1, 4; N7; R23 o 3, 4; R7; R23 o 3, 4; N7; N23.

Trataremos este importante tema plenamente mas abajo.

A partir de ahora llamaremos a la forma (1,0, -D), que es indudablemente la mas simple de las formas con determinante D, la forma principal; y llamaremos a la clase completa en la cual esta se encuentra la clase principal; y finalmente el genero

completo en el cual se encuentra la clase principal se llamará el género principal. Por lo tanto, hay que distinguir claramente entre la forma principal, una forma de la clase principal, y una forma del genero principal; y entre la clase principal y una clase del genero principal. Siempre usaremos esta terminología, aún cuando quizas para un determinante en particular no exista otra clase mús que la clase principal o ningun otro genero mas que el genero principal. Esto sucede muy a menudo, p. ej., cuando D es un número primo positivo de la forma 4n +1.

232.

Aún cuando todo lo que se ha explicado sobre los caracteres de las formas fue con el propúsito de encontrar una subdivision para todo el orden de clases positivas propiamente primitivas, nada nos impide ir mas lejos. Podemos aplicar las mismas reglas a formas y clases negativas o impropriamente primitivas, y bajo el mismo principio podemos subdividir en gúeneros tanto un orden positivo impropiamente primitivo, como un orden negativo propiamente primitivo, como un orden negativo impropiamente primitivo. Así pues, por ejemplo, despues de que se ha subdividido el orden propiamente primitivo de formas de determinante 145 en los dos siguientes generos:

R5, R29 (1,0,-145),(5,0, -29)

N5, N29 (3,1, -48),(3 - 1, -48)

el orden impropiamente primitivo puede tambien ser subdividido en dos generos:

R5, R29 (4,1, -36), (4, -1, -36)

N5, N29 (2,1, -72),(10, 5,-12)

o, tal como las clases positivas de las formas de determinante -129 se distribuyen en cuatro gúeneros:

(1,0,129), (10,1,13), (10,-1,13) (2,1,65), (5,1, 26), (5,-1, 26)

1, 4; R3; R43 1, 4; N3; N43 3, 4; R3; N43 3, 4; N3; R43

(3,0,43), (7, 2,19), (7,-2,19)

(6,3, 23), (11, 5,14), (11, -5,14)

las clases negativas también se pueden distribuir en cuatro órdenes:

(-1, 0,-129), (-10,1,-13), (-10,-1,-13) (-2,1, -65), (-5,1, -26), (-5,-1,-26) (-3, 0, -43), (-7, 2,-19), (-7,-2,-19) (-6, 3,-23), (-11, 5,-14), (-11, -5,-14)

3, 4; N3; N43 3, 4; R3; R43 1, 4; N3; R43 1, 4; R3; N43

Sin embargo, puesto que el sistema de clases negativas es siempre muy similar al sistema de clases positivas, resulta superfluo construirlo por aparte. Mostraremos luego como reducir un orden impropiamente primitivo a uno propiamente primitivo.

Finalmente, en cuanto a la subdivision de ordenes obtenidos a partir de otros, no son necesarias reglas nuevas. Es así puesto que cualquiera de estos órdenes tiene origen en algón orden primitivo (con un determinante menor), y las clases de uno pueden relacionarse de manera natural con las clases del otro, y entonces es claro que la subdivision de una de estas formas puede obtenerse a partir de la subdivisión de un orden primitivo.

233.

Si la forma (primitiva) F = (a, 6, c) es tal que se puede encontrar dos enteros g y h, tales que g2 ξ a, gh ξ 6, h2 ξ c con respecto a un modulo dado m, diremos que la forma es un residuo cuadratico del nómero m, y que gx + hy es un valor de la expresión yjax2 + 26xy + cy2 (mod. m) o simplemente que (g, h) es un valor de la expresion yj(a, 6, c) o \/F (mod. m). De manera mas general, si el multiplicador M, primo relativo al modulo m es tal que tenemos

g2 ξ aM, gh ξ 6M, h2 ξ cM (mod. m)

diremos que M · (a, 6, c) o MF es un residuo cuadratico de m y que (g, h) es el valor de la expresión \JM(a, 6, c) o VMF (mod. m). Por ejemplo, la forma (3, 1, 54) es

un residuo cuadratico de 23 y (7, 10) un valor de la expresión yj(3, 1, 54) (mod. 23);

similarmente (2, -4) es un valor de la expresion ^5(10, 3,17) (mod. 23). El uso de estas definiciones se demostraró despues. Anotaremos las siguientes proposiciones:

1. Si M(a, 6, c) es un residuo cuadratico del número m, m sera un divisor del determinante de la forma (a, 6, c). Pues si (g,h) es un valor de la expresión M(a, 6, c) (mod. m) es decir, si

g2 ξ aM, gh ξ 6M, h2 ξ cM (mod. m)

tendremos b2M2 — acM2 ξ 0 o sea (b2 — ac)M2 es divisible por m. Pero, puesto que hemos supuesto que M y m son primos relativos, b2 — ac sera divisible por m.

1. Si M(a, b, c) es un residuo cuadrático de m, donde m es un numero primo o una potencia ρμ de un námero primo, el carácter particular de la forma (a, b, c) con respecto al numero p sera Rp o Np segán M sea un residuo o no residuo de p. Esto se sigue inmediatamente del hecho de que ambos aM y cM son residuos de m o p, y que al menos uno de los námeros a y c no es divisible por p (art. 230).

Similarmente, si (con todo lo demás igual) m = 4, entonces 1, 4 o 3, 4 será un carácter particular de la forma (a, b, c) segán M ξ 1 á M ξ 3; y si m = 8o una potencia mayor del número 2, entonces, 1, 8; 3, 8; 5, 8; 7, 8 serán caracteres particulares de la forma (a, b, c) segun M ξ 1; 3; 5; 7 (mod. 8) respectivamente.

1. En cambio, suponga que m es un námero primo o una potencia p^ de un námero primo impar y que es divisor del determinante b2 — ac. Si M es un residuo o no de p segán el carácter de la forma (a, b, c) respecto a p sea Rp o Np respectivamente, entonces M(a, b, c) sera un residuo cuadrático de m. Pues cuando a no es divisible por p, aM sera un residuo de p y así tambien de m; por lo tanto, si g es un valor de la expresión VaM (mod. m), h un valor de la expresián (mod. m), tendremos g2 ξ aM, ah ξ bg. Entonces

agh ξ bg2 ξ abM y gh ξ bM

y finalmente

ah2 ξ bgh ξ b2M ξ b2M — (b2 — ac)M ξ acM

Así h2 ξ cM; i.e. (g, h) es un valor de la expresion ^M(a, b, c). Cuando a es divisible por m es de seguro que c no lo sera. Entonces obviamente obtendremos el mismo resultado si h asume un valor de la expresion VcM (mod. m) y g un valor de la expresion ^ (mod. m).

De manera similar se puede mostrar que si m = 4 y es divisor de b2 — ac, y si el námero M se toma ξ 1o ξ 3 segun 1, 4 o 3, 4 sea un carácter particular de la forma (a, b,c), entonces, M(a, b, c) sera un residuo cuadrático de m. Ademas, si m = 8 o una potencia mayor de 2 y divisor de b2 — ac, y si M ξ 1; 3; 5; 7 (mod. 8) segun el carácter particular de la forma (a, b, c) respecto al numero 8; entonces M(a, b, c) sera un residuo cuadratico de m.

1. Si el determinante de la forma (a, b, c) es = D y M(a, b, c) es un residuo cuadrático de D, a partir del numero M pueden conocerse inmediatamente todos los caracteres particulares de la forma (a, b, c) respecto a cada uno de los divisores primos impares de D y respecto al número 4 u 8 (si dividen a D). Entonces, por ejemplo, puesto que 3(20, 10, 27) es un residuo cuadrútico de 440, es decir, que (150, 9) es un valor de la expresión ^3(20,10, 27) respecto al modulo 440 y 3N5, 3R11, los caracteres de la forma (20, 10, 27) son 3, 8; N5; R11. Los caracteres particulares con respecto a los nuúmeros 4 y 8, siempre que no sean divisores del determinante, son los únicos que no tienen una conexiún necesaria con el número M.
2. En cambio, si el número M es primo relativo a D y contiene todos los caracteres particulares de la forma (a, b, c) (excepto por aquellos respecto a los números 4 y 8 cuando no son divisores de D), entonces M(a,b,c) sera un residuo cuadratico de D. Pues, a partir de III es claro que si D se reduce a la forma ±AaBeC ... donde A, B, C, etc. son numeros primos distintos, M(a,b,c) sera un residuo cuadrútico de cada uno de los Aa, Be, Cγ, etc. Ahora supongamos que el valor de la expresion yj M (a, b, c) respecto al modulo Aa es (A, A0); respecto al modulo Bβ es (B, B0); respecto al modulo CY es (C, C0) etc. Si los números g y h se determinan tales que g = A, B, C etc; h = A0, B0, C0 etc. respecto a los módulos Aa, Be, CY, etc. respectivamente (art. 32): es fúcil ver que tendremos g2 = aM, gh = bM, h2 = cM respecto a cada uno de los modulos Aa, Be, Cγ, etc. y, por lo tanto, tambiúen respecto al múodulo D, que es su producto.
3. Por esta razon números como M se llamaran números característicos de la forma (a,b,c). Muchos de estos números pueden encontrarse facilmente mediante los múetodos de V, una vez que se conocen todos los caracteres particulares de la forma. Los mús sencillos se encontraran por tanteo. Claramente, si M es un número característico de una forma primitiva de determinante D dado, todos los números congruentes a M respecto al modulo D serún números característicos de la misma forma. Tambien es claro que formas de la misma clase o de diferentes clases del mismo genero tienen los mismos números característicos. Como consecuencia, cualquier número característico de una forma dada tambien se puede asignar a toda la clase y a todo el genero. Finalmente, 1 es siempre un número característico de cualquier forma, clase o gúenero principal; es decir, toda forma de un gúenero principal es un residuo de su determinante.
4. Si (g, h) es un valor de la expresion -y/M (a, b, c) (mod. m) y g0 = g y h0 = h (mod. m), entonces (g0,h0) tambien sera un valor de la misma expresion. Tales valores se denominaran equivalentes. Sin embargo, si (g, h) y (g0,h0) son valores de la expresion M(a, b, c), pero no se cumple que g0 = g, h0 = h (mod. m), se denominarán diferentes. Es claro que siempre que (g, h) sea un valor de una expresiún como la anterior, (—g, —h) tambien sera un valor, y estos valores

siempre serán diferentes excepto cuando m = 2. También es fácil mostrar que una expresión -y/M(a, b, c) (mod. m) no puede tener más que dos valores diferentes opuestos cuando m es un námero primo impar, una potencia de un námero primo impar o = 4; sin embargo, cuando m = 8 o una potencia mayor de 2, habrá cuatro en total. Entonces, a partir de VI vemos facilmente que si el determinante D de la forma (a, b, c) es = ±2μΑαΒβ ... donde A, B, etc. son n námeros primos impares diferentes en total, y M es un námero característico de la forma; entonces habrá, en total, 2n á 2n+1 á 2n+2 valores diferentes de la expresion -y/M (a, b, c) (mod. D)

segun μ sea < 2 á = 2o > 2. Entonces, por ejemplo, hay 16 valores de la expresión yV(12, 6,-17) (mod. 240), a saber (±18, f11), (±18, ±29), (±18, f91), (±18, ±109), (±78, ±19), (±78, ±59), (±78, f61), (±78, =f101). Para abreviar, y puesto que no es particularmente importante para lo que sigue, omitiremos una demostracioán maás detallada.

1. Finalmente observamos que si el determinante de dos formas equiva­lentes (a, b, c) y (a',b',c') es D, el numero característico es M y la primera se puede transformar en la segunda mediante la sustitucián α, β, γ, δ; entonces, a partir de cualquier valor (g, h) de la expresión M(a,b,c) se obtiene un valor (g,h') de la

expresión \JM(a',V,d), a saber (ag + γh,βg + δΚ). El lector puede demostrar esto facilmente.

Sobre la composición de formas.

234.

Ahora que hemos explicado la distribucion de formas entre clases, generos y ordenes, y las propiedades generales que resultan de estas distinciones, pasaremos a otro tema muy importante, la composition de formas. Hasta el momento, nadie ha considerado este punto. Antes de iniciar la discusiáon enunciaremos el siguiente lema para no interrumpir, máas adelante, la continuidad de nuestra demostracioán.

LEMA: Suponga que tenemos cuatro series de enteros.

a, a', a'', ... an; b, b', b'', ...bn; c, c', c'', ... cn; d, d', d", ...cd

donde cada serie tiene el mismo numero (n +1) de términos y están ordenados tal

que

cd' — dcr , cd" — dc" etc., c'd'' — d'c'' etc., etc.

son respectivamente

= k(ab' — ba'), k(ab'' — ba") etc., k(a'b'' — b'a") etc., etc.

o en general

cxdA — *dxc!* = k(axbk — bxaμ)

Aquí k es un entero dado; λ y μ son dos enteros distintos cualesquiera entre 0 y n inclusive, con μ el mayor de los dos[[173]](#footnote-174)). Además, no debe haber un divisor común entre todos los axbμ — bxaμ. Bajo estas condiciones, se pueden encontrar cuatro enteros α, β, γ y δ tales que

aa + βb = c, aa' + βb' = é, aa" + βb" = é' etc.

Ya + δb = d, Ya' + δϋ = d', *γο!'* + *δb"* = *d"* etc.

o en general

*aav* + *β&* = *cv*, *Yav* + *δ&* = *dv*

y tenemos

*αδ — βγ* = *k*

Puesto que por hipótesis los números ab' — ba', ab" — ba", etc. a'b" — b'a''

etc. (el número de ellos serú = ^ (n + 1)n) no tienen un divisor común, podemos encontrar la misma cantidad de enteros (diferentes) tal que si multiplicamos el primer conjunto por el segundo respectivamente, la suma de los productos sera = 1 (art. 40). Designaremos estos multiplicadores por (0, 1), (0, 2) etc., (1, 2) etc. o en general el multiplicador de axbμ — bxaμ por (λ, μ) y

χ(λ, μ)^1 — bxa1) = 1

(Mediante la letra Σ indicamos la suma de todos los valores de la expresiún cuando le damos sucesivamente a λ ya μ, todos los valores diferentes entre 0 y n y tal que μ > λ). Ahora si se pone

X (λ,μ)(^μ — bxcA) = a, X (λ,μ)^/::1 — cxaμ) = β X (λ, μ)(dxb1 — bxdμ) = γ, X (λ, μ)(axdμ — dxaμ) = δ

estos números α, β, γ y δ tienen las propiedades deseadas.

Demostración. I. Si ν es cualquier entero entre 0 y n, tenemos

ααν + βόν = X (λ, μ)(βλ6μαν - + axd1bv - cVbv)

= 1 Σ (λ,μ)(ο^μον - dVcv)

= 1 Σ (λ, μ)(cλdμ - dλcμ)

= cv Σ (λ, μ)(αν - bV) = cv

Y mediante un cálculo similar se demuestra

γαν + δbν = dv. Q. E. P.

1. Entonces, puesto que

ολ = ααλ + βbλ, αμ = ααμ + βbμ

se tiene

νμ - bV = α(α^μ - bV)

y similarmente

αλομ - cV = β(αλbμ - bλaμ) dV - bλdμ = γ(α^μ - bV) aλdμ - dV = δ(α^μ - bλaμ)

A partir de estas fármulas pueden obtenerse los valores de α, β, γ y δ mucho mas facilmente, siempre y cuando λ y μ sean escogidos tales que α^μ - bλαμ no sea 0. Esto de seguro se puede lograr, ya que por hipótesis no hay un divisor comán de todos los αλbμ - bλaμ y por lo tanto todos no pueden ser 0. A partir de estas mismas ecuaciones, si multiplicamos la primera por la cuarta, la segunda por la tercera y restamos, obtenemos

(αδ - βγ)(αν - bλαμ)2 = (α^μ - bV)(cV - dV) = - bλαμ)2

y necesariamente entonces

αδ - βγ = k. Q. E. S.

235.

Si la forma AX2 + 2BXY + CY2 ...F se transforma en el producto de dos

formas

ax2 + 2bxy + cy2 ...f, y a'x'2 + 2b'x'y' + c'y'2 ...f mediante la sustitución

X = pxx + p xy + p yx + p yy Y = qxx + q xy + q yx + q yy

(para abreviar, en lo que sigue expresaremos esta situación de la siguiente manera: Si F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q'''[[174]](#footnote-175))), diremos simplemente que la forma F es transformable en ff'. Si ademós se construye esta transformacióon de tal manera que los seis nuómeros

*pq - qp ,*

*pq*

// ///

*qp ,pq*

/// / //

*qp ,p q*

/ // / ///

*q p ,p q*

/ /// // ///

*q p ,p q*

// ///

*q p*

no tienen un divisor comón, llamaremos a F una forma compuesta de las formas f y f .

Iniciaremos esta discusión con la suposición mas general de que la forma F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q''' y descubriremos que es lo que deducimos de esto. Claramente las nueve ecuaciones siguientes son completamente equivalentes a esta suposición (i.e. cuando estas ecuaciones se cumplen F seró transformada, mediante las sustituciones dadas, en ff', y vice-versa):

Ap2 + 2Bpq + Ccq2 = aa [1]

Ap 2 + 2Bp q + Cq 2 = ac [2]

*Ap*''2 + *2Bp"q"* + Cq'2 = ca [3]

*Api''2* + *2Bp"'q"'* + *CeT2* = *cC* [4]

App' + B(pq' + qp') + Cqq' = ab' [5]

App" + B(pq" + qp'') + Cqq'' = ba' [6]

App'' + B (p'q''' + q'p''') + Cq'q''' = bc' [7]

Ap''p''' + B (p'q"' + q'p'') + Cq''q''' = cb' [8]

A(pp'' + p'p'') + B(pq'' + qp''' + p'q'' + q'p'') + C (qq''' + q'q'') = 2bb' [9]

Sean D, d y d' los determinantes de las formas F, f y f' respectivamente; y sean M, m y m' los máximos comunes divisores de los números A, 2B, C; a, 2b, c; a!, 2b0, c0, respectivamente (suponemos que todos estos námeros son positivos). Ademas sean los seis enteros A, B, C, A', B', C' determinados de modo que

Aa + 2Bb + Cc = m, A'a' + 2B 'b' + Cc' = m'

Finalmente desígnense los námeros

/ / // // /// ///

pq — qp , pq — qp , pq — qp ,

/ //

pq

/ //

q p ,

/ ///

p q

/ ///

q p ,

// ///

p q

**// ///**

q p

por P, Q, R, S, T, U respectivamente y sea k su maximo comán divisor tomado positivamente. Ahora, haciendo

App''' + B (pq''' + qp''') + Cqq''' = bb' + Δ [10]

de la ecuacián [9] obtenemos

Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' — Δ [11]

A partir de esas once ecuaciones desarrollamos las siguientes\*):

DP2 = d'a2 [12]

DP (R — S) = 2d'ab [13]

DPU = d'ac — (Δ2 — dd') [14]

D(R — S)2 = 4d'b2 + 2(Δ2 — dd') [15]

D(R — S)U = 2d'bc [16]

DU2 = d'c2 [17]

DQ2 = da'2 [18]

DQ(R + S) = 2da'b' [19]

DQT = da'c' — (Δ2 — dd') [20]

D(R + S)2 = 4db'2 + 2(Δ2 — dd') [21]

D(R + S)T = 2db'c' [22]

DT2 = dc 2 [23]

\*) El origen de estas ecuaciones es como sigue: [12] de [5]2 — [1][2]; [13] de [5][9] — [1][7] — [2][6]; [14] de [10][11] — [6][7]; [15] de 2[5][8] + [10]2 + [11]2 — [1][4] — [2][3] — 2[6][7]; [16] de [8][9] — [3][7] — [4][6]; [17] de [8]2 — [3][4]. Podemos deducir las seis ecuaciones restantes por medio de los mismos esquemas, si reemplazamos las ecuaciones [3], [6], [8] por las ecuaciones [2], [5], [7] respectivamente y dejamos [1], [4], [9], [10], [11] tal como aparecen. Por ejemplo, la ecuación [18] viene de [6]2 — [1][3], etc.

Y a partir de ellas deducimos las dos siguientes:

0 = 2d'a2(Δ2 - dd')

0 = (Δ2 - dd')2 - 2d'ac(^2 - *dd')*

la primera a partir de las ecuaciones [12][15] - [13]2, la segunda a partir de las ecuaciones [14]2 - [12][17]; y es fácil notar que Δ2 - dd' = 0 tanto si a es igual a cero como si no lo es[[175]](#footnote-176)). Supongamos que se ha cancelado Δ2 - dd' de las ecuaciones [14], [15], [20] y [21].

Ahora

AP + B(R - S) + CU = mn'

A Q + B' (R + S) + C' T = m'n

(donde n y n' pueden ser fracciones siempre que mn' y m'n sean enteros). A partir de las ecuaciones [12]-[17] se deduce que

Dm2n'2 = d' (Aa + 2Bb + Cc)2 = d'm2 y de las ecuaciones [18]-[23]

Dm' 2n2 = d' (A a' + 2B' b' + C' c' )2 = dm'2

Tenemos entonces d = Dn2, d' = Dn'2 y a partir de esto obtenemos una

PRIMERA Conclusión: Los cocientes de los determinantes de las formas F, f y

f necesariamente son cuadrados; y una SEGUNDA: D siempre divide a los números

dm'2 y d'm2. Entonces es claro que D, d y d' tienen el mismo signo y que ninguna

forma puede transformarse en el producto ff' si su determinante es mayor que el

maximo comán divisor de dm'2 y d'm2.

Multiplicamos las ecuaciones [12], [13], [14] por A, B, C respectivamente y

similarmente a las ecuaciones [13L [15L [16] y [14L [16L [17] por los mismos nuámeros

2

y sumamos los tres productos. Divida la suma por Dmn', escribiendo Dn' en vez de d . Entonces se obtiene

P = an', R - S = 2bn , U = cn

De manera semejante, multiplicando las ecuaciones [18], [19], [20] y [19], [21], [22] y [20], [22], [23] por A0, B0 y C resulta

Q = a0n, R + S = 2b'n, T = c0n

A partir de esto obtenemos una TERCERA CONCLUSIÓN: Los números a, 2b, y c son proporcionales a los números P, R — S y U. Si la razón del primero al segundo se toma como 1a n0, n0 sera la *raúz* cuadrada de D; de la misma manera los números a', 2b' y c0 son proporcionales a los números Q, R + S y T y si tomamos la *razún* como 1a n, n serú la *raúz* cuadrada de D.

Ahora, las cantidades n y n0 pueden ser o raíces positivas o raíces negativas de D y D7, así haremos una distinción que puede parecer esteril a primera vista, pero su uso quedara claro en lo que sigue. Diremos que en la transformation de la forma F en ff0 la forma f se toma directamente cuando n es positivo e inversamente cuando n es negativo; de manera analoga f0 se toma directamente o inversamente de acuerdo con que n0 sea positivo o negativo. Dada la condición de que k sea igual a 1, se dice que la forma F esta compuesta de las dos formas f y f0 directamente o de las dos inversamente o de f directamente y de f0 inversamente o de f inversamente y de f directamente segón que n y n0 sean ambos positivos o ambos negativos o que el primero sea positivo y el segundo negativo o el primero negativo y el segundo positivo. Es fócil notar que estas relaciones no dependen del orden en que se hayan tomado las formas (vease la primera nota de este artículo).

Notamos ademas que k, el maximo comun divisor de los nómeros P, Q, R, S, T y U, divide a los numeros mn0 y m0n (como queda claro a partir de los valores que establecimos mas arriba). Por tanto el cuadrado k divide a m2n y m n2, y Dk2 divide a d0m2 y d0m02. Pero recíprocamente, todo divisor comón de mn0 y m0n divide a k. Sea e un divisor tal: evidentemente este dividiró a an0, 2bn0, cn0, a0n, 2b0n y c0n; i.e., a los nómeros P, R — S, U, Q, R + S y T y tambien a 2R y 2S. Ahora si 2- es un nómero impar, — tambien debe ser impar (pues la suma y la

diferencia son pares) y el producto tambien deberá ser impar. Este producto es igual

4 /7/2 2 i2 /2\ 4/7/ 2i //2 7/2 /2\ 4 / / / 2 /2\ , ,

a ^2 (b n2 — b2n ) = ^2 (d n2 + a c n2 — dn — acn ) = ^2 (a c n — acn ) y por tanto

par, porque e divide a a0n, c'n, an0 y cn0. Asó es necesariamente par y ambos

R y S son divisibles por e. Ya que e divide a los seis P, Q, R, S, T y U, tambien

dividirá a k, su maximo comun divisor. Q. E. D. Concluimos que k es el máximo comón divisor de los nómeros mn0 y m0n, y Dk2 sera el múximo común divisor de los números dm02, d'm2. Esta es nuestra CUARTA CONCLUSIÓN. Ahora es claro

que siempre que F se componga de f y f', D será el máximo común divisor de los números dm' y d'm2 y vice versa. Estas propiedades pudieron tambien utilizarse como la definición de las formas compuestas. Por ende, la forma que esta compuesta de las formas f y f', posee el maximo determinante posible de todas las formas que son transformables en el producto ff'.

Antes de que continuemos más adelante, definiremos primero el valor de Δ mas exactamente. Mostramos que Δ = Vdd' = VD2n2n'2, pero no se ha determinado aún su signo. Para tal propásito deducimos a partir de las ecuaciones fundamentales [1] a [11] que DPQ = Δαα! (obtenemos esto a partir de [5][6] — [1][11]). Así Daa'nn' = Δαα', y a menos que uno de los numeros α o α' sea igual a 0, tenemos Δ = Dnn'. Exactamente de la misma forma, a partir de las ecuaciones fundamentales podemos deducir otras ocho en las cuales tenemos Dnn' a la izquierda y Δ en la derecha multiplicados por 2α6', α^, 26α', 466', 2bc', cα', 2cb' y cc'[[176]](#footnote-177)). Ahora, dado que no todos α, 2b y c ni todos α', 26' y c' pueden ser iguales a 0, en todos los casos Δ = Dnn' y Δ posee el mismo signo que D, d y d' o el opuesto, según que n y n' posean el mismo signo o signos diferentes.

Observamos que los números αα', 2α6', α^, 26α', 466', 2bc', cα', 2cb', cc', 266' + 2Δ y 266' — 2Δ son todos divisibles por mm'. Esto es obvio para los primeros nueve numeros. Para los otros dos podemos mostrar, como hicimos al principio, que R y S son divisibles por e. Es claro que 466' + 4Δ y 466' — 4Δ son divisibles por mm' (dado que 4Δ = \/16dd' y 4d es divisible por m2, 4d' por m'2, y así 16dd' por m2m'2 y 4Δ por mm') y que la diferencia de los cocientes es par. Es fúcil demostrar que el producto de los cocientes es par, y asú que cada cociente es par y que 266' + 2Δ, 266 — 2Δ son divisibles por mm .

Ahora a partir de las once ecuaciones fundamentales derivamos las seis siguientes:

AP2 = αα'ί'2 — 2α6'^' + α^2 AQ2 = αα'^''2 — 26α'^'' + cα'q2 AR2 = αα'^'''2 — 2(bb' + Δ)^''' + cc'q2 AS2 = α^''2 — 2(bb' — Δ)^'^'' + ca'q'2 AT2 = α^ί'''2 — 2bc'q'q''' + cc'q'2 AU2 = c^q'''2 — 2cb'q''q''' + cc'q''2

Se sigue por lo tanto que todos AP2, AQ2, etc. son divisibles por mm' y dado que k2 es el máximo común divisor de los números P2, Q2, R2, etc., Ak2 sera tambien divisible por mm'. Si sustituimos por a, 2b, c, a', 2b' y c' sus valores ny, etc. o n(pq' — qp'), etc., ellos podrían cambiarse por otras seis ecuaciones en las cuales tendremos, en el lado derecho, productos de la cantidad (q'q'' — qq''') por P2, Q2,

R2, etc. Dejaremos estos sencillos calculos al lector. Se sigue (puesto que no todo P2, Q2, etc. = 0) que Aun' = q'q'' — qq'''.

Similarmente, a partir de las ecuaciones fundamentales podemos obtener otras seis ecuaciones que difieren de las anteriores en que se reemplazan A y q, q', q'', q''' por C y p, p', p'', p''' respectivamente. Para abreviar omitimos los detalles. Finalmente, de modo semejante se sigue que Ck2 es divisible por mm' y Cun' = p'p'' — pp'''.

Nuevamente podemos deducir otras seis ecuaciones a partir de los mismos

datos:

BP2 = — aa'p'q' + ab' (pq' + qp') — ac'pq BQ2 = —aa'p''q'' + ba' (pq'' + qp'') — ca'pq BR2 = — aa'p'''q''' + (bb' + A)(pq''' + qp''') — cc'pq BS2 = —ac'p''q'' + (bb' — A)(p'q'' + q'p'') — ca'p'q'

BT = —acp q + bc (pq + qp ) — ccpq BU = —ca pq + cb (pq + qp ) — ccpq

y a partir de esto, como en el caso anterior, concluimos que 2Bk2 es divisible por mm' y 2Bnn' = pq''' + qp''' — p'q'' — q'p''.

Ahora, puesto que Ak2, 2Bk2 y Ck2 son divisibles por mm', es facil ver que Mk2 tambien debe ser divisible por mm'. De las ecuaciones fundamentales sabemos que M es divisor de aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb' y cc' y por lo tanto tambien de am', 2bm' y cm' (los cuales son los maximos comunes divisores de los primeros, segundos y últimos tres respectivamente); y finalmente que tambien es divisor de mm', el cual es el maximo común divisor de todos estos. Por lo tanto, en este caso, donde la forma F está compuesta por las formas f, f', eso es k = 1, M necesariamente = mm'. Esta es nuestra QUINTA CONCLUSIÓN.

Si designamos el maximo común divisor de los números A, B y C por M, sera = M (cuando la forma F es propiamente primitiva o se obtiene a partir de una forma propiamente primitiva) ú = 1M (cuando F es impropiamente primitiva o se obtiene a partir de una forma impropiamente primitiva); similarmente, si designamos los múximos comunes divisores de los numeros a, b y c; a', b' y c' por m y m' respectivamente, m sera = m o = ^m y m' sera = m' ú = ^m'. Ahora, es claro

que m2 es divisor de d, m'2 es divisor de d'. Por lo tanto m2m'2 es divisor de dd' o de Δ2, y mm' es divisor de Δ. De las ultimas seis ecuaciones para BP2 etc. se sigue que mm' es divisor de Bk2 y (puesto que tambien es divisor de Ak2 y de Ck2) de Mk2. Por lo tanto, cada vez que F este compuesta por f y f, mm' sera divisor de M. Y cuando ambos f y f' son propiamente primitivas u obtenidas a partir de formas propiamente primitivas, o mm' = mm' = M, entonces M = M o F es una forma similar. Pero, si bajo las mismas condiciones una o ambas formas f y f son impropiamente primitivas u obtenidas a partir de formas impropiamente primitivas, entonces (si la forma f por ejemplo lo es) a partir de las ecuaciones fundamentales se sigue que aa', 2ab', ad, ba!, 2bb', bC, ca', 2cb', cC son divisibles por M y así

tambien am', bm', cm' y mm' = 1 mm' = 2M; en este caso M = 2M y la forma F es impropiamente primitiva u obtenida a partir de una forma impropiamente primitiva. Esta es nuestra SEXTA CONCLUSIÓN.

Finalmente observamos que, si se supone que las siguientes nueve ecuaciones

|  |  |  |  |
| --- | --- | --- | --- |
| son verdaderas, | an = P, | 2bn = R - S, | cn = U |
|  | an = Q, | 2b n = R + S, | c n = T |
| Ann = q q - qq , | 2Bnn = | pq''' + qp''' - p'q'' | - q'p'', Cnn' = p'p'' - pp''' |

(en lo que sigue, designaremos estas condiciones por Ω, ya que las retomaremos frecuentemente) entonces, tomando n y n' como incógnitas pero ninguna = 0, encontramos mediante una sustitución sencilla que las ecuaciones fundamentales [1] a [9] son necesariamente verdaderas, o sea, que la forma (A, B, C) sera transformada en el producto de las formas (a, b, c)(a',b,C) mediante la sustitución p, p', p'', p''; q, q', q'', q'''. Tambien tendremos

b2 - ac = n2 (B2 - AC), b2 - a'c' = n'2 (B2 - AC)

El calculo, que sería demasiado largo para exponerlo aquí, lo dejamos al lector. [[177]](#footnote-178)

Solución. Sean (a, b, c) ...f y (a/,b/,c/) ...f las formas iniciales; d y d' sus determinantes; m y m' los máximos comunes divisores de los números a, 2b, c; a0, 2b0, d respectivamente; D el máximo común divisor de los números dm'2 y d'm2 tomados con el mismo signo que d y d'. Entonces ^ y d j serán números positivos primos relativos y su producto será un cuadrado; por lo tanto cada uno de ellos sera un cuadrado (art. 21). Así pues, y \fD serán cantidades racionales que dejaremos ser = n, n' y escogeremos para n un valor positivo o negativo dependiendo de si la forma f debe entrar directa o inversamente en la composicián. De manera similar determinaremos el signo de n' segán la manera en la cual la forma f debe entrar en la composicián. Entonces mn' y m'n serán enteros primos entre sí; n y n' pueden ser fracciones. Ahora observamos que an', cn', a'n, dn, bn' + b'n y bn' — b'n son

enteros. Esto es obvio para los primeros cuatro (puesto que an' = mmn' etc.); para los ultimos dos lo probamos tal como se hizo en el ultimo artículo para probar que R y S son divisibles por e.

Tomemos ahora cuatro enteros Q, Q', Q'' y Q''' arbitrarios con solo una condición, que las cuatro cantidades a la izquierda de las siguientes ecuaciones (I) no sean todas = 0. Ahora, considerense las ecuaciones:

Q'an + Q" a'n + Q'^bn' + b'n) = μq (I)

—Qan' + Q///c/n — Q" (bn' — b'n) = μq/

Q"'cn' — Qa'n + Q' (bn' — b'n) = μq//

—Q" cn' — Q' c'n — Q(bn' + b'n) = μq///

tales que q, q', q'' y q''' son enteros sin un divisor comán. Esto se puede lograr tomando para μ el maximo comán divisor de los cuatro námeros que estan a la izquierda de las ecuaciones. Ahora, segun el artáculo 40 podemos encontrar cuatro enteros P, P', P' y P'' tales que

Pq + p q' + p'q" + P'Y' = 1

Una vez logrado esto, determánense los námeros p, p', p" y p''' mediante las siguientes ecuaciones:

P an' + p 'a'n + p''(bn' + b'n) = p (II)

—Pan' + p''c'n — p(bn' — b'n) = p'

P''cn' — Pa'n + p (bn' — b'n) = p''

—P''cn' — P' c'n' — P(bn' + b'n) = p'''

Ahora se hacen las siguientes sustituciones:

q q — qq = Ann , pq + qp — pq — qp = 2Bnn , p p — pp = Cnn

Entonces A, B y C serán enteros y la forma (A, B, C) . ..F será compuesta por las formas f y f'.

Demostración. I. A partir de (I) obtenemos las siguientes cuatro ecuaciones:

0 = q0cn0 — q//c/n — q'"(bn' — bbn) (III)

0 = qcn0 + q,"a'n — q"(bn' + b0n)

0 = q'" an' + qC n — q' (bn' + b0n)

0 = q an — qan — q(bn — b'n)

II. Ahora supongamos que los enteros A, B, C, A, B', C, N, N' se determinan de modo que

Aa + 2Bb + Cc = m A' a + 2B' b' + C c = m'

Nm'n + N' mn' = 1

Entonces tendremos

AaN'n' + 2BbN'n + CcN'n + A'a Nn + 2B'b'Nn + C'c Nn = 1

A partir de esto y las ecuaciones (III), si dejamos que

—q' AN' — q''A'N — q'' '(BN' + B'N) = q qAN' — q'''C'N + q''(BN' — B'N) = q'

—/'CN' + qA'N — q' (BN' — B'N) = q'' q''CN' + q' C'N + q(BN' + B'N) = q'''

obtendremos

q' an + q''a'n + q"'(bn + b'n) = q (IV)

— qan' + q'' 'c'n — q''(bn' — b'n) = q' q''' cn' — qa'n + q' (bn' — b'n) = q''

— q''cn' — q' c'n — q(bn' + b'n) = q'''

Cuando μ = 1 estas ecuaciones son innecesarias y se pueden utilizar las

ecuaciones (I), que son enteramente análogas, en su lugar. Ahora, a partir de las

ecuaciones (II) y (IV) determinamos los valores de Ann0, 2Bnn' y Cnn' (i.e. de

los námeros q'q'' — qq'" etc.) y suprimimos los valores que se anulan entre sí, y

2

encontramos que los terminos diferentes son productos de enteros por nn', dn' o d'n2. Además, todos los terminos de 2Bnn' contienen el factor 2. Concluimos que A, B y C son enteros (porque dn'2 = d'n2 y por lo tanto ^¡L— = d'¡¡¡¡7· = ^/dd! son

enteros). Q. E. P.

1. Si tomamos los valores de p, p', p'' y p''' de (II), utilizamos las ecuaciones (III) y la siguiente:

Pq + Pq' + P'q'' + P''q''' = 1

encontramos que

pq' — qp' = an', pq'" — qp"' — p'q'' + q'p'' = 2bn', p''q''' — q''p''' = cn'

pq'' — qp'' = a'n, pq''' — qp''' + p'q'' — q'p'' = 2b'n, p'q'" — q'p'" = c'n

Estas ecuaciones son identicas a las primeras seis (Ω) del artículo anterior. Las tres restantes son parte de la hipótesis. Por lo tanto (final del mismo artículo) la forma F se transformará en ff' mediante la sustitucion p, p', p'', p'''; q, q', q'', q'''; su determinante sera = D, o sea, sera igual al maximo comán divisor de los námeros dm' y d'm2. Segun la cuarta conclusion del artáculo anterior esto significa que F está compuesta por f y f', Q. E. S. Y finalmente se sabe que F se compone de f y f seguán la forma prescrita puesto que los signos de n y n se determinaron correctamente al comienzo. [[178]](#footnote-179)

Para abreviar designaremos estos coeficientes como sigue:

ap + γp , βρ + δp' etc. = P, p', p', P"; O, O', O'', O'''

y sea el número αδ — βγ = e. A partir de las ecuaciones Ω, artículo 235, es fácil ver que

PO' — Qp = an'e PO''' — Qp'' — p Q" + Q'p' = 2bn'e P' O''' — Q''p'' = cn'e PO'' — Qp' = a2a'n + 2aqb'n + q2c'n = a" n PO''' — Qp'' + pQ'' — Q'p' = 2b''n pQ''' — Q'p'' = C'n O'O'' — QQ''' = Ann e PO''' + Qp'' — pQ'' — Q'p' = 2Bnn e PP' — PP''' = Cnn'e

Ahora, si designamos el determinante de la forma f'' por d'', e sera una raíz cuadrada de j, positiva o negativa según la forma f implica la forma f' propia o impropiamente. Así pues n'e sera una raíz cuadrada de jy; y las nueve ecuaciones anteriores serán completamente analogas a las ecuaciones Ω del artículo 235. La forma f se tomará en la transformacián de la forma F en ff'' de manera identica a como se tomo en la transformacián de la forma F en ff'. La forma f'' en la primera debe tomarse como se tomá f' en la segunda si f' implica f'' propiamente. Si f' implica f impropiamente, debe tomarse de manera opuesta. [[179]](#footnote-180)

F' se convierte en lo mismo que F mediante la sustitución p, p, p", p'"; q, q0, q00, q000 y por lo tanto a traves de esta transformación F0 se transforma en ff0. Q. E. D.

Mediante un cálculo similar al del artículo anterior tambien es posible comprobar que F0 es transformable en ff0 de la misma manera que F, cuando F0 implica F propiamente. Pero cuando F esta contenida impropiamente en F0 las transformaciones de las formas F y F0 en ff0 serán opuestas respecto a cada una de las formas f y f0; eso es, si una forma aparece en una de las transformaciones directamente, aparecerá en la otra de manera inversa.

Si combinamos este teorema con el del artículo anterior obtendremos la siguiente generalizacion. Si la forma F es transformable en el producto ff', si las formas f y f0 implican las formas g y g0 respectivamente, y si la forma F esta contenida en la forma G: entonces G será transformable en el producto gg'. En efecto, segun el teorema de este artículo G es transformable en ff0 y así segun el teorema anterior en fg0 y así tambien en gg0. Tambien es claro que, si todas las tres formas f, f0 y G implican las formas g, g0 y F propiamente, G sera transformable en gg0 con respecto a las formas g y g0 de igual manera que F en ff0 con respecto a las formas f y f0. Lo mismo es cierto si las tres implicaciones son impropias. Si una de las implicaciones es diferente de las otras dos, es igualmente facil determinar como G es transformable en gg0.

Si las formas F, f y f0 son equivalentes a las formas G, g y g0 respectivamente, los segundos tendrán los mismos determinantes que los primeros. Y m y m0 serán para g y g0 los mismos que para f y f0 (art. 161). Así pues, segun la cuarta conclusion del artículo 235 se deduce que G esta compuesta por g y g0 si F esta compuesta por f y f0; y de hecho la forma g entrara en la primera composicion de igual manera que f lo hace en la segunda, siempre y cuando F sea equivalente a G de la misma manera que f lo es a g y vice versa. Similarmente g0 debe tomarse en la primera composicion de manera igual u opuesta a como se tomo f0 en la segunda, segun la equivalencia de las formas f0 y g0 sea similar o no a la equivalencia de las formas F y G. [[180]](#footnote-181)

F' = (A',B',C') cuyo determinante = D' se transforma en el producto ff' mediante la sustitución p, p', p00, p000; q, q', q00, q000. Designemos los números

pq' - qp0,

**///**

pq - qp , pq - qp'

///

p0q00

q0p00,

p0q000

Jjn

q p ,

p q - q p

respectivamente por

P', Q', R', S0, T0, U0

Entonces se tendran nueve ecuaciones que son completamente similares a las de Ω, a saber

P' = an', R' - S' = 2bn', U' = cn'

Q' = a' n, R' + S' = 2b'n, T = c'n

q'q'' - qq'0' = A'nn', pq'0' + qp'0' - p'q'' - q'p'' = 2B'nn', p'p'' - pp'0' = C'nn'

Designaremos estas ecuaciones por Ω'. Las cantidades n y n' son, en este caso, las raíces cuadradas de j y j, y tienen el mismo signo que n y n' respectivamente; entonces, si tomamos la raíz cuadrada positiva de j (sera un entero) y lo hacemos = k, tendremos n = kn, n' = kn'. Entonces, a partir de las primeras seis ecuaciones de Ω y Ω' obtenemos

P' = kP, Q' = kQ, R' = kR S' = kS, T = kT, U' = kU

Según el lema del artículo 234 podran encontrarse cuatro enteros α, β, γ, δ tales que

ap + βq = p, γp + δq = q α^ + βq' = p', qp' + δq' = q' etc.

y

αδ - βγ = k

Sustituyendo estos valores de p, q, p', q', etc. en las ultimas tres ecuaciones de Ω' y utilizando las ecuaciones n = kn, n' = kn' y las ultimas tres ecuaciones de Ω encontramos que

A'a2 + 2Β'αγ + C'q2 = A Α'αβ + B' (αδ + βγ) + ^γδ = B Α'β2 + 2Β'βδ + C^2 = C

Por lo tanto, mediante la sustitución α, β, γ, δ (que será propia puesto que αδ-βγ = k es positivo) F' se transformara en F i.e. implicara la forma F propiamente. Q. E. D.

Por lo tanto si F' está compuesta por las formas f y f (de la misma manera que F), las formas F y F' tendrán el mismo determinante y serán propiamente equivalentes. De manera más general, si la forma G está compuesta por las formas g y g de la misma manera que F está compuesta por las formas f y f0 respectivamente y las formas g y g0 son propiamente equivalentes a f y f0: entonces las formas F y G son propiamente equivalentes.

Puesto que este caso, donde ambas formas a componer entran directamente en la composition, es el mas sencillo y los otros se pueden reducir facilmente a el, solo consideraremos este en lo que sigue. Entonces si alguna forma se dice estar compuesta por otras dos, se debe interpretar siempre como si estuviera propiamente compuesta de cada una de ellas\*). La misma restriction quedara implícita cuando se dice que una forma es transformable en un producto de otras dos.

240.

TEOREMA. Si la forma F está compuesta de las formas f y f; la forma F de F y f"; la forma F0 de f y f"; la forma F0 de F0 y f: entonces las formas F y F0 serán propiamente equivalentes.

Demostración. I. Sea

f = ax2 + 2bxy + cy f0 = a0x02 + 2b0x0y0 + c0y02

¿η u //2 i 0,// n n . n //2

f = a x +2bxy + cy F = AX2 + 2BXY + CY2 F0 = A0X02 + 2B0X0Y0 + C0Y02 F = AX2 + 2BXY + CY2 F0 = A0X02 + 2B0X0Y0 + c0y02

y sean d, d', d00, D, D0, D y D0 los determinantes de las siete formas respectivamente. Todos tendrán los mismos signos y diferirán por factores cuadrados. Además, sea m el

\*) Tal como en una composición de razones (la cual es muy similar a la composición de formas) normalmente entendemos que las razones son tomadas directamente a menos que se indique lo contrario.

máximo común divisor de los números a, 2b, c y sean m0, m" y M con el mismo sentido

respecto a las formas f0, f00 y F. Entonces a partir de la cuarta conclusiún del artículo

235, D serú el múximo común divisor de los números dm' , d0m2; Dm'0 el maximo

2 2 2

comuún divisor de los nuúmeros dm' m" , dm2m00 ; M = mm0; D el maximo comun divisor de los nuúmeros Dm002, d00M2 o de los números Dm002, d00m2m02. Concluimos que D es el máximo comun divisor de los tres números dm02m002, d0m2m002, d00m2m02. Por razones similares D0 sera el maximo común divisor de los mismos tres números. Entonces, puesto que D y D0 tienen el mismo signo, D = D0 y las formas F y F0 tendrúan el mismo determinante.

II. Ahora, sea F que se transforma en ff0 mediante la sustitución

X = pxx + p xy + p yx + p yy

* = qxx + q xy + q yx + q yy y F en Ff mediante la sustituciún

X = pXx00 + p' Xy" + p00 Y x00 + p000Yy00

* = qXx00 + q0Xy00 + q00Yx00 + q000Yy00

y designemos las raíces positivas de D, D, y, y Por n, n0, N, n00. Entonces, segun el artículo 235 habrá 18 ecuaciones, la mitad de las cuales pertenecen a la transformaciún de la forma F en ff0 y la otra mitad a la transformacion de la forma F en Ff00. La primera de ellas serú pq0 — qp0 = an!. Las demús se podran generar de la misma manera, pero para abreviar, las omitiremos aquú. Note que las cantidades n, n!, N, n00 serán racionales pero no necesariamente enteros.

1. Si los valores de X e Y se sustituyen en los valores de X e Y obtenemos un resultado de la forma:

X = (1)xx0x00 + (2)xx0y00 + (3)xy0x00 + (4)xy0y00

+ (5)yx0x00 + (6)yx0y00 + (7)yy0x00 + (8)yy0y00 Y = (9)xx0x00 + (1O)xx0y00 + (11)xy0x00 + (12)xy0y00

+ (13)yx0x00 + (14)yx0y00 + (15)yy0x00 + (16)yy0y00

Obviamente, mediante esta sustitucion F se transformará en el producto ff0f00. El coeficiente (1) sera = pp+qp00 y el lector podra desarrollar los quince valores restantes. Designaremos el número (1)(10) — (2)(9) por (1, 2), el número (1)(11) — (3)(9) por (1, 3) y en general (g)(8 + h) — (h)(8 + g) por (g, h) donde g y h son enteros diferentes

entre 1 y 16 con h el mayor de ellos\*); de esta manera tenemos 28 símbolos en total. Ahora si designamos las raíces cuadradas positivas de D y dD por n y n0 (serán = nN y n0N) tendremos las siguientes 28 ecuaciones:

(1, 2) = aa0n (1, 3) = αα00η0

1. = ab' η00 + ab'0 η'

(1, 5) = α0α00η

(1, 6) = a0bn00 + a0b00n

(1, 7) = a00bn0 + a00b0n

(1,8) = bb0n00 + bb00n0 + b0 b00n + Dnn0n00

(2, 3) = ab00n0 - ab0n00

1. = ac00n0

(2, 5) = a0b00n — a0bn00 (2, 6) = a0c00n

(2, 7) = bb00n0 + b0b00n — bb0n00 — Dnn0n00 (2, 8) = bc00n0 + b0c00n

1. = ac0n00

(3, 5) = a b0n — a00bn0

(3,6) = bb0n00 + b0b00n — bb00n0 — Dnn0n00

(3, 7) = a00c0n

(3, 8) = bc0n00 + b00c0n

(4,5) = b0b00n — bb0n00 — bb00n0 + Dnn0n00

(4, 6) = b0c00n — bc00n0

(4, 7) = b00c0n — bc0n00

(4, 8) = c0c00n

(5, 6) = ca0n00

(5, 7) = ca00n0

(5, 8) = b0cn00 + b00cn0

(6, 7) = b00cn0 — b0cn00

(6, 8) = cc00n0 (7, 8) = cc0n00

Designaremos estas ecuaciones por Φ, y tendremos otras nueve:

(10)(11) — (9)(12) = an0n00A (1)(12) — (2)(11) — (3)(10) + (4)(9) = 2an0n00B

= 4bn0n00B

1. (3) — (1)(4) = an0n00C — (9)(16) + (10)(15) + (11)(14) — (12)(13) = 2bn0n00a (1)(16) — (2)(15) — (3)(14) + (4)(13)'

+ (5)(12) — (6)(11) — (7)(10) + (8)(9),

— (1)(8) + (2)(7) + (3)(6) — (4)(5) = 2bn0n00C (14)(15) — (13)(16) = cn0n00 A (5)(16) — (6)(15) — (7)(14) + (8)(13) = 2cn0n00B

(6)(7) — (5)(8) = cn0n00 C [[181]](#footnote-182) [[182]](#footnote-183)

a las que designaremos por Ψ[[183]](#footnote-184)).

1. Tomarla demasiado tiempo deducir todas las 37 ecuaciones, nos confor­maremos con establecer algunas de ellas como un modelo para las demás.
2. Tenemos

(1,2) = (1)(10) - (2)(9)

= (pq' - qp')p2 + (pq'" - qp''' - p'q" + q'p")pq + (p"q"' - q''p''')q2

= n''(Ap2 + 2Bpq + Cq2) = n''aa'

que es la primera ecuaciáon.

1. Tenemos

(1, 3) = (1)(11) - (3)(9) = (pq00 - qp'')(pq' - qp') = a"Nan' = aa''n'

la segunda ecuaciáon

1. Y tenemos

(1, 8) = (1)(16) - (8)(9)

= (pq' - qp')pp''' + (pq''' - qp''')pq''' - (p'q'' - q'p'')qp''' + (p''q''' - q''p''')qq'''

= n'' (App'' + B (pq''' + qp''') + Cqq''') + b''N(pq''' - qp''')

= n''(bb' + Vdd) + b''N(b'n + bn') j)

= n''bb' + n' bb'' + nb'b'' + Dnn'n'',

la octava ecuacián en Φ. Dejamos al lector la comprobacián de las restantes

ecuaciones.

1. Mediante las ecuaciones Φ, mostraremos que los 28 numeros (1, 2), (1, 3) etc. no tienen ningán divisor común. Primero observamos que se puede hacer 27 productos de tres factores tales que el primero es n, el segundo es uno de los nuámeros a', 2b', c' y el tercero es uno de los námeros a'', 2b'', C'; o que el primero es n', el segundo es uno de los námeros a, 2b, c y el tercero uno de los numeros a'', 2b'', c''; o finalmente que el primero es n'', el segundo uno de los námeros a, 2b,

c y el tercero uno de los números a0, 2b0, C. Cada uno de estos 27 productos, debido a las ecuaciones Φ, serú igual a uno de los 28 numeros (1, 2), (1,3) etc. o la suma o diferencia de algunos de ellos (ej. na0a00 = (1, 5), 2na'b00 = (1, 6) + (2, 5), 4nb'b00 = (1, 8) + (2, 7) + (3,6) + (4, 5) etc.). Por lo tanto si estos números tuvieran un divisor común, necesariamente dividiría todos estos productos. Entonces mediante el artículo 40 y el metodo utilizado tantas veces anteriormente, el mismo divisor tambien debe dividir los números nm0m00, n0mm00, n00mm0 y el cuadrado de este divisor debe tambien dividir a los cuadrados de estos números, es decir,

d'm2m"2 d"'m2m'2 D , D ·■

*dm'2m"* 2 D ,

Q. E. A. , pues según I el maximo comun divisor de los tres

numeradores es D y asú estos tres cuadrados no pueden tener un divisor común.

1. Todo esto se refiere a la transformación de la forma F en ff0f00; y se puede deducir de la transformaciún de la forma F en ff0 y de la forma F en Ff0. De manera completamente similar se deriva la transformaciún de la forma F' en fff0 a partir de transformaciones de la forma F0 en ff00 y de la forma F' en F0f0:

X0 = (1)0xx0x00 + (2)0xx0y00 + (3)0xy0x00 + etc.

Y = (9)0xx0x00 + (1O)0xx0y00 + (11)0xy0 x00 + etc.

(aquú los coeficientes son designados de la misma manera que en la transformaciún de la forma F en fff00, pero se les ha puesto primos para distinguirlos). A partir de estas transformaciones deducimos, igual que antes, 28 ecuaciones anaúlogas a las ecuaciones Φ que llamaremos Φ0 y otras nueve anúlogas a las ecuaciones Ψ que llamaremos Ψ0. Asú pues si denotamos

(1)0(1O)0 - (2)0(9)0 por (1,2)0, (1)0(11)0 - (3)0(9)0 por (1,3)0, etc.

las ecuaciones Φ0 serúan

(1, 2)0 = aa0n00, (1,3)0 = aa00n0, etc.

y las ecuaciones Ψ0 serún

(1O)0(11)0 - (9)0(12)0 = an0n00A0 etc.

(Para abreviar dejamos un estudio mas detallado de esto al lector; el experto no necesitara realizar nuevos calculos puesto que hay una analogía entre este y el primer anúlisis). Ahora, a partir de Φ y Φ0 se sigue inmediatamente que

(1, 2) = (1, 2)0, (1,3) = (1,3)0, (1,4) = (1,4)0, (2, 3) = (2, 3)0, etc.

Y puesto que todos los (1, 2), (1, 3), (2, 3), etc. no poseen un divisor común (según V), con la ayuda del lema del artículo 234 podemos determinar cuatro enteros α, β, γ, δ tales que

α(1)' + β(9)' = (1), α(2)' + β(10)' = (2), α(3)' + β(11)' = (3) etc.

γ(1)' + δ(9)' = (9), γ(2)' + δ(10)' = (10), γ(3)' + δ(11)' = (11) etc.

y αδ — βγ = 1.

1. Ahora, si sustituimos de las tres primeras ecuaciones de Ψ, valores para aA, aB, aC, y de las tres primeras ecuaciones de Ψ' los valores de aA', aB', aC se confirma facilmente que:

a(Aa2 + 2Βαγ + £γ2) = a A' a(Aαβ + Β(αδ + βγ) + £γδ) = aB' a(aβ2 + 2Ββδ + £δ2) = aC

y a menos que a = 0 se sigue que la forma F se transforma en la forma F' mediante la sustitución propia α, β, γ, δ. Si en lugar de las primeras tres ecuaciones de Ψ y Ψ' utilizamos las tres siguientes, obtendremos tres ecuaciones como las anteriores excepto que ahora los factores a serían reemplazados con b; y la misma conclusiún es valida siempre y cuando no sea b = 0. Finalmente si utilizamos las últimas tres ecuaciones en Ψ y Ψ' las conclusiones son las mismas a menos que c = 0. Y puesto que ciertamente no todos los factores a, b, c pueden ser = 0 simultúneamente, la forma F necesariamente se transformarú en la forma F' mediante la sustitucion α, β, γ, δ y las formas serán propiamente equivalentes. Q. E. D. [[184]](#footnote-185)

también que el orden de composición es arbitrario; i.e. no importa en que orden se componen estas formas, las formas resultantes serán propiamente equivalentes. Es claro tambien que si las formas g, g, g", etc. son propiamente equivalentes a las formas f, f, f", etc. respectivamente, la forma compuesta de las primeras sera propiamente equivalente a la forma compuesta de las uóltimas.

242.

Las proposiciones anteriores se refieren a la composición de formas en toda su universalidad. Ahora pasaremos a aplicaciones mas particulares que no estudiamos anteriormente para no interrumpir el orden del desarrollo. Primero retomaremos el problema del artículo 236 limitóndolo segón las siguientes condiciones: primero las formas a componer deben tener el mismo determinante, i.e. d = d'; segundo, m y m deben ser primos relativos; tercero, la forma que buscamos debe ser compuesta directamente por f y f. Entonces m2 y m/2 tambien serán primos relativos; y así el maximo comun divisor de los numeros dm02 y d0m2 i.e. D sera = d = d0 y n = n0 = 1. Puesto que podemos escogerlos libremente, haremos que las cuatro cantidades Q, Q0, Q0/, Q'" = -1, 0, 0, 0 respectivamente. Esto esta permitido excepto cuando a, a', b + b0 son todos = 0 simultáneamente, así que omitiremos este caso. Claramente esto no puede ocurrir excepto en formas con un determinante cuadrado positivo. Ahora, si μ es el maximo comun divisor de los numeros a, a', b + b', los numeros P', P", P'" pueden escogerse tales que

P'a + PV + P"(b + b0) = μ

En cuanto a P, este puede escogerse arbitrariamente. Como resultado, si sustituimos p, q, p, q0 etc. por sus valores, tenemos:

*A*

*aa*

*B*

1

μ

(Paa + P0 ab + p//ab + P^bb0 + D))

y C puede determinarse de la ecuacion AC = B2 — D siempre y cuando a y a0 no sean simultaneamente = 0.

Ahora, en esta solucion el valor de A es independiente de los valores de P, P0, P", P'" (los cuales se pueden determinar de una infinidad de maneras); pero B tendra valores diferentes al asignar valores variados a estos numeros. Entonces valela pena investigar cómo están interconectados todos estos valores de B. Para esto observamos

1. No importa cómo se determinan P, P0, P00, P000, todos los valores de B son congruentes segón el modulo A. Supongamos que si

P = p, P0 = p0, P00 = p00, P000 = p000 tenemos B = B

pero haciendo

P = p + d, P0 = p0 + d0, P00 = p00 + d00, P000 = p000 + d000 tenemos B = B + D Entonces tendremos

ad0 + a0d00 + (b + b0)d000 = 0, aa0d + ab'd0 + a0bd00 + (bb0 + D)d000 = μ©

Multiplicando el primer miembro de la segunda ecuación por ap0 + a0p00 +(b + b0)p000, el segundo miembro por μ, y restando del primer producto la cantidad

(ab0p0 + a0bp00 + (bb0 + D)p000)(ad0 + a0d00 + (b + b0)d000)

lo cual segun la primera ecuacion anterior es claramente = 0, se encontraró, despues de cancelar los tóerminos nulos que

aa0^d + ((b0 - b)p00 + c0p 000)d0 - ((b - b0)p0 + cp000)d00 - (c0p0 + cp00)d000} = μ2©

De donde es claro que μ2© seró divisible por aa0 y D por μτ i.e. por A y

B = B + D (mod. A)

1. Si los valores p, p0, p00, p000 de P, P0, P00, P000 hacen B = B, entonces

se pueden encontrar otros valores de estos números que harón que B sea igual a cualquier nómero dado que sea congruente a B segón el módulo A, a saber B + kA. Primero observamos que los cuatro nómeros μ, c, c0, b - b0 no pueden tener un divisor comón; pues si lo hubiera, sería un divisor de los seis nómeros a, a0, b + b0, c, c0, b - b0 y luego de a, 2b, c y a0, 2b0, c0 y por lo tanto tambien de m y m0 que son por hipotesis primos relativos. Así pues, se pueden encontrar cuatro enteros h, h0, h00 y h000 tales que

Λ,μ + h0c + h00c0 + h000(b - b0) = 1

Y si ponemos

kh = d,

k(h0(b + b0) + h'"a) = μd00,

k(h00(b *+* b0) *— h000a0) =* μΰ0 — *k(h'a'* + *h"a) =* μΰ000

es claro que d, d0, d00 y d000 son enteros y

ad0 + a0d00 + (b + b0)d000 = 0

aa0k

*μ*

aa0d + ab0d0 + a0bd00 + (bb0 + D) d000

(μΛ, + ch0 + c'h" + (b — b0)h000) = μkA

A partir de la primera ecuación es claro que p+d, p0+d0, p00+d00 y p000+d000 son tambien valores de P, P0, P00 y P000; y de la ultima, que estos valores nos dan B = B + kA, Q. E. D. En este caso queda claro que B siempre puede escogerse tal que quede entre 0 y A — 1 inclusive, para A positivo; o entre 0 y —A — 1 para A negativo. [[185]](#footnote-186)

P0a + P00a0 + P000(b + b0) = μ,

B

1

μ

(P aa0 + P0 ab0 + P"a'b + P000 (bb0 + D))

deducimos

B

b + - (Pa0 + P0(b0 — b) — P000c) μ

b0 +

a0

μ

(Pa + P00(b — b0) — P000 c0)

y por lo tanto

a a0

B = b (mod. —) y B = b0 (mod. —)

Ahora, cuando μ y a son primos relativos, existira entre 0 y A — 1 (o entre 0 y — A — 1 cuando A es negativo) solo un numero que seró = b (mod. μ) y = b0 (mod. μ). Si

dejamos que sea = B y B = C es claro que (A,B,C) estara compuesta de las formas (a, b, c) y (a0,b0,c0). Entonces en este caso no es necesario considerar losnúmeros P, P0, P00 y P000 para encontrar la forma compuesta[[186]](#footnote-187)). Así pues, si se busca la forma compuesta por las formas (10, 3, 11) y (15, 2, 7) tendremos a, a0, b + b0 = 10, 15, 5 respectivamente; μ = 5; tal que A = 6; B = 3 (mod. 2) y ξ 2 (mod. 3). Por lo tanto B = 5 y (6, 5, 21) es la forma buscada. Pero la condiciún de que μ y μ sean primos relativos es equivalente a pedir que los dos números a y a0 no tengan divisor común mayor que los tres números a, a0, b + b0 o lo que es lo mismo, que el maximo común divisor de a y a0 tambien sea divisor del número b + b0. Se notan los siguientes casos particulares.

1. Suponga que tenemos dos formas (a,b,c) y (a0,b0,c0) con el mismo

determinante D y relacionadas tales que el maximo común divisor de los números a, 2b, c es primo relativo al maximo común divisor de a0, 2b0, c0 y que a y a0 son primos relativos: entonces la forma (A,B, C), que es la composición de estas dos, se encuentra haciendo A = aa0, B ξ b (mod. a) y ξ b0 (mod. a0), C = B —D. Este

caso siempre ocurrirúa cuando una de las dos formas a ser compuestas es la forma principal; esto es a = 1, b = 0, c = —D. Luego A = a0, B se puede tomar = b0 y tendremos C = c0; así pues cualquier forma está compuesta de sí misma y de la forma principal del mismo determinante.

1. Si queremos componer dos formas opuestas propiamente primitivas, esto es (a, b, c) y (a, —b, c), tendremos μ = a. Es fácil ver que la forma principal (1, 0, —D) esta compuesta por estas dos.
2. Suponga que tenemos un nuúmero arbitrario de formas propiamente primitivas (a, b, c), (a0,b0,c0), (a00,b00,c00), etc. con el mismo determinante y con los primeros terminos a, a0, a00, etc. primos relativos entre sí. Entonces se puede encontrar la forma (A, B, C) compuesta por todas ellas fijando A igual al producto de todos los a, a0, a00, etc.; tomando B congruente a b, b0, b00, etc. respecto a los modulos a, a0, a'

00

2,

Obviamente la forma (aa0,B, Bq-,D)

B2—D  
A

etc. respectivamente; y haciendo C = estarú compuesta por las dos formas (a, b, c) y (a0,b0,c0); la forma (aa0a00,B, B —D) estarú compuesta por las formas (aa0,B, Ba—,D) y (a00,b00,c00) etc. En cambio

aa

1. Suponga que tenemos una forma (A, B,C) propiamente primitiva de determinante D. Si se resuelve el termino A en un número cualquiera de factores

a *B  
μ*

*ab'*

*,*

*μ*

*a'B*

*μ*

a 'b μ

(b + b')B \_ (bb' + D)

μ

μ

(mod. A).

primos relativos a, a', a'', etc.; si se toman los números b, b', b", etc. todos iguales a B o por lo menos congruentes a B segun los modulos a, a', a'', etc. respectivamente; y si c, c', c'', etc. son tales que ac = b2 — D, a!c' = b' — D, a''c'' = b'' — D, etc.: entonces la forma (A, B,C) estará compuesta por las formas (a, b,c), (a',b',C), (a",b",C), etc., o diremos que se puede descomponer en estas formas. Es facil demostrar que esta proposición es tambien valida cuando la forma (A, B, C) es impropiamente primitiva u obtenida a partir de una forma de tal tipo. Así, de esta manera, cualquier forma puede resolverse en otras con el mismo determinante, en las cuales los primeros terminos son números primos o potencias de números primos. Tal descomposicion en muchos casos puede ser muy útil si queremos componer una forma a partir de varias formas dadas. Así pues, por ejemplo, si queremos una forma compuesta de las formas (3, 1, 134), (10, 3,41) y (15, 2, 27), descomponemos la segunda en (2,1, 201) y (5, —2, 81), la tercera en (3, —1,134) y (5, 2, 81). Es claro que la forma compuesta por las cinco formas (3,1,134), (2,1, 201), (5, —2, 81), (3, —1,134) y (5, 2, 81) independientemente del orden en el cual se toman, tambien sera una composicion de las tres formas originales. Ahora, la composicion de la primera con la cuarta da la forma principal (1, 0, 401); y lo mismo resulta de la composicion de la tercera con la quinta; así de la composicion de las cinco obtenemos la forma (2, 1, 201).

1. Debido a su utilidad es conveniente describir mas detalladamente este metodo. De la observacion anterior es claro que siempre y cuando las formas dadas son propiamente primitivas con el mismo determinante, el problema se puede reducir a la composicion de formas cuyos terminos iniciales son potencias de numeros primos (puesto que un numero primo se puede considerar como su propia primera potencia). Por esta razon es apropiado considerar el caso especial en el cual se componen dos formas propiamente primitivas (a, b, c) y (a',b,c) siendo a y a' potencias del mismo número primo. Por lo tanto, sean a = hA, a' = hA, donde h es un numero primo y vamos a suponer que χ no es menor que λ (lo cual es legítimo). Ahora hA sera el maximo comun divisor de los numeros a, a'. Si ademas es divisor de b + b' tendremos el caso que consideramos al inicio del artículo y la forma (A, B,C) sera la forma compuesta si A = hx-A, B ξ b (mod. hx-A) y ξ b' (mod. 1). Esta ultima condicion obviamente puede omitirse. Finalmente C = B . Si hA no divide a b+b', el maximo comun divisor de estos numeros sera necesariamente una potencia de h, digamos hv con ν < λ (donde ν = 0 si hA y b + b' son primos entre sí). Si P', P'' y P''' se

determinan de modo que

P' hx + p''hA + P'''(b + b') = hv

con P arbitrario, la forma (A, B, C) será compuesta de las formas dadas si se escoge

B 2 D

A = hx+A-2v, B = b + hx-v(Phx - P'(b - b') - P"c), C =

A

Pero es facil ver que en este caso tambien P' puede escogerse arbitrariamente; entonces poniendo P = P' = 0 resulta

B = b - P'''chx-V

o más generalmente

B = kA + b - P'''chx-V

donde k es un numero arbitrario (artículo anterior). Sálo P''' entra en esta fármula muy sencilla, y es el valor de la expresión (mod. hA)[[187]](#footnote-188)). Si, por ejemplo, se busca

la forma compuesta de (16, 3,19) y (8,1, 37), resulta h = 2, χ = 4, λ = 3, ν = 2. Por esto A = 8 y P''' es un valor de la expresián | (mod. 8), digamos 1, de donde B = 8k - 73, y poniendo k = 9, B = -1 y C = 37, la forma buscada es (8, -1, 37).

Entonces, si se proponen varias formas cuyos terminos iniciales son todos potencias de námeros primos, hay que examinar si algunos de estos terminos son potencias del mismo námero primo y, en este caso, las formas se componen de acuerdo con las reglas que acabamos de dar. Así se obtienen formas cuyos primeros terminos son potencias de námeros primos diferentes. La forma compuesta de estas puede encontrarse por la tercera observaciáon. Por ejemplo, cuando se proponen las formas (3,1,47), (4,0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21) y (16, 6,11), de la primera y la quinta resulta (27, 7, 7); de la segunda y la cuarta (16, -6,11); y de esta y la sexta (1, 0,140), que puede omitirse. Se quedan (5, 0, 28) y (27, 7, 7) que producen (135,-20, 4), que se reemplaza con la forma propiamente equivalente (4, 0, 35). Esta es la forma que resulta de la composicián de las seis formas propuestas.

Similarmente pueden desarrollarse más artificios útiles en la practica, pero nos obligamos a suprimir esta direccion para pasar a asuntos mas difíciles.

244.

Si el námero a puede ser representado por alguna forma f, el námero a' por la forma f', y si la forma F es transformable en ff': no es difícil ver que el producto

aa' será representable por la forma F. Se sigue inmediatamente que cuando los determinantes de estas formas sean negativos, la forma F sera positiva si ambas f y f' son positivas o ambas negativas; al contrario F sera negativa si una de las formas f y f' es positiva y la otra es negativa. Detengamonos particularmente en el caso que hemos considerado en el artículo previo, donde F está compuesta por f y f' y f, f' y F tienen el mismo determinante D. Ademas, supongamos que las representaciones de los numeros a y a' por las formas f y f' se hacen por medio de valores relativamente primos de los incognitas. Supondremos tambien que la primera pertenece al valor b de la expresión \JD (mod. a), la ultima al valor b' de la expresión \/D (mod. a') y

que b2 — D = ac, b'2 — D = a'c'. Luego, por el artículo 168, las formas (a, b, c) y (a', b', c') serán propiamente equivalentes a las formas f y f', de modo que F estará compuesta por esas dos formas. Pero la forma (A, B, C) estará compuesta por las mismas formas si el maximo comun divisor de los numeros a, a', b + b' es μ, y si se fijan A = μτ, B = b, ξ b' segun los modulos μ, a respectivamente, AC = B2 — D; y esta forma sera propiamente equivalente a la forma F. Ahora bien, el numero aa esta representado por la forma Ax2 + 2Bxy + Cy2, haciendo x = μ, y = 0 cuyo maximo comun divisor es μ; de modo que aa' puede ser tambien representado por la forma F de manera que los valores de las incognitas tengan a μ como su maximo comun divisor (art. 166). Siempre y cuando μ sea 1, aa' puede ser representado por la forma F asignando valores primos entre sí a las incognitas, y esta representation pertenecerá al valor B de la expresion \/D (mod. aa'), la cual es congruente con b y b' segun los modulos a y a' respectivamente. La condition μ = 1 siempre tiene lugar cuando a y a' son primos entre sí; o mas generalmente cuando el maximo comun divisor de a y a' es primo a b + b'.

Composición de ordenes.

245.

TEOREMA. Si la forma f pertenece al mismo orden que g, y f' es del mismo orden que g', entonces la forma F compuesta por f y f tendrá el mismo determinante y sera del mismo orden que la forma G compuesta por g y g'.

Demostración. Sean las formas f, f' y F que son = (a, b, c), (a', b', c') y (A, B, C), respectivamente, y sean sus determinantes = d, d' y D. Seguidamente sea m el maximo comun divisor de los numeros a, 2b y c y sea m el maximo comun divisor de los numeros a, b y c; y que m', m' con respecto a la forma f' y M, M con respecto a la forma F tengan similares significados. Entonces el orden de la forma

f será determinado por los números d, m y m, de donde estos números también serán válidos para la forma g; por la misma razón los números d', m' y m' jugarán el mismo rol para la forma g' como para la forma f'. Ahora bien, por el artículo 235, los números D, M y M están determinados por d, d', m, m', m y m'; esto es, D sera el máximo común divisor de dm'2,d0m2; M = mm'; M = mm' (si m = m y m' = m') o = 2mm' (si m = 2m o m' = 2m'). Dado que estas propiedades de D, M y M se siguen del hecho de que F esta compuesta por f y f', es facil ver que D, M y M juegan la misma función para la forma G, así que G es del mismo orden que F. Q. E. D.

Por esta razón diremos que el orden de la forma F esta compuesto de los ordenes de las formas f y f'. De este modo, p.ej., si tenemos dos ordenes propiamente primitivos, su composicion sera propiamente primitiva; si uno es propiamente primitivo y el otro impropiamente primitivo, la composicion sera impropiamente primitiva. Se debe entender de una manera similar si se dice que un orden esta compuesto de varios otros ordenes.

Composición de géneros.

246.

PROBLEMA. Propuestas dos formas primitivas cualesquiera f y f' y la forma F compuesta de estas dos: determinar el género al cual pertenece F a partir de los generos a los cuales pertenecen f y f'.

Solución. I. Consideremos primero el caso donde al menos una de las formas f o f' (p.ej. la primera) es propiamente primitiva, y designemos los determinantes de las formas f, f' y F por d, d' y D. D sera el maximo comun divisor de los numeros dm'2 y d', donde m' es 1 o 2 segun la forma f' sea propia o impropiamente primitiva. En el primer caso F pertenecerá a un orden propiamente primitivo, en el segundo a un orden impropiamente primitivo. Ahora bien, el genero de la forma F estará definido por sus caracteres particulares, esto es con respecto a los divisores impares primos individuales de D y tambien para algunos casos con respecto a los numeros 4 y 8. Sera conveniente considerar estos casos separadamente.

1. Si p es un divisor impar primo de D, necesariamente dividirá a d ya d', y así tambien entre los caracteres de las formas f y f' se encuentran las relaciones de F con p. Ahora bien, si el numero a puede ser representado por f, y el numero a' por f', el producto aa' puede ser representado por F. Así que si los residuos cuadráticos de p (no divisibles por p) pueden ser representados tanto por f como por f0, ellos pueden ser también representados por F; i.e. si ambos f y f' tienen el carácter Rp, la forma F tendrá el mismo carácter. Por una razón similar F tendrá el carácter Rp si ambos f y f' tienen el carácter Np; contrariamente F tendrá al carácter Np si una de las formas f o f' tiene el carácter Rp y la otra tiene el carácter Np.
2. Si una relación con el nómero 4 entra dentro del carácter total de la forma F, tal relación tambien debe entrar dentro de los caracteres de las formas f y f'. En efecto, esto solo puede pasar cuando D es ξ 0 á ξ 3 (mod. 4). Cuando D es divisible por 4, dm' y d' son tambien divisibles por 4, y es inmediatamente claro que f' no puede ser impropiamante primitiva y así m' = 1. Luego tanto d como d' son divisibles por 4 y una relacion con 4 entrará dentro del carácter de cada cual. Cuando D ξ 3 (mod. 4), D dividirá a d ya d', los cocientes serán cuadrados y así d y d' serán necesariamente ξ 0 á ξ 3 (mod. 4) y una relacion con el námero 4 estará incluida entre los caracteres de f y f'. De este modo, asá como en (1), se seguirá que el carácter de la forma F sera 1, 4 si ambos f y f' tienen el carácter 1, 4 o 3, 4; contrariamente el carácter de la forma F sera 3, 4 si una de las formas f o f' tiene el caráacter 1, 4 y la otra 3, 4.
3. Cuando D es divisible por 8, d' lo sera tambien; de donde f' seguramente sera propiamente primitivo, m' = 1 y d tambien sera divisible por 8. Y asá uno de los caracteres 1, 8; 3, 8; 5, 8; 7, 8 aparecerá entre los caracteres de la forma F solo si tal relacián con 8 aparece tambien en el carácter de ambas formas f y f'. De la misma manera como antes, es fácil ver que 1, 8 será un carácter de la forma F si f y f' tienen el mismo carácter con respecto a 8; que 3, 8 sera un carácter de la forma F si una de las formas f o f' tiene el carácter 1, 8, la otra 3, 8; á una de ellas tiene el carácter 5, 8 y la otra 7, 8; F tendrá el carácter 5, 8 si f y f' tienen 1, 8 y 5, 8 á 3, 8 y 7, 8; y F tendrá el carácter 7, 8 si f y f' tienen ya sea 1, 8 y 7, 8 o 3, 8 y 5, 8 como caracteres.
4. Cuando D ξ 2 (mod. 8), d' sera ξ 0 á ξ 2 (mod. 8), asá que m' = 1 y d sera tambien ξ 0 o ξ 2 (mod. 8); pero dado que D es el máximo comun divisor de d y d', ellos no pueden ser ambos divisibles por 8. Entonces en este caso el carácter de la forma F solo puede ser 1 y 7, 8 o 3 y 5, 8 cuando ambas formas f y f' tienen uno de estos caracteres y el otro tiene uno de los siguientes: 1, 8; 3, 8; 5, 8; 7, 8. La siguiente tabla determinará el carácter de la forma F. El carácter en el margen pertenece a una de las formas f o f', y el carácter en la cabeza de las columnas pertenece a la otra.

|  |  |  |
| --- | --- | --- |
|  | 1 y 7,8 | 3 y5,8 |
|  | o 1,8 | o 3, 8 |
|  | o 7, 8 | o 5, 8 |
| 1 y 7,8 | 1 y 7,8 | 3 y5,8 |
| 3 y 5,8 | 3 y 5,8 | 1 y 7,8 |

1. De la misma manera, puede ser probado que F no puede tener el carácter 1 y 3, 8 ó 5 y 7, 8a no ser que al menos una de las formas f o f0 tenga a uno de estos caracteres. La otra puede tener uno de ellos tambien o uno de estos: 1, 8; 3, 8; 5, 8; 7, 8. El carácter de la forma F esta determinado por la siguiente tabla. Los caracteres de las formas f y f de nuevo aparecen en el margen y en la cabeza de las columnas.

|  |  |  |
| --- | --- | --- |
|  | 1 y 3,8 | 5 y 7,8 |
|  | o 1,8 | o 5, 8 |
|  | o 3, 8 | o 7, 8 |
| 1 y 3,8 | co  00 | 5 y 7,8 |
| 5 y 7,8 | 5 y 7,8 | 1 y 3,8 |

1. Si cada una de las formas f y f es impropiamente primitiva, D sera el maximo comón divisor de los nómeros 4d, 4d0 o sea 4D el móximo comón divisor de los nómeros d, d0. Se sigue que d, d' y 4D serón todos ξ 1 (mod. 4). Poniendo F = (A, B, C), el maximo comón divisor de los nómeros A, B, C será = 2, y el maximo comón divisor de los nómeros A, 2B, C sera 4. Luego F seró una forma derivada de la forma impropiamente primitiva (4A, 4B, 4C), cuyo determinante sera 1D, y su genero determinará el genero de la forma F. Pero, dado que es impropiamente primitiva, su carácter no implicará relaciones con 4 u 8, sino solo con los divisores impares primos individuales de 4D. Ahora todos estos divisores manifiestamente dividen tambien a d ya d', y si los dos factores de un producto son representables uno por f, el otro por f', entonces la mitad del producto es representable por la forma (4A, 4B, 4C). Se sigue que el carácter de esta forma con respecto a cualquier nómero impar primo p que divida a 4 D seró Rp cuando 2Rp y las formas f, f0 tengan el mismo carácter con respecto a p y cuando 2Np y los caracteres de f y f0 con respecto a p son opuestos. Contrariamente el carácter de la forma seró Np cuando f y f0 tengan iguales caracteres con respecto a p y 2Np, y cuando f y f tengan caracteres opuestos y se tiene 2Rp.

247.

De la solución del problema precedente, es manifiesto que si g es una forma primitiva del mismo orden y genero que f, y g0 es una forma primitiva del mismo orden y genero que f0: entonces la forma compuesta por g y g0 sera del mismo genero que la forma compuesta por f y f0. Así se ve lo que significa un género compuesto por dos (o incluso varios) generos. Además, si f y f tienen el mismo determinante, f es una forma del genero principal, y F está compuesta por f y f0: entonces F sera del mismo genero que f0; de ahí que el genero principal puede siempre ser omitido en la composicion de otros generos del mismo determinante. Es así como, siendo otras cosas iguales, si f no esta en el genero principal y f es una forma primitiva, F ciertamente estará en un genero que no es f0. Finalmente, si f y f0 son formas propiamente primitivas del mismo genero, F estará en el genero principal; si, de hecho f y f0 son ambas propiamente primitivas con el mismo determinante pero en distintos generos, F no puede pertenecer al genero principal. Y si una forma propiamente primitiva se compone consigo misma, la forma resultante, la cual tambien sera propiamente primitiva con el mismo determinante, necesariamente pertenecerá al genero principal. [[188]](#footnote-189) forma puede ser determinado por el artículo 246 y dado que F está derivado de la misma manera, su genero será conocido asimismo.

A partir de esta solución es manifiesto que el teorema en el articulo precedente, que ha sido restringido a las formas primitivas, es valido para cualquier forma, a saber: si f y g son de los mismos géneros respectivamente que f y g, la forma compuesta por f y g sera del mismo genero que la forma compuesta por f y g.

Composición de Clases.

249.

TEOREMA. Si las formas f y f son de los mismos ordenes, géneros y clases que g y g' respectivamente, entonces la forma compuesta por f y f' será de la misma clase que la forma compuesta por g y g'.

De este teorema (cuya verdad se sigue inmediatamente del articulo 239) es evidente lo que queremos decir cuando hablamos de una clase compuesta por dos (o mas) clases dadas.

Si cualquier clase K esta compuesta con una clase principal, el resultado será la clase K misma; esto es, en composicion con otras clases del mismo determinante una clase principal puede ser ignorada. De la composicion de dos clases propiamente primitivas opuestas siempre obtendremos una clase principal del mismo determinante (vease articulo 243). Dado que por este motivo cualquier clase ambigua es opuesta a si misma, siempre obtendremos una clase principal del mismo determinante si componemos cualquier clase propiamente primitiva ambigua consigo misma.

El reciproco de la ultima proposicion tambien vale; esto es si de la composicion de una clase K propiamente primitiva consigo misma proviene una clase principal H con el mismo determinante, K necesariamente sera una clase ambigua. Puesto que si K' es una clase opuesta a K, la misma clase surgiri de la composicion de H y K' como de las tres clases K, K y K'; a partir de las ultimas proviene K (dado que K y K' producen a H, y H y K producen a K). De las primeras obtenemos K'; de ahi que K y K0 coinciden y la clase es ambigua.

Ahora se nota la proposiciin siguiente: Si las clases K y L son opuestas a las clases K' y L' respectivamente, la clase compuesta por K y L sera opuesta a la clase compuesta por K0 y L0. Sean f, g, f0 y g0 las formas de las clases K, L, K0 y L0 respectivamente, y sea F compuesta por f y g, y F' compuesta por f' y g'. Dado que f' es impropiamente equivalente a f, y g' impropiamente equivalente a g, mientras que F esti compuesto por ambas f y g directamente: F estari tambien compuesta

por f y g pero con cada una de ellas indirectamente. De este modo cualquier forma que es impropiamente equivalente a F estará compuesta por f y g directamente y así será propiamente equivalente a F' (art. 238, 239). De ahí que F y F' serán impropiamente equivalentes y las clases a las que pertenecen son opuestas.

Sigue de esto que, si se compone una clase ambigua K con una clase ambigua L, siempre se produce una clase ambigua. En efecto, ella sera opuesta a la clase que es compuesta de las clases opuestas a K y L; a saber, a si misma, ya que estas clases son opuestas a sí mismas.

Finalmente observamos que si se proponen dos clases cualesquiera K y L del mismo determinante y la primera es propiamente primitiva, siempre podemos encontrar una clase M con el mismo determinante tal que L este compuesta por M y K. Manifiestamente esto puede hacerse tomando por M la clase que esta compuesta por L y la clase opuesta a K; es facil ver que esta clase es la ánica que disfruta de esta propiedad; es decir, si componemos diferentes clases del mismo determinante con la misma clase propiamente primitiva, se producen distintas clases.

Es conveniente denotar la composicián de clases por el signo de adición, + , y la identidad de clases por el signo de igualdad. Usando estos signos la proposicián recien considerada puede ser enunciada como sigue: Si la clase K' es opuesta a K, K+K0 sera una clase principal del mismo determinante, de modo que K+K0+L = L; si se toma K' + L = M, tenemos K + M = L, como se desea. Ahora, si además de M tenemos otra clase M' con la misma propiedad, esto es K + M' = L, tendremos K+K0+M0 = L+K0 = M y así M' = M. Si muchas clases identicas son compuestas, esto puede indicarse (como en la multiplicacián) prefijando su número, así que 2K significa lo mismo que K + K, 3K lo mismo que K + K + K, etc. Podríamos tambien transferir los mismos signos a formas de tal modo que (a, b, c) + (a0, b0, c0) indicaría a la forma compuesta por (a, b, c) y (a0, b0, c0); pero para evitar ambigüedad preferimos no usar esta abreviaciáon, especialmente puesto que ya habáíamos asignado un significado especial al símbolo \/M(a, b, c). Diremos que la clase 2K surge de la duplicación de la clase K, la clase 3K de la triplicación, etc. [[189]](#footnote-190) positivo) y puede ser correctamente considerada la forma más simple en el orden (justo como (—m, 0, —) sera la más simple en el orden negativo cuando D es negativo). Si además tenemos -2 = 1 (mod. 4), habrá tambien un orden de formas de determinante D derivado del determinante impropiamente primitivo -¾. La forma (2m, m, m2m ) pertenecerá a este y será la más simple en el orden. (Cuando D es negativo, habrá de nuevo dos ordenes y en el orden negativo (—2m, —m, -- ) sera la forma mas simple.) Así, e.g., si aplicamos esto al caso donde m = 1, el siguiente sera el mas simple entre los cuatro ordenes de formas con determinante 45; (1, 0, —45), (2, 1, —22), (3, 0, —15), (6, 3, —6).

Todas estas consideraciones dan lugar a lo siguiente.

PROBLEMA. Dada cualquier forma F del orden O, encontrar una forma propiamente primitiva (positiva) del mismo determinante que produzca F cuando está compuesta con la forma más simple en O.

Solucián. Sea la forma F = (ma, mb, mc) derivada de la forma primitiva f = (a, b, c) de determinante d y supondremos primero que f es propiamente primitiva. Observamos que si a y 2dm no son primos entre sí, ciertamente hay otras formas propiamente equivalentes a (a, b, c) cuyos primeros terminos tienen esta propiedad. Debido al artículo 228, hay numeros primos a 2dm representables por esta forma. Sea tal numero a0 = aa2 + 2baq + cq2 y supondremos (es legítimo hacerlo) que a y γ son primos entre sí. Ahora si escogemos β y δ tales que αδ — βγ = 1, f sera transformada por la sustitución a, β, γ, δ en la forma (a0, b0, c0) que es propiamente equivalente a ella y tiene la propiedad prescrita. Ahora, dado que F y (a'm, b'm, c0m) son propiamente equivalentes es suficiente considerar el caso donde a y 2dm son relativamente primos. Ahora (a, bm, cm2) sera una forma propiamente primitiva del mismo determinante que F (pues si a, 2bm, cm2 tuvieran un divisor común, tambien significar ia que el divide a 2dm = 2b2m — 2acm). Es facil confirmar que F sera transformada en el producto de las formas (m, 0, —dm) y (a, bm, cm2) por la sustitucion 1, 0, —b, —cm; 0, m, a, bm. Note que, a no ser que F sea una forma negativa, (m, 0, —dm) sera la forma mas simple del orden O. Usando el criterio de la cuarta observacion en el artículo 235, se concluye que F esta compuesta por (m, 0, —dm) y (a, bm, cm2). Cuando de todos modos F es una forma negativa, sera transformada por la sustitucion 1, 0, b, —cm; 0, —m, —a, bm en el producto de (—m, 0, dm), la forma mas simple del mismo orden, y la forma positiva (—a, bm, —cm2) y así estará compuesta por estas dos.

Segundo, si f es una forma impropiamente primitiva, se puede suponer que

2a y 2dm son primos entre sí; pues si esta propiedad no es cierta ya, de la forma f se puede encontrar una forma propiamente equivalente a f que tenga la propiedad. De esto se sigue fácilmente que (2a, bm, 2cm2 ) es una forma propiamente primitiva del mismo determinante que F; y es igualmente facil confirmar que F sera transformada en el producto de las formas

(±2m, ±m, ± ^(m — dm)) y (± - a, bm, ±2cm2)

por la sustitución

1. 0, -(1 ^ b), —cm ; 0, ±2m, ± - a, (b + l)m 22

donde los signos inferiores deben ser tomados cuando F es una forma negativa y los signos superiores en caso contrario. Concluimos que F esta compuesta por estas dos formas y la primera es la mas simple de orden O, la ultima es una forma propiamente primitiva (positiva).

251.

PROBLEMA. Dadas dos formas F y f del mismo determinante D y pertene­cientes al mismo orden O: encontrar una forma propiamente primitiva de determi­nante D que produzca a F cuando ésta esté compuesta con f.

Solución. Sea φ la forma mas simple de orden O; F y f formas propiamente primitivas de determinante D que producen a F y f respectivamente cuando estan compuestas con φ; y sea f0 la forma propiamente primitiva que produce a F cuando esta compuesta con f. Entonces la forma F estará compuesta de las tres formas φ, f y f0 o de las dos formas f y f0. Q. E. I.

De ahí que toda clase de un orden dado puede ser considerada como compuesta por cualquier clase dada del mismo orden y otra clase propiamente primitiva del mismo determinante.

Para un determinante dado existe el mismo número de clases  
en cada genero del mismo orden.

252.

TEOREMA. Para un determinante dado existe el mismo numero de clases en cada genero del mismo orden.

Demostración. Suponga que los géneros G y H pertenecen al mismo orden, que G esta compuesta por n clases K, K', K'',...Kn-1 y que L es cualquier clase del genero H. Por el artículo precedente se encuentra una clase propiamente primitiva M del mismo determinante cuya composición con K produce a L, y se designan por L', L'',...Ln-1 a las clases que surgen de la composición de la clase M con K', K'',...Kn-1 respectivamente. Entonces a partir de la óltima observación del artículo 249, se sigue que todas las clases L, L', L'',...Ln-1 son distintas, y por el artículo 248 que todas ellas pertenecen al mismo genero H. Finalmente es facil ver que H no puede contener ninguna otra clase mós que estas, dado que cada clase del genero H puede ser considerada como compuesta por M y otra clase del mismo determinante, y este necesariamente debe ser del genero G. De ahí que H, como G, contendró n clases distintas. Q. E. D.

Se compara el número de clases contenidas en géneros individúales de ordenes distintos.

253.

El teorema precedente supone la identidad del orden y no puede ser extendido a distintos ordenes. Así por ejemplo para el determinante -171 hay 20 clases positivas que son reducidas a cuatro ordenes: en el orden propiamente primitivo hay dos generos y cada cual contiene seis clases; en el orden impropiamente primitivo dos generos tienen cuatro clases, dos en cada cual; en el orden derivado a partir del orden propiamente primitivo de determinante -19 hay sólo un genero que contiene tres clases; finalmente, el orden derivado del orden impropiamente primitivo de determinante -19 tiene un genero con una clase. Lo mismo es cierto para las clases negativas. Es útil, por ende, inquirir sobre el principio general que gobierna la relacion entre el número de clases en ordenes diferentes. Supongase que K y L son dos clases del mismo orden (positivo) O de determinante D, y M es una clase propiamente primitiva del mismo determinante que produce a L cuando estó compuesta con K. Por el articulo 251 tal clase siempre puede ser encontrada. Ahora bien, en algunos casos ocurre que M es la única clase propiamente primitiva con esta propiedad; en otros casos puede existir varias clases propiamente primitivas con esta propiedad. Supongamos en general que hay r clases propiamente primitivas de este tipo M, M', M",...Mr-1 y que cada uno de ellas produce a L cuando estó compuesta con K. Designaremos este conjunto por la letra W. Ahora sea L' otra clase del orden O (distinta de la clase L), y sea N' una clase propiamente primitiva de determinante D la cual resulta en L0 cuando está compuesta con L. Usaremos W0 para designar el conjunto de las clases N0 + M, N0 + M0, N0 + M00, . .. N0 + Mr— (todas estas seran propiamente primitivas y distintas una de la otra). Es fácil ver que K producirá a L0 si esta esta compuesta con cualquier otra clase de W0, y por eso concluimos que W y W0 no tienen clases en común; y cada clase propiamente primitiva que produzca a L0 cuando este compuesta con K esta contenida en W0. De la misma manera, si L00 es otra clase de orden O distinta de L y L0, entonces habrá r formas propiamente primitivas todas distintas una de la otra y de las formas en W y W0, cada una de ellas producirá a L00 cuando este compuesta con K. Lo mismo es cierto para todas las otras clases del orden O. Ahora bien, dado que cualquier clase propiamente primitiva (positiva) de determinante D produce una clase de orden O cuando esta compuesta con K, es claro que si el numero de todas las clases de orden O es n, el numero de todas las clases propiamente primitivas (positivas) del mismo determinante sera rn. De este modo tenemos una regla general: Si denotamos por K y L dos clases cualesquiera de orden O y por r el numero de clases propiamente primitivas distintas pero del mismo determinante, cada una de las cuales produce a L cuando esta compuesta con K, entonces el numero de todas las clases en el orden propiamente primitivo (positivo) sera r veces mayor que el numero de clases de orden

O.

Dado que en el orden O las clases K y L pueden ser escogidas arbitrariamente, es permisible tomar clases identicas y sera particularmente ventajoso escoger aquella clase que contenga a la forma mas simple de este orden. Si, por esta razón, escogemos aquella clase para K y L, la operation se vera reducida a asignar todas las clases propiamente primitivas que producen a K misma cuando esten compuestas con K. Desarrollaremos este metodo en lo que sigue.

254.

TEOREMA. Si F = (A, B, C) es la forma más simple de orden O y de determinante D, y f = (a, b, c) es una forma propiamente primitiva del mismo determinante: entonces el número A2 puede ser representado por esta forma siempre y cuando F resulte de la composición de las formas f y F; y recíprocamente F estará compuesta por sí misma y f si A2 puede ser representada por f.

Demostración. I. Si F es transformada en el producto f F por la sustitucion

p, p, p", p'"; q, q , q" , q'" luego, por el artículo 235, tendremos

A(aq//2 — 2bqq" + cq2) = A3

A2 = aq//2 — 2bqq" + cq2 Q. E. P.

y por ende

1. Presumiremos que A2 puede ser representado por f y designaremos los valores desconocidos por medio de los cuales es hecho esto como q'', —q; esto es, A2 = aq//2 — 2bqq" + cq2. Seguidamente pongase que

q' a — q(b + B) = Ap, — qC = Ap/, q"(b — B) — qc = Ap/

—q"C = Ap", q"a — q(b — B) = Aq/, q/(b + B) — qc = Aq"

Es fácil confirmar que F es transformada en el producto f F por la sustitución p, p/, p", p'" ; q, q/, q", q///. Si los numeros p, p/, etc. son enteros entonces F estaró compuesta por f y F. Ahora, de la descripción de la forma mós simple, B es 0 ó 2A, así que ^ es un entero; de la misma manera es claro que ^ es tambien siempre un entero. De este modo q/ — p, p/, q/// — p" y p/// serán enteros y solo queda probar que p y p" son enteros. Ahora tenemos

2 , 2pqB q2C „2 , 2p//q//B q^C

p + Λ— = a —, p + : = c —

A

A

A

A

Si B = 0 obtenemos

q2c //2 q//2c

p2 = a

■χ, p =c

y así p y p" son enteros; pero si B = 1A tenemos

2 , q2c

p + pq = a — ^,

2

p + p q = c —

q 2C

A

y en este caso tambien p y p" son enteros. De ahí que F estó compuesta por f y F. Q. E. S.

255.

Así, el problema se ve reducido a encontrar todas las clases propiamente primi­tivas de determinante D cuyas formas puedan representar a A2. Manifiestamente A2 puede ser representado por cualquier forma cuyo primer termino es A2 o el cuadrado de un factor de A; recíprocamente si A2 puede ser representado por la forma f, f sera

a2

transformado en una forma cuyo primer termino es — por la sustitución α, β, γ, δ siempre y cuando asignemos ae y Ye, cuyo maximo común divisor es e, como los valores de las incognitas. Esta forma serú propiamente equivalente a la forma f si β y δ son escogidas de tal modo que αδ — βγ = 1. Así resulta claro que en cualquier clase que tenga formas que puedan representar a A2, se puede encontrar formas cuyo primer termino es A2 o el cuadrado de un factor de A. El proceso entero depende entonces de encontrar todas las clases propiamente primitivas de determinante D que contengan formas de este tipo. Hacemos esto del siguiente modo. Sean a, a', a'' etc. todos los divisores (positivos) de A; ahora encuentre todos los valores de la expresiún yJD (mod. a2) entre 0 y a2 — 1 inclusive y llamelos b, b', b'', etc. Haga

b2 D =

a2c,

b'2 - D = a2c',

22  
b — D = a c ,

etc.

y desígnese el conjunto de formas (a2, b, c), (a2, b', c'), etc. por la letra V. Obvi­amente cada clase de determinante D que tenga una forma con primer túermino a2 tambien debe contener alguna forma de V. De un modo similar determinamos todas las formas de determinante D con primer termino a' y segundo termino entre 0 y

o

a' — 1 inclusive y designamos el conjunto con la letra V'; por una construccion similar

o

sea V'' el conjunto de formas similares cuyo primer termino es a'' etc. Ahora elimine de V, V', V'', etc. todas las formas que no sean propiamente primitivas y reduzca el resto a clases. Si hubiera muchas formas que pertenecen a la misma clase, retenga solo una de ellas. De este modo tendremos todas las clases que se buscan, y la razún de este numero con respecto a la unidad serú la misma que la razon del número de todas las clases propiamente primitivas (positivas) con respecto al número de todas las clases en el orden O.

Ejemplo. Sea D = —531 y O el orden positivo derivado a partir del orden propiamente primitivo de determinante -59; su forma mas simple es (6, 3, 90), asú que A = 6. Aquú a, a', a'' y a''' serán 1, 2, 3 y 6, V contendrú a la forma (1, 0, 531), V' contendrú a (4, 1, 133) y (4, 3, 135), V'' a (9, 0, 59), (9, 3, 60) y (9, 6, 63), y V''' a (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35) y (36, 33, 45). Pero de estas doce formas seis deben ser rechazadas, la segunda y la tercera de V'', laprimera, la tercera, la cuarta, y la sexta de V'''. Todas estas son formas derivadas; todas las seis restantes pertenecen a distintas clases. De hecho el numero de clases propiamente primitivas (positivas) de determinante -531 es 18; el número de clases propiamente primitivas (positivas) de determinante -59 (o el número de clases de determinante -531 derivadas de estas) es 3, y así la razón es de 6 a 1.

256.

Esta solucion se harú mús clara por medio de las siguientes observaciones generales.

I. Si el orden O es derivado a partir de un orden propiamente primitivo, A2 dividirú a D; pero si O es impropiamente primitivo o derivado a partir de un orden impropiamente primitivo, A sera par, D serú divisible por 4A2 y el cociente serú = 1 (mod. 4). Así el cuadrado de cualquier divisor de A dividirá a D o al menos a 4D y en el ultimo caso el cociente serú siempre ξ 1 (mod. 4).

II. Si a2 divide a D, todos los valores de la

expresioún

\/ü (mod. a2) que

a

2

*c\*

caen entre 0 y a — 1 serún 0, a, 2a,

— a y así a serú el numero de formas

en V; pero entre ellas habrá súlo tantas formas propiamente primitivas como hayan nuúmeros entre

DD

D

D

„2, a2 ^-, -2 ^... „2 (a 1)

2

a

a

a

que no tengan un divisor común con a. Cuando a = 1, V consistirú de solo una forma (1, 0, — D) que sera siempre propiamente primitiva. Cuando a es 2 o una potencia de 2, la mitad de los a números serú par, la mitad impar; por lo cual habrá 2¡a formas propiamente primitivas en V. Cuando a es cualquier otro número primo p o una potencia del numero primo p, se deben distinguir tres casos: a saber, si D no es divisible por p y no es un residuo cuadrático de p, todos estos a números serán relativamente primos a a de tal modo que todas las formas en V serúan propiamente primitivas; pero si p divide a ^2 habrá formas propiamente primitivas en V;

finalmente si D es un residuo cuadrático de p no divisible por p, habrá ^2)α formas

propiamente primitivas. Todo esto puede ser demostrado sin ninguna dificultad. En general, si a = 2vpnqxrp ... donde p, q, r etc. son números primos impares distintos,

el número de formas propiamente primitivas en V será NPQR..., donde

N = 1 (si ν = 0) o N = 2ν-1 (si ν > 0)

P = pn (si β es un no residuo cuadrútico de p) o

P = (p — 1)pn-1 (si β es divisible por p) o

P = (p — 2)pn-1 (si β es un residuo cuadrútico de p no divisible por p)

y Q, R, etc. serán definidos de la misma manera por q, r, etc. como lo es P por p.

III. Si c2 no divide a D, βτ serú un entero y ξ 1 (mod. 4) y los valores de la expresiún \[D (mod. c2) serán 2c, |c, 5c,.. . c2 — 2c. De ahí que el número de formas en V sera c y habrá tantas propiamente primitivas entre ellas como haya nuúmeros entre

D 1 D 9 D 25

c2 4, c2 4, c2 4 ,

D

c2

(c—2)

2

que son relativamente primos a c. Toda vez que -aj ξ 1 (mod. 8), todos estos números serún pares y así no habrá ninguna forma propiamente primitiva en V; pero cuando (β ξ 5 (mod. 8), todos estos numeros serún impares, de modo que todas las formas en V serán propiamente primitivas si c es 2 o una potencia de 2. En este caso, como una norma general, habrúa tantas formas propiamente primitivas en V como haya números no divisibles por algun divisor primo impar de c. Habra NPQR. . . de ellas si c = 2vpn qxrp .... Aquí N = 2V y P, Q, R, etc. serán derivados a partir de p, q, r, etc. de la misma manera que en el caso precedente.

1. Hemos, por tanto, mostrado cúmo determinar el número de formas propiamente primitivas en V, V0, V00, etc. Podemos encontrar el número total por medio de la siguiente regla general. Si A = 2νAaBeC . .., donde A, B, C, etc. son nuúmeros primos impares distintos, el nuúmero total de todas las formas propiamente primitivas en V, V0, V00, etc. sera = AsnseBCC· donde

n = 1 (si —2 ξ 1 (mod. 8)), o

n = 2 (si es un entero), o

n = 3 (si 42 ξ 5 (mod. 8)); y

a = A (si A divide a —j), o

a = A ± 1 (si A no divide a -—2; el signo superior e inferior se toma de acuerdo a si —2 es un no residuo o un residuo de A)

Finalmente, b, c, etc. serán derivados a partir de B, C, etc. de la misma manera que a a partir de A. La brevedad no nos permite demostrar esto mas completamente.

1. Ahora, con relación al numero de clases que resultan de las formas propiamente primitivas en V, V', V'', etc., debemos distinguir entre los tres casos siguientes.

Primero, cuando D es un número negativo, cada una de las formas propia­mente primitivas en V, V', etc. constituye una clase separada. Por eso el número de clases serú expresado por la formula dada en la observation previa excepto por dos casos, mús exactamente cuando 4A2 es = —4 ú = -3; esto es, cuando D es = —A2 o = — 4A2. Para probar este teorema solamente debemos mostrar que es imposi­ble para dos formas de V, V', V'', etc. distintas, el ser propiamente equivalentes. Supongamos, por tanto, que (h2, i, k), (h' , i', k') son dos formas propiamente prim­itivas de V, V', V'', etc., y ambas pertenecen a la misma clase. Y supongamos que la primera es transformada en la última por medio de la sustituciún propia α, β, γ, δ; obtendremos las ecuaciones

αδ — βγ = 1, h2a2 + 2ίαγ + kγ2 = h'2,

ύ,2αβ + ί(αδ + βγ) + kγδ = i'

De esto es facil concluir, primero, que γ ciertamente no es =0 (y se sigue que α = ±1, h2 = h'2, i' = i (mod. h2), y las formas propuestas son identicas, contrario a la hipotesis); segundo, que γ es divisible por el maximo común divisor de los números h, h' (pues si hacemos este divisor = r, manifiestamente tambien este divide a 2i, 2i' y es relativamente primo a k; ademas, r2 divide a h2k — h' k' = i2 — i' ; obviamente entonces r debe tambien dividir a i — i'; pero ai' — βύ,' = ai + γk de modo que γk y γ tambien serún divisibles por r); tercero, (ah2 + γί)2 — Dj2 = h2h'2. Si de ahí hacemos ah2 + γϊ = rp, γ = rq, p y q serún enteros y q no sera = 0 y tendremos

p2 — Dq2 = h . Pero hrh es el menor número divisible por ambos h2 y h'2 y, por ende, dividira a A2 ya 4D. Como resultado será un entero (negativo). Si lo

hacemos = —e tenemos p2 — Dq2 = — 42 o 4 = (hp)2 + eq2, en esta ecuacion (hp)2 es necesariamente un cuadrado menor que 4 y así serú o 0 ú 1. En el primer caso eq2 = 4 y D = — (p2-)2 y se sigue que ^2 es un cuadrado con signo negativo y, por ello, ciertamente no es ξ 1 (mod. 4) y de ahú que O no es un orden impropiamente primitivo ni derivado de un orden impropiamente primitivo. Asú que ^2 sera un entero, y claramente e serú divisible por 4, q2 = 1, D = — (hh-)2 y A es tambien

un entero. Por esta razón, D = —A2 ó A2 = — 1, que es la primera excepción. En el ultimo caso eq2 = 3 de modo que e = 3 y 4D = —3()2. Así que 3()2 sera

un entero, y no puede ser otra cosa que 3, dado que cuando lo multiplicamos por el entero cuadrado () obtenemos 3. Por todo esto, 4D = —3A2 o D = —3A2 que es la segunda excepcion. En todos los casos restantes todas las formas propiamente primitivas en V, V', V'', etc. pertenecerán a distintas clases. Para los casos de excepcion es suficiente dar el resultado que puede encontrarse sin dificultad, pero es demasiado largo para presentarlo aquí. En el primer caso siempre habrá un par de formas propiamente primitivas en V, V', V'', etc. que pertenecen a la misma clase; en el ultimo caso, habrá una terna. De modo que en el primer caso el numero de clases sera la mitad del valor dado arriba, en el ultimo caso sera un tercio.

Segundo, cuando D es un numero cuadrado positivo, cada forma propiamente primitiva en V, V', V'', etc. constituye una clase separada sin excepcion. Pues, supongamos que (h2, i, k), (h'2, i', k') son dos de tales formas distintas propiamente equivalentes y la primera es transformada en la ultima por medio de la sustitucion propia α, β, γ, δ. Obviamente todos los argumentos que usamos en el caso previo, cuando no supusimos a D negativo, valen aquí. De ahí que si determinamos p, q, r como arriba, ^2^-2 sera un entero aquí tambien, pero positivo en lugar de negativo y mas aun, sera un cuadrado. Si lo hacemos = g2 tendremos (jT’.)2 — g2q2 = 4. Q. E. A. , debido a que la diferencia de dos cuadrados no puede ser 4 a no ser que el menor sea 0; entonces nuestra suposicion es inconsistente.

Tercero, adonde D sea positivo pero no un cuadrado no tenemos aun una regla general para comparar el numero de formas propiamente primitivas en V, V', V'', etc. con el numero de clases diferentes que resultan de ellas. Solo podemos decir que el ultimo o es igual al primero o es un factor de este. Tambien hemos descubierto una conexion entre el cociente de estos numeros y los valores mínimos de t y u que satisfagan la ecuacion t2 — Du2 = A2, pero tomaría mucho explicarla aquí. No podemos decir con certeza si es posible conocer este cociente en todos los casos simplemente inspeccionando los numeros D y A (como en los casos previos). Damos algunos ejemplos y el lector puede anadir algunos suyos. Para D = 13, A = 2 el numero de formas propiamente primitivas en V etc. es 3, todas las cuales son equivalentes y por ende conforman una clase simple; para D = 37, A = 2 tambien habra tres formas propiamente primitivas en V etc. que perteneceran a tres clases diferentes; para D = 588, A = 7 tenemos ocho formas propiamente primitivas en V etc., y ellas conforman cuatro clases; para D = 867, A =17 habrá 18 formas

propiamente primitivas, y el mismo número para D = 1445, A = 17, pero para el primer determinante se dividirán en dos clases mientras que en el segundo habrá seis.

1. De la aplicación de esta teoría general al caso donde O es un orden

impropiamente primitivo, encontramos que el nuámero de clases contenido en este orden posee la misma razán con respecto al número de todas las clases en el orden propiamente primitivo como 1 lo hace con respecto al nuámero de clases propiamente primitivas distintas producido por las tres formas (1, 0, —D), (4, 1, ), (4, 3, ). Ahora, cuando D ξ 1 (mod. 8), habrá sálo una clase

puesto que en este caso la segunda y la tercera formas son impropiamente primitivas; pero cuando D ξ 5 (mod. 8) estas tres formas serán todas propiamente primitivas y producirán el mismo numero de distintas clases si D es negativo excepto cuando D = —3, en cuyo caso habrá solo una; finalmente, cuando D es positivo (de la forma 8n+5) tenemos uno de los casos para el cual no hay regla general. Pero podemos decir que en este caso las tres formas perteneceraán a tres distintas clases o a una sola clase, nunca a dos; pues es fácil ver que si las formas (1, 0, —D), (4, 1, ), (4, 3, )

pertenecen respectivamente a las clases K, K', K'', tendremos K + K' = K', K' + K' = K" y así si K y K' son identicas, K' y K" tambien serán identicas;

similarmente si K y K'' son identicas, K' y K'' tambien lo serán; finalmente, dado que tendremos K' + K'' = K, si suponemos que K' y K'' son identicas, se sigue que K y K' coincidirán. Asá las tres clases K, K', K'' serán o todas distintas o todas identicas. Por ejemplo, hay 75 números de la forma 8n + 5 menores que el número 600. Entre ellos hay 16 determinantes para los cuales el caso anterior se aplica; esto es, el nuámero de clases en el orden propiamente primitivo es de tres multiplicado por el námero de clases en el orden impropiamente primitivo, o sea, 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573; para los otros 59 casos el námero de clases es el mismo en ambos ordenes.

1. Es escasamente necesario observar que el metodo precedente se aplica no sáolo a los nuámeros de clases en oárdenes distintos del mismo determinante, sino tambien a determinantes distintos, siempre que su cociente sea un námero cuadrado. Por tanto si O es un orden de determinante dm2, y O' un orden de determinante dm' , O puede ser comparado con un orden propiamente primitivo de determinante dm2, y este con un orden derivado a partir de un orden propiamente primitivo de determinante d; o, lo que viene a ser lo mismo, respecto al numero de clases, con este ultimo orden en sí; y en una manera similar el orden O' puede ser comparado con este mismo orden.

Sobre el número de clases ambiguas.

257.

Entre todas las clases en un orden dado con determinante dado, las clases ambiguas especialmente demandan un tratamiento mayor, y la determinación del número de clases abre la vía a varios otros resultados interesantes. Es suficiente considerar el número de clases en el orden propiamente primitivo solamente, dado que los otros casos pueden ser facilmente reducidos a este. Haremos esto de la siguiente manera. Primero determinaremos todas las formas propiamente primitivas ambiguas (A, B, C) de determinante D para las cuales ya sea B = 0 ó B = 2A y, entonces, a partir del número de estos podemos encontrar el número de todas las clases propiamente primitivas ambiguas con determinante D.

1. Se encuentran todas las formas propiamente primitivas (A, 0, C) de determinante D, tomando por A a cada divisor de D (ambos positivos y negativos) para el cual C = — es relativamente primo a A. De esta manera cuando D = —1 habrú dos de estas formas: (1, 0, 1), (—1, 0, —1); y el mismo numero cuando D = 1, sean estas (1, 0, —1), (—1, 0, 1); cuando D es un número primo o la potencia de un numero primo (ya sea el signo positivo o negativo), habrá cuatro (1, 0, — D), (—1, 0, D), (D, 0, —1), (—D, 0, 1). En general, cuando D es divisible por n números primos distintos (aquí contamos al numero 2 entre ellos), se darán en total 2n+1 formas de este tipo; es decir si D = ±PQR. . . donde P, Q, R, etc. son numeros primos diferentes o potencias de primos y si su numero = n, los valores de A serán 1, P, Q, R, etc. y los productos de todas las combinaciones de estos numeros. Por la teoría de combinaciones, el numero de estos valores es 2n, pero debe ser doblado dado que cada valor debe ser tomado con un signo positivo y un signo negativo.
2. Similarmente es claro que todas las formas propiamente primitivas (2B, B, C) de determinante D serán obtenidas si por B tomamos todos los divisores (positivos y negativos) de D para los cuales C = 1 (B — BB) es un entero y es relativamente primo a 2B. Dado que de ahí C es necesariamente impar y C2 ξ 1 (mod. 8), a partir de la ecuación D = B2 — 2BC = (B — C)2 — C2 se sigue que D o es ξ 3 (mod. 4) cuando B es impar, o ξ 0 (mod. 8) cuando B es par; toda vez que, por esto, D sea congruente (mod. 8) con alguno de los numeros 1, 2, 4, 5, 6 no habrá ninguna forma de este tipo. Cuando D ξ 3 (mod. 4), C sera un entero e impar, no importa cual divisor de D tomemos por B; pero a razon de que C no tenga un divisor en comun con 2B, debemos escoger a B de tal manera que D y B sean relativamente primos; así para D = —1 tenemos dos formas (2, 1, 1), (—2, —1, —1), y en general si el numero de todos los divisores primos de D es n, habrá

2n+l formas

en total. Cuando D es divisible por 8, C sera un entero si tomamos por B a cualquier divisor par de 1D; en tanto para la otra condición, de que C = 1B — ^B sea relativamente primo a 2B, se satisfacerá primero tomando por B a todos los divisores ξ 2 (mod. 4) de D para los cuales y B no tengan un divisor en común. El número de estos (contando a ambos signos) serú 2n+1 si D es divisible por n números primos impares distintos. Segundo, se toma por B a todos los divisores ξ 0 (mod. 4) de 1D para los cuales ^B y B son relativamente primos. Su número tambien serú 2n+1, de modo que en este caso tendremos 2n+2 formas en total. Por esto, si D = ±2^'PQR. . . donde μ es un exponente mayor que 2, P, Q, R, etc. son nuúmeros primos impares diferentes o potencias de nuúmeros primos, y si el nuúmero de estos es n: entonces tanto para 2¡B como para ^B se pueden tomar todos los valores 1, P, Q, R, etc. y los productos de cualquier numero de estos numeros, cada uno con un signo positivo o un signo negativo.

A raíz de todo esto vemos que si D es divisible por n números impares primos distintos (siendo n = 0 cuando D = ±1 o ±2 o una potencia de 2), el numero de todas las formas propiamente primitivas (A, B, C) para las cuales B es, ya sea 0 o 2A, sera 2n+1 cuando D ξ 1o ξ 5 (mod. 8); sera 2n+2 cuando D ξ 2, 3, 4, 6, o 7 (mod. 8); finalmente sera 2n+3 cuando D ξ 0 (mod. 8). Si comparamos este resultado con lo que encontramos en el artículo 231 con respecto al numero de todos los caracteres posibles de las formas primitivas con determinante D, observamos que el primer numero es precisamente el doble de este en todos los casos. Pero es claro que, cuando D es negativo, habrá tantas formas positivas como negativas entre ellas.

258.

Todas las formas consideradas en el artículo previo pertenecen manifiesta­mente a las clases ambiguas. Por otro lado, al menos una de estas formas debe ser contenida en cada clase ambigua propiamente primitiva de determinante D; pues, ciertamente, hay formas ambiguas en tal clase y toda forma ambigua propiamente primitiva (a, b, c) de determinante D es equivalente a alguna de las formas del artículo anterior, a saber, o

i\*\* — f)

( 1 1 D\

o a, -a, —a

V 2 4 aj segun b sea ξ 0o ξ ^ a (mod. a). De este modo, el problema se reduce a encontrar cuantas clases son determinadas por estas formas.

Si la forma (a, 0, c) aparece entre las formas del artículo precedente, la forma (c, 0, a) tambien aparecerá y ellas serán distintas, excepto cuando a = c = ±1 y luego D = -1, un caso que dejaremos a un lado, por el momento. Ahora, dado que estas formas pertenecen manifiestamente a la misma clase, es suficiente retener una, y rechazaremos aquella cuyo primer termino es mayor que el tercero; tambien dejaremos a un lado el caso donde a = —c = ±1 y D = 1. De esta manera, podemos reducir todas las formas (A, 0, C) a la mitad, reteniendo solo una de cada par; y en aquellas que restan siempre resulta A < V±D.

Similarmente, si la forma (2b, b, c) aparece entre las formas del artículo previo, lo siguiente tambiáen apareceráa

. . í 2D D \

(4c — 2^ 2c — ^ c) = ^——, — —, cj

Estas dos serán propiamente equivalentes, pero diferentes entre sí, excepto en el caso que hemos omitido, donde c = b = ±1 o D = —1. Es suficiente retener aquella, de estas dos formas, cuyo primer termino es menor que el primer termino de la otra (en este caso no pueden ser iguales en magnitud pero diferentes en signo). De modo que todas las formas (2B, B, C) pueden ser reducidas a la mitad, rechazando una de cada par; y en aquellas que quedan siempre tendremos B < BB o B < V±D. De acuerdo con esto, permanece sálo la mitad de todas las formas del artículo previo. Designaremos el conjunto con la letra W, y solo resta mostrar cuantas clases diferentes surgen a partir de estas formas. Manifiestamente, en el caso cuando D es negativo habrá tantas formas positivas en W como negativas.

1. Cuando D es negativo, cada una de las formas en W pertenecerá a una clase distinta. Pues todas las formas (A, 0, C) se verán reducidas; y todas las formas (2B, B, C) serán reducidas, excepto aquellas para las cuales C < 2B; pues en tal forma 2C < 2B + C; luego (dado que B < BB, eso es B < 2C — B, y que 2B < 2C o sea B < C), 2C — 2B < C y C — B < 2¡C y la forma reducida es (C, C — B, C), la cual obviamente es equivalente a esta. De esta manera habrá tantas formas reducidas como formas haya en W, y dado que cualesquiera dos de ellas no serán identicas u opuestas (excepto para el caso donde C — B = 0, en el cual B = C = ±1 y por ende D = 1, que es el caso que habáamos dejado de lado), todas pertenecerán a clases distintas. Así, el numero de todas las clases ambiguas propiamente primitivas de determinante D sera igual al numero de formas en W á a la mitad del numero de formas en el artáculo previo. Con respecto al caso exceptuado, cuando D = —1, ocurre lo mismo por compensación; esto es, hay dos clases; una a la cual pertenecen las formas (1, 0, 1), (2, 1, 1), la otra a la cual pertenecen (-1, 0, -1), (-2, -1, -1). En general, por todo esto, para un determinante negativo, el número de todas las clases ambiguas propiamente primitivas es igual al numero de todos los caracteres asignables de las formas primitivas de este determinante; el número de clases ambiguas propiamente primitivas que son positivas serú la mitad de este.
2. Cuando D es un cuadrado positivo = h2, no es difícil mostrar que cada forma en W pertenece a una clase diferente; pero este problema puede ser resuelto mús simplemente de la siguiente manera. Por el artículo 210, debe haber una forma reducida (a, h, 0) contenida en cada clase ambigua propiamente primitiva de determinante h2, donde a es el valor de la expresión -\/I (mod. 2h), que cae entre 0 y 2h - 1 inclusive. Dado que esto es así, resulta claro que hay tantas clases ambiguas propiamente primitivas de determinante h2 como hay valores para esta expresion. Del artículo 105, el numero de estos valores es 2n, 2n+1 o 2n+2, dependiendo de si h es impar, o ξ 2 (mod. 4) o ξ 0 (mod. 4); esto es, según sea D ξ 1, ξ 4 o ξ 0 (mod. 8) donde n designa al numero de divisores primos impares de h o de D. De este modo, el numero de clases ambiguas propiamente primitivas sera siempre la mitad del nuúmero de formas consideradas en el artúculo previo e igual al nuúmero de formas en W, o sea, el numero de todos los posibles caracteres.
3. Cuando D es un entero positivo no cuadrado, deduciremos, a partir de cada una de las formas (A, B, C) en W a otras formas (A!, B0, C0), tomando a B' ξ B (mod. A), que esta entre los Emites \/D y \/D ^ A (el signo superior o inferior sera usado segun sea A positivo o negativo), y C' = B ; designaremos este conjunto con la letra W0. Manifiestamente, estas formas serán propiamente primitivas y ambiguas de determinante D, todas distintas, y, mas aun, todas seran formas reducidas. Pues cuando A < λ/D, B' sera < \[D y positivo; ademas, B0 > \JD ^ A y A > \JD - B' y luego A, tomado positivamente, cae entre \/D + B0 y \JD - B0. Cuando A > \/D, no se puede tener B = 0 (habíamos rechazado estas formas), pero B debe ser = ^A. De ahí que B0 sera igual, en magnitud, a 2¡A y de signo positivo (pues dado que A < ^/D, ±^ A caerá entre los límites asignados a B0 y sera congruente con B segun el modulo A; así B0 = ±^A). Como resultado B0 < \/D y 2B0 < λ/D + B0, o bien, A < \JD + B0, de tal modo que ±A necesariamente caerá entre los límites -^/D + B0 y yJD - B0. Finalmente W0 contendrá a todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues si (a, b, c) es de esta forma, resultara, ya sea b ξ 0 o b ξ ^a (mod. a). En el primer caso, no se puede tener b < a, ni por esto ultimo a > λ/D, así que la forma (a, 0, -D) ciertamente estará contenida en W y la forma correspondiente (a, b, c) en W0; en el ultimo caso,

ciertamente a < 2\f~D y, por ende, (a, 2a, 4a — D) estará contenida en W y la forma correspondiente (a, b, c) en W'. Así, el námero de formas en W es igual al numero de todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues, dado que cada clase ambigua contiene un par de formas reducidas ambiguas (art. 187, 194), el námero de todas las clases ambiguas propiamente primitivas de determinante D será la mitad del námero de formas en W, o bien, la mitad del nuámero de todos los caracteres posibles.

259.

El námero de clases ambiguas impropiamente primitivas de un determinante D dado es igual al nuámero de ellas propiamente primitivas del mismo determinante. Sea K la clase principal y K0, K00, etc. las restantes clases ambiguas propiamente primitivas del mismo determinante; sea L una clase ambigua impropiamente primitiva del mismo determinante, p. ej. aquella que contiene a la forma (2, 1, 2 — 2D). Si componemos la clase L con K, obtenemos la clase L misma; supongamos que la composición de la clase L con K', K", etc. produce las clases L', L", etc. respectivamente. Manifiestamente, todas ellas pertenecerán al mismo determinante y serán impropiamente primitivas y ambiguas. Es claro que el teorema sera probado tan pronto como probemos que todas las clases L, L', L", etc. son diferentes y que no hay otras clases ambiguas impropiamente primitivas de determinante D ademas de estas. Para este propásito, distinguimos los siguientes casos.

1. Cuando el numero de clases impropiamente primitivas es igual al numero de clases propiamente primitivas, cada una de las primeras resultara de la composicion de la clase L con una clase propiamente primitiva determinada, y así todas las L, L', L", etc. serán diferentes. Si designamos por L a cualquier clase ambigua impropiamente primitiva de determinante D, existirá una clase propiamente primitiva R tal que R + L = L; si R0 es la clase opuesta a R, resultara tambien (dado que las clases L y L son sus propias opuestas) R0 + L = L, de donde necesariamente R y R0 seran identicas, o sea una clase ambigua. Como resultado de esto, R se encontrara entre las clases K, K0, K00, etc. y L entre las clases L, L0, L00, etc.
2. Cuando el numero de clases impropiamente primitivas es un tercio del

námero de clases propiamente primitivas, sea H la clase en la cual aparece la forma (4, 1, ), y H0 aquella en la cual aparece (4, 3, ). H y H0 serán propiamante

primitivas, distintas entre sí y de la clase principal K, y H + H0 = K, 2H = H0, 2H0 = H; y si L es cualquier clase impropiamente primitiva de determinante D que

surge de la composición de L con la clase propiamente primitiva R, también se tendrá L = L + R + H y L = L + R + H0. Además de las tres clases (propiamente primitivas y distintas) R, R + H, R + H0 no hay otras que produzcan a L cuando se componen con L. Dado que, a raíz de esto, si L es ambigua y R0 es opuesta a R, tambien tendremos L + R0 = L, R0 será necesariamente identica a una de las tres clases. Si R0 = R, R sera ambigua; si R0 = R + H, resulta K = R + R0 = 2R + H = 2(R + H0) y, por lo tanto, R + H0 es ambigua; similarmente, si R0 = R + H0, R + H sera ambigua y concluimos que L necesariamente se encuentra entre las clases L, L0, L00, etc. Es facil ver que no puede haber más de una clase ambigua entre las tres clases R, R+H, R+H0; pues si ambas R y R+H fueran ambiguas y, por lo tanto, identicas a sus opuestas R0, R0 + H0, tendríamos R + H = R + H0; la misma conclusion resulta a partir de la suposición de que R y R + H0 son ambiguas; finalmente, si R + H y R + H0 son ambiguas e identicas con sus opuestas R0 + H0 y R0 + H, tendríamos R + H + R0 + H = R0 + H0 + R + H0 y así 2H = 2H0, á bien, H0 = H. Por esta razón, solo habrá una clase ambigua propiamente primitiva que produce a L cuando esta es compuesta con L, y, por lo tanto, todas las L, L0, L00, etc. serán diferentes.

El numero de clases ambiguas en un orden derivado es obviamente igual al námero de clases ambiguas en el orden primitivo a partir del cual es derivado, y así, este numero siempre puede determinarse. [[190]](#footnote-191)

H, H", etc. y R entre k, k/,k//, etc.; por todo esto, estas clases dan una solución completa del problema.

Es evidente que, cuando D es negativo, la mitad de las clases k,k',k", etc. serán positivas, la mitad negativas.

Dado que, a raíz de esto, toda clase propiamente primitiva de determinante D que pueda surgir a partir de la duplicacioón de una clase similar, proviene de la duplicacióon de tantas clases similares como clases ambiguas propiamente primitivas de determinante D hubiere; es claro que, si el nómero de todas las clases propiamente primitivas de determinante D es r, y si el numero de todas las clases ambiguas propiamente primitivas de este determinante es n, entonces el nómero de todas las clases propiamente primitivas del mismo determinante que puede ser producido por la duplicación de una clase similar seró n. La misma fórmula resulta si, para un determinante negativo, r y n designan los correspondientes nuómeros de clases positivas. De este modo, p.ej., para D = -161, el número de todas las clases positivas propiamente primitivas es 16, el numero de clases ambiguas es 4, así que el nómero de clases que pueden surgir a partir de la duplicación de cualquier clase debe ser 4. De hecho, encontramos que todas las clases contenidas en el genero principal esrán provistas de esta propiedad; por esto, la clase principal (1, 0, 161) resulta a partir de la duplication de las cuatro clases ambiguas; (2, 1, 81) a partir de la duplicación de las clases (9, 1, 18), (9, -1, 18), (11, 2, 15), (11, -2, 15); (9, 1, 18) a partir de la duplicación de las clases (3, 1, 54), (6, 1, 27), (5, -2, 33), (10, 3, 17); finalmente (9, -1, 18) duplicando las clases (3, -1, 54), (6, -1, 27), (5, 2, 33), (10, -3, 17).

La mitad de todos los caracteres asignables para un determinante dado no puede  
estar en un género propiamente primitivo (positivo para un determinante negativo).

261.

TEOREMA. La mitad de todos los caracteres asignables para un determinante positivo no cuadrado no puede pertenecer a ningún género propiamente primitivo; si el determinante es negativo, a ningun género propiamente primitivo positivo.

Demostración. Sea m el numero de todos los generos propiamente primitivos (positivos) de determinante D; sea k el nómero de clases contenidas en cada genero, de tal manera que km es el nómero de todas las clases propiamente primitivas (positivas); sea n el nómero de todos los caracteres diferentes asignables a este determinante. Entonces, por el artóculo 258, el nuómero de todas las clases ambiguas propiamente primitivas (positivas) seró 2n; y, por el articulo precedente, el numero de todas

las clases propiamente primitivas que puedan resultar a partir de la duplicación de una clase similar seró · Pero, por el artículo 247, todas estas clases pertenecen al genero principal que contiene a k clases; si, por esta razón, todas las clases del genero principal resultan a partir de la duplication de alguna clase (mostraremos en lo que sigue que esto es siempre cierto), entonces ‘2kp = k, o bien, m = 2n; pero es cierto que no podemos tener > k ni, consecuentemente, m > 2n. Dado

que, por esto, el nuómero de todos los góeneros propiamente primitivos (positivos), ciertamente, no puede ser mayor que la mitad de todos los caracteres asignables, al menos la mitad de ellos no puede corresponder con tales generos. Q. E. D. Nótese, sin embargo, que todavía no se sigue a partir de esto que la mitad de todos los caracteres asignables de hecho corresponden a generos propiamente primitivos (positivos), pero luego estableceremos la validez de esta profunda proposition concerniente al misterio mas recondito de los nómeros.

Dado que, para un determinante negativo hay siempre tantos generos neg­ativos como positivos, manifiestamente, no mas que la mitad de todos los carac­teres asignables pueden pertenecer a los generos propiamente primitivos negativos. Hablaremos de esto y de generos impropiamente primitivos abajo. Finalmente, ob­servamos que el teorema no se aplica a determinantes cuadrados positivos. Por esto, es facil ver que cada carócter asignable corresponde a un genero.

Una segunda demostración del teorema fundamental  
y de los demas teoremas acerca de los residuos -1, +2, -2.

262.

Así pues, en el caso donde solo dos caracteres diferentes pueden ser asignados a un determinante no cuadrado dado D, solo uno corresponderá a un genero propiamente primitivo (positivo) (este tiene que ser el genero principal). El otro no corresponderó a ninguna forma propiamente primitiva (positiva) de ese determinante. Esto ocurre para los determinantes -1, 2, -2, -4, para nómeros positivos primos de la forma 4n +1, para negativos de primos de la forma 4n + 3, para todas las potencias positivas impares de nuómeros primos de la forma 4n + 1, y para potencias pares positivas o impares negativas de números primos de la forma 4n+3. A partir de este principio, podemos desarrollar un nuevo metodo, no solamente para el teorema fundamental, sino tambien para demostrar los otros teoremas de la seccion previa que tengan que ver con los residuos -1, +2, -2. Este metodo sera completamente diferente de aquellos usados en la sección anterior y, de ninguna manera, menos

elegante. Sin embargo, omitiremos la consideración del determinante —4 y de los determinantes que son potencias de nómeros primos, dado que no nos enseñarían nada nuevo.

Para el determinante —1, no hay forma positiva con el carácter 3, 4; para el determinante +2 no hay ninguna con el carócter 3 y 5, 8; para el determinante —2 no habrá forma positiva con el carócter 5 y 7, 8; y para el determinante —p, donde p es un nómero primo de la forma 4n + 3, ninguna forma propiamente primitiva (positiva) tendrá al carácter Np; mientras que para el determinante +p, donde p es un nómero primo de la forma 4n + 1, ninguna forma propiamente primitiva tendrá al carácter Np. De este modo, demostraremos los teoremas de la sección previa de la siguiente manera.

1. —1 es un no residuo de cualquier nómero (positivo) de la forma 4n + 3. Pues si —1 fuera un residuo de tal nuómero A, al tomar — 1 = B2 — AC, (A, B, C) sería una forma positiva de determinante —1 con el carácter 3, 4.
2. —1 es un residuo de cualquier numero primo p de la forma 4n + 1. Pues el carócter de la forma (—1, 0, p), asó como de todas las formas propiamente primitivas de determinante p, sera Rp y, por tanto, — 1Rp.
3. Ambos +2 y —2 son residuos de cualquier nómero primo p de la forma 8n + 1. Pues cualquiera de las formas (8, 1, 1—2), (—8, 1, 2—1), o bien, las formas (8, 3, 9—2), (—8, 3, 2—9) son propiamente primitivas (segun sea n impar o par), y asó su carácter sera Rp; de tal manera que +8Rp, y —8Rp, y tambien 2Rp, y —2Rp.
4. +2 es un no residuo de cualquier número de la forma 8n+3 u 8n+5. Pues si fuera un residuo de tal nómero A, habría una forma (A, B, C) de determinante +2 con el caróacter 3 y 5, 8.
5. Similarmente, —2 es un no residuo de cualquier numero de la forma 8n + 5 u 8n + 7, pues, de otro modo, habría una forma (A, B, C) de determinante —2 con el caróacter 5 y 7, 8.
6. —2 es un residuo de cualquier nómero primo p de la forma 8n + 3. Se muestra esta proposicion por dos metodos. Primero, dado que, por IV, +2Np y, por I, — 1Np, necesariamente tenemos —2Rp. La segunda demostracion comienza con una consideracion del determinante +2p. A raóz de este, cuatro caracteres son asignables, y son estos Rp, 1 y 3, 8; Rp, 5 y 7, 8; Np, 1 y 3, 8; Np, 5 y 7, 8. De estos, al menos dos no corresponden a ningun genero. Ahora bien, la forma (1, 0, — 2p) estará de acuerdo con el primer carácter; la forma (—1, 0, 2p) con el cuarto; de ahí que el segundo y el tercero deben ser rechazados. Y dado que el carácter de la forma

(p, 0, -2) relativo al número 8 es 1 y 3, 8, su carácter relativo a p debe ser Rp, y así —2 Rp.

1. +2 es un residuo de cualquier número primo p de la forma 8n + 7. Esto

puede ser mostrado por dos metodos. Primero, dado que, por I y V, — 1Np, —2Np, tendrú +2Rp. Segundo, dado que, ya sea (8, 1, ) o (8, 3, ) es una forma

propiamente primitiva de determinante —p (dependiendo de si n es par o impar), su carúcter sera Rp y, por lo tanto, 8Rp y 2Rp.

1. Cualquier número primo p de la forma 4n + 1 es un no residuo de cualquier numero impar q que sea un no residuo de p. Pues, claramente, si p fuera un residuo de q, habría una forma propiamente primitiva de determinante p con el carácter Np.
2. Similarmente, si un número impar q es un no residuo de un número primo p de la forma 4n + 3, —p sera un no residuo de q; de cualquier otra manera, habría una forma propiamente primitiva de determinante —p con el carácter Np.
3. Cualquier nuúmero primo p de la forma 4n + 1 es un residuo de cualquier otro número primo q que sea un residuo de p. Si q es tambien de la forma 4n + 1, esto se sigue inmediatamente a partir de VIII; pero si q es de la forma 4n + 3, —q serú tambien un residuo de p (por II) y, asú, pRq (por IX).
4. Si un número primo q es un residuo de otro número primo p de la forma 4n + 3, —p serú un residuo de q. Pues si q es de la forma 4n + 1, se sigue inmediatamente, a partir de VIII, que pRq y, asú, (por II) —pRq; este metodo no funciona cuando q es de la forma 4n + 3, pero puede ser fúcilmente resuelto considerando al determinante +pq. Pues, dado que, de los cuatro caracteres asignables para este determinante Rp, Rq; Rp, Nq; Np, Rq; Np, Nq, dos de ellos no pueden corresponder a cualquier gúenero y, dado que los caracteres de las formas (1, 0, —pq) y (—1, 0, pq) son el primero y el cuarto, respectivamente, entonces el segundo y el tercero son los caracteres que no corresponden a ninguna forma propiamente primitiva de determinante pq. Y, dado que, por hipútesis, el carácter de la forma (q, 0, —p) con respecto al número p es Rp, su carácter con respecto al número q debe ser Rq y, por ende, —pRq. Q. E. D.

Si en las proposiciones VIII y IX se supone que q es un nuúmero primo, estas proposiciones, junto con X y IX, nos darún el teorema fundamental de la secciún previa.

Se determina más exactamente la mitad de los caracteres  
que no pueden corresponder a ningún género.

263.

Ahora que hemos dado una nueva prueba del teorema fundamental, mostramos como distinguir a la mitad de los caracteres de un determinante no cuadrado dado que no puedan corresponder a ninguna de las formas propiamente primitivas (positivas). Podemos tratar esto más brevemente, dado que la base para nuestra discusión esta ya contenida en los artículos 147-150. Sea e2 el mayor cuadrado que divide al determinante dado D, y sea D = D'e2, de tal modo que D' no incluye ningán factor cuadrado. Más aán, sean a, b, c, etc. todos los divisores impares primos de D'. De manera que D', excepto quizás por su signo, será un producto de estos numeros o el doble de este producto. Desígnese por Ω el conjunto de caracteres particulares Na, Nb, Nc, etc., tomado por sí mismo cuando D' ξ 1 (mod. 4); tomado junto con el carácter añadido 3, 4 cuando D' ξ 3 y e es impar o ξ 2 (mod. 4); tomado junto con 3, 8 y 7, 8 cuando D' ξ 3 y e ξ 0 (mod. 4); tomado ya sea junto con el carácter 3 y 5, 8 cuando D' ξ 2 (mod. 8) y e es impar, o bien con los dos caracteres 3, 8 y 5, 8 cuando e es par; finalmente tomado ya sea junto con el carácter 5 y 7, 8 cuando D' ξ 6 (mod. 8) y e es impar o con los dos caracteres 5, 8 y 7, 8 cuando e es par. Hecho esto, ningun genero propiamente primitivo (positivo) de determinante D puede corresponder a ninguán caráacter completo que contenga un nuámero impar de caracteres particulares Ω. En cada caso, los caracteres particulares, los cuales expresan una relacioán con aquellos divisores de D que no dividen a D , no contribuyen en nada a la posibilidad o imposibilidad de los generos. A partir de la teoría de combinaciones, sin embargo, es fácil ver que, de esta manera, la mitad de todos los caracteres completos asignables están excluidos.

Demostramos esto de la siguiente manera. Por los principios de la seccioán previa, o por los teoremas que reciáen hemos demostrado en el artáculo precedente, es claro que si p es un numero primo (impar positivo) que no divide a D y que posee a uno de los caracteres rechazados correspondientes a este, D' involucrara a un námero impar de factores que son no residuos de p. De ahí que D' y D tambien serán no residuos de p. Mas aun, el producto de numeros impares relativamente primos a D, ninguno de los cuales corresponde a alguno de los caracteres rechazados, no puede corresponder a un carácter cualquiera como tal. Y, recíprocamente, cualquier numero impar positivo relativamente primo a D, que corresponda con uno de los caracteres rechazados, ciertamente implica algun factor primo de la misma calidad. Si, por este motivo, se da una forma propiamente primitiva (positiva) de determinante D correspondiente a uno de los caracteres rechazados, D sería un no residuo de algún número impar positivo relativamente primo a este y representable por tal forma. Pero esto es evidentemente inconsistente con el teorema del artículo 154.

Las clasificaciones en los artículos 231 y 232 dan buenos ejemplos de esto, y el lector puede aumentar su número a su gusto.

264.

De este modo, dado un determinante no cuadrado, todos los caracteres asignables estarún equitativamente distribuidos en dos tipos, P y Q, de tal manera que ninguna forma propiamente primitiva (positiva) puede corresponder a uno de los caracteres Q. En tanto para los caracteres P, de lo que sabemos hasta el momento, no hay nada que les impida el pertenecer a formas de esta especie. Se nota especialmente la siguiente proposiciún concerniente a estos tipos de caracteres, la cual puede ser fúcilmente deducida a partir de los criterios concernientes a ellos. Si se compone un carácter de P con un carácter de Q (como en el articulo 246, si el carúcter de Q tambien correspondiera a un genero) se producirú un carúcter de Q; pero si se componen dos caracteres de P o dos de Q, el carácter resultante pertenecerú a P. Con la ayuda de este teorema, se puede excluir tambien a la mitad de todos los caracteres asignables para gúeneros negativos e impropiamente primitivos de la siguiente manera.

I. Para un determinante negativo D, los generos negativos serán contrarios a los generos positivos en el sentido de que ninguno de los caracteres de P pertenecerú a un gúenero negativo propiamente primitivo, pero todos esos gúeneros tendraún caracteres de Q. Pues cuando D' = 1 (mod. 4), —D0 sera un numero positivo de la forma 4n+3, y asú, entre los números a, b, c, etc. habrá un número impar de la forma 4n + 3 y — 1 serú un no residuo de cada uno de ellos. Se sigue en este caso que el carácter completo de la forma (—1, 0, D) incluirá un número impar de caracteres particulares de Ω y asú pertenecerú a Q; cuando D0 ξ 3 (mod. 4), por una razón similar, entre los numeros a, b, c, etc. habrá, o bien ningún número de la forma 4n + 3, o bien dos o cuatro, etc. Y, dado que en este caso 3, 4 o 3, 8 o 7, 8 ocurrirán entre los caracteres particulares de la forma (—1, 0, D), es claro que el carácter completo de esta forma tambien pertenecerá a Q. Se obtiene la misma conclusión con igual facilidad para los casos restantes de tal modo que la forma negativa (—1, 0, D) siempre tendrá un carúacter de Q. Pero dado que esta forma compuesta con cualquier otra forma negativa propiamente primitiva del mismo determinante producirúa una forma positiva similar,

es claro que ninguna forma propiamente primitiva negativa puede tener un carácter de P.

1. Se puede probar, de la misma manera, que los generos impropiamente

primitivos (positivos) tienen, ya sea, la misma propiedad o la opuesta de los generos propiamente primitivos, dependiendo de si D ξ 1o ξ 5 (mod. 8). Pues en el primer caso tambien tendremos D0 ξ 1 (mod. 8), y se concluye que, entre los námeros a, b, c, etc., o bien no habrá numeros de la forma 8n + 3 y 8n + 5, o bien dos de ellos, o cuatro, etc. (esto es, el producto de cualquier námero de enteros impares que incluya a un námero impar de enteros de la forma 8n + 3 y 8n + 5, será siempre ξ 3 o ξ 5 (mod. 8), y el producto de todos los námeros a, b, c, etc. sera igual a D0 o a —D0): de este modo, el carácter completo de la forma (2, 1, ) no involucrará a ningun

carácter particular de Ω, o bien involucrará a dos o a cuatro, etc. y así pertenecerá a P. Ahora bien, dado que cualquier forma impropiamente primitiva (positiva) de determinante D puede ser considerada como si estuviera compuesta por (2, 1, )

y por una forma propiamente primitiva (positiva) del mismo determinante, es obvio que ninguna forma impropiamente primitiva (positiva) puede tener a uno de los caracteres de Q en este caso. En el otro caso, cuando D ξ 5 (mod. 8), sucede lo contrario, esto es D0, el cual tambien será ξ 5, ciertamente involucrará un numero impar de factores de la forma 8n + 3 y 8n + 5. De este modo, el carácter de la forma (2, 1, ), y tambien el carácter de cualquier forma impropiamente primitiva

(positiva) de determinante D pertenecerá a Q y ningún genero propiamente primitivo positivo puede tener a un caráacter en P.

1. Finalmente, para un determinante negativo, los generos negativos impropiamente primitivos son, de nuevo, contrarios a los gáeneros impropiamente primitivos. Ellos no pueden tener un carácter que pertenezca a P o a Q, dependiendo a si D ξ 1o ξ 5 (mod. 8), o bien, dependiendo de si —D es de la forma 8n + 7 u 8n + 3. Se deduce esto del hecho de que si componemos la forma (—1, 0, D), cuyo carácter está en Q, con formas negativas impropiamente primitivas del mismo determinante, obtenemos formas positivas impropiamente primitivas. De este modo, cuando los caracteres de Q son excluidos de estas, los caracteres de P deben tambien ser excluidos, y recíprocamente.

Un método especial para descomponer primos en dos cuadrados.

265.

Todo lo anterior esta basado en las consideraciones de los artículos 257 y

258, concernientes al número de clases ambiguas. Hay muchas otras conclusiones muy dignas de atención, las cuales, para ser breve omitiremos, pero no podemos pasar sobre la siguiente, que es significativa por su elegancia. Para un determinante positivo p, que es un numero primo de la forma 4n + 1, hemos mostrado que solo hay una clase ambigua propiamente primitiva. Así pues, todas las formas ambiguas propiamente primitivas de este determinante serán propiamente equivalentes. Si, por este motivo, b es el entero positivo inmediatemente menor que y/p y p — b2 = a', las formas (1, b, —a'), (—1, b, a') serán propiamente equivalentes y, dado que ambas son formas reducidas, una estará contenida en el período de la otra. Si se asigna el índice 0 a la primera forma en su período, el índice de la última necesariamente serú impar (dado que los primeros terminos de estas dos formas tienen signos opuestos); supongase, por tanto, que este índice es = 2m + 1. Es fúcil ver que, si las formas de índices 1, 2, 3, etc. son respectivamente

(—a , b , a ), (a , b , —a ), (—a , b , a ), etc.,

las siguientes formas corresponderán a los índices 2m, 2m — 1, 2m — 2, 2m — 3, etc., respectivamente:

*(a , b, —* ^

*í* **////** *-un ttt\ ±*

*(—a , b , a* ), etc.

(—a", b', a'),

*í !!! -Ut H\*

*(a , b , —a* ),

Así, si la forma de índice m es (A, B, C), (—C, B, —A) sera la misma y, por ende, C = —A y p = B2 + A2. Por esta razín, cualquier nímero primo de la forma 4n + 1 puede ser descompuesto en dos cuadrados (deducimos esta proposicion a partir de principios enteramente diferentes en el artículo 182). Y podemos encontrar esta descomposicion por un metodo muy simple y completamente uniforme; esto es, mediante el computo del período de la forma reducida cuyo determinante es aquel nímero primo y cuyo primer termino es 1, hacia una forma cuyos terminos exteriores son iguales en magnitud pero opuestos en signo. Entonces, p.ej., para p = 233 tenemos (1, 15, —8), (—8, 9, 19), (19, 10, —7), (—7, 11, 16), (16, 5, —13), (—13, 8, 13) y 233 = 64 + 169. Es claro que A es necesariamente impar (dado que (A, B, —A) debe ser una forma propiamente primitiva) y que B es par. Dado que, para el determinante positivo p, el cual es un nímero primo de la forma 4n+1, sílo una clase ambigua esta contenida en el orden impropiamente primitivo, es claro que, si g es el numero impar inmediatamente menor que y/p y p — g2 = 4h, las formas reducidas impropiamente primitivas (2, g, — 2h), (—2, g, 2h) serán propiamente equivalentes

y, por tanto, una estará contenida en el período de la otra. Así pues, por un razonamiento similar, se concluye que se puede encontrar una forma en el período de la forma (2, g, — 2h), la cual tiene terminos exteriores de igual magnitud y signo opuesto. De este modo, podemos descomponer el número p en dos cuadrados. Los terminos exteriores de esta forma serán pares, el de la mitad sera impar; y dado que se sabe que un numero primo puede ser descompuesto en dos cuadrados de solo una manera, la forma que encontramos por este metodo sera (B, ±A, —B) o (-B, ±A, B). Por eso, en nuestro ejemplo para p = 233 tendremos (2, 15, —4), (—4, 13, 16), (16, 3, —14), (—14, 11, 8), (8, 13, —8) y 233 = 169 + 64, como arriba.

UNA DIGRESION CONTENIENDO UN ESTUDIO DE FORMAS TERNARIAS.

266.

Hasta aquí hemos restringido nuestra discusión a funciones de segundo grado con dos incognitas y no había necesidad de darles a ellas un nombre especial. Pero, evidentemente, este tema es solo una seccion del tratado general concerniente a las funciones algebraicas racionales enteras y homogéneas con varias incognitas y de varios grados. Tales funciones, segun su exponente, pueden ser apropiadamente divididas en formas de segundo, tercero, cuarto grado, etc., y, segun su numero de incognitas, en formas binarias, ternarias, cuaternarias, etc. De este modo, las formas que hemos venido considerando pueden ser llamadas simplemente formas binarias de segundo grado. Pero las funciones como

Ax2 + 2Bxy + Cy2 + 2Dxz + 2Eyz + Fz2

(donde A, B, C, D, E y F son enteros) son llamadas formas ternarias de segundo grado, y así sucesivamente. Hemos dedicado la presente seccion al tratamiento de formas binarias de segundo grado. Pero hay muchas verdades bellas concernientes a estas formas cuya fuente real se indaga en la teoría de formas ternarias de segundo grado. Haremos, por tanto, una breve digresion dentro de esta teoría y trataremos especialmente de aquellos elementos que son necesarios para completar la teoría de las forma binarias, esperando, gracias a esto, complacer a los geometras quienes se desilusionarían si ignoramos esta parte o la traráramos de una manera menos natural. Debemos, sin embargo, reservar un tratamiento mas exacto de este importante tema para otra ocasion porque su utilidad sobradamente excede los límites de este trabajo y porque, con esa esperanza, seríamos capaces de enriquecer la discusion con un

desarrollo más profundo más adelante. En este momento excluiremos completamente de la discusión a las formas cuaternarias, quinarias, etc. y a todas las formas de grados mas altos[[191]](#footnote-192)). Es suficiente dirigir este ancho campo a la atencion de los geometras. Hay material amplio para el ejercicio de su genio, y la Aritmetica trascendental seguramente se beneficiara con sus esfuerzos.

267.

Sera de gran ventaja para nuestro entendimiento establecer un orden fijo para los valores desconocidos de la forma ternaria, justo como lo hicimos para formas binarias, de tal manera que podamos distinguir las incógnitas primera, segunda y tercera entre sí. Al disponer las distintas partes de una forma siempre observaremos el siguiente orden; fijaremos, en primer lugar, el termino que involucra el cuadrado de la primera incognita, luego el termino que involucra el cuadrado de la segunda incógnita, el cuadrado de la tercera incógnita, el doble producto de la segunda por la tercera, el doble producto de la primera por la tercera, y luego el doble producto de la primera por la segunda. Finalmente, llamamos a los enteros por los cuales estos cuadrados y doble productos estan multiplicados, en el mismo orden, los coefi cientes primero, segundó, tercero, cuarto, quintó, y sexto. De este modo,

ax + a x + a x + 2bx x + 2b xx + 2b xx

sera una forma ternaria correctamente ordenada. La primera incógnita es x, la segunda x', la tercera x". El primer coeficiente es a etc., el cuarto es b etc. Pero, dado que contribuye mucho a la brevedad, si no es siempre necesario denotar las incóognitas de una forma ternaria por letras especiales, tambien designaremos tal forma por

í a, a', a"\

U b', b'' J

Poniendo

1. 2 2

b — a a = A, b — aa = A , b — aa = A

ab — b'b" = B, a'b' — bb'' = B', a'b'' — bb' = B'

í aD, a'D, a'D! bD, b D, b D .

obtendremos otra forma

*(A, A', A"* yB, B', *B"*

a la que llamamos la adjunta de la forma

*(a,* a', *a"\*

U *b', b"j*

*F*

*f.*

De nuevo, si denotamos por brevedad al número

ab2 + a'b'2 + a''b''2 - add' - 2bb'b'' por D,

tendremos

B2 - A'A'' = aD, B'2 - AA'' = a'D,

AB - B'B'' = bD, A'B' - BB'' = b'D,

B''2 - AA' = a''D A'B'' - BB' = b'D

y es obvio que la adjunta de

la forma F sera la forma

Las propiedades de la forma ternaria f dependen, primero, de la naturaleza del número D. Lo llamaremos el determinante de esta forma. De la misma manera, el determinante de la forma F serú = D2, esto es, igual al cuadrado del determinante de la forma f, de la cual es adjunta.

Así, p.ej., la adjunta de la forma ternaria

/29,

U

13,

-1,

9

14

es

-68,

217,

260,

111,

181

133

y el determinante de cada una es = 1.

Excluiremos enteramente de nuestra siguiente investigaciún a las formas ternarias de determinante 0. Mostraremos en otro momento, cuando tratemos mús completamente la teoría de formas ternarias, que estas son formas ternarias solo en apariencia. Ellas son de hecho equivalentes a formas binarias.

268.

Si una forma ternaria f de determinante D y con incógnitas x, x0, x" (la primera = x etc.) es transformada en una forma ternaria g de determinante E e incognitas y, y0, y00 por medio de una sustitución tal como esta

x = ay + βy0 + yy00 x0 = a'y + β 0y0 + y0y00 x00 = a00 y + e00y0 + y00 y00

donde los nueve coeficientes a, β, etc. son todos enteros, entonces por brevedad, ignoraremos las incognitas y diremos simplemente que f es transformada en g por medio de la sustitución (S)

y que f implica a g o bien que g esta contenida en f. A partir de esta suposición se seguiróan seis ecuaciones para los seis coeficientes en g, pero es innecesario transcribirlas aquí. Y a partir de estas, resultan las siguientes conclusiones:

|  |  |  |
| --- | --- | --- |
| a, | β, | y |
| a0, | β0, | y0 |
| a00, | β00, | y00 |

1. Si por brevedad denotamos al nómero

0///,0///, / *off of* n r *off* o r n ¡

αβ y + βγ a + ya β — yβ a — ay β — βα y por k

encontramos, luego del calculo adecuado, que E = k2D. De este modo, D divide a E y el cociente es un cuadrado. Es claro que, con respecto a las transformaciones de formas ternarias, el nómero k es similar al nómero aó — βy del artículo 157 con respecto a las transformaciones de formas binarias, a saber, la raíz cuadrada del cociente de los determinantes. Podemos conjeturar que, en este caso, una diferencia del signo de k indica una diferencia esencial entre transformaciones propias e impropias y sus implicaciones. Pero si examinamos la situación mas de cerca, vemos que f es transformada en g por medio de esta sustitucioón tambióen

|  |  |  |
| --- | --- | --- |
| —a, | —β, | —y |
| — a0, | —β0, | —y0 |
| — a00, | —β00, | —y00 |

En la ecuacion para k, poniendo —a por a, —β por β, etc., obtendremos —k. De esta manera, esta sustitucion sería similar a la sustitución S y cualquier forma ternaria

que implique a otra de una manera, también implicaría la misma forma de la otra manera. Así que abandonaremos enteramente esta distinción, dado que no es de ningUn uso para formas ternarias.

1. Si denotamos por F y G las formas que son adjuntas a f ya g respectivamente, los coeficientes en F estarán determinados por los coeficientes en f, los coeficientes en G por los valores de los coeficientes de la forma g a partir de la ecuación que es proveída por la sustitución S. Si expresamos los coeficientes de la forma f por letras y comparamos los valores de los coeficientes de las formas F y G, es facil ver que F implica a G y que es transformada en G por medio de la sustitución (S')

nf ft off f f ff ff f / oft ft nt

β γ — β γ , γ α — γ α , α β — α β β "γ — βγ", γ "α — γ α", α"β — αβ"

βγ' — β' γ, γ α — γ' α, αβ' — α β.

Dado que el calculo no presenta ninguna dificultad, no lo escribiremos. III. Por medio de la sustitucion (S'')

|  |  |  |  |
| --- | --- | --- | --- |
| nf ff  βγ | off f  — β γ , | β" γ — βγ'', | βγ' — β'γ |
| r ff | ff f | ff ff | f f |
| γα | — Ί α, | γ α — γα , | γα — γ α |
| f off  αβ | ff Qf  — α β , | α' β — αβ", | αβ' — α β |

g seróa transformada en la misma forma que f por medio de la sustitucioón

|  |  |  |
| --- | --- | --- |
| k, | 0, | 0 |
| 0, | k, | 0 |
| 0, | 0, | k |

Esta es la forma que surge de multiplicar cada uno de los coeficientes de la forma f por k2. Designaremos esta forma por f'.

1. Exactamente de la misma manera, probamos que, por medio de la sustitucióon (S )

|  |  |  |
| --- | --- | --- |
| α, | α , | α |
| β, | β , | β |
| γ, | γ , | γ |

la forma G seraó transformada en la forma que surge a partir de F, multiplicando cada coeficiente por k2. Designaremos esta forma por F'.

Diremos que la sustitución S''' surge a partir de la transposición de la susti­tución S, y, manifiestamente, obtendremos S de nuevo a partir de la transposición de la sustitución S'''; de la misma manera, cada una de las sustituciones S', S'' se produce de la transposición de la otra. Podemos llamar a la sustitucion S' como la adjunta de la sustitución S, y la sustitución S'' seró la adjunta de la sustitución S'''.

269.

Si la forma f implica a g y g tambien implica a f, entonces f y g se llaman formas equivalentes. En este caso D divide a E, pero E tambien divide a D y así D = E. En el sentido contrario, si la forma f implica a una forma g del mismo determinante, estas formas serón equivalentes. Pues (si usamos los mismos símbolos del artóculo previo excepto por el caso cuando D = 0) tenemos k = ±1 y asó la forma f', en la cual g es transformada por medio de la sustitución S'', es identica a f y f estó contenida en g. Mas aún, en este caso las formas F y G, las cuales son adjuntas a f ya g, serán equivalentes entre só, y la ultima sera transformada en la primera por medio de la sustitucion S'''. Finalmente, en el sentido contrario, si se supone que las formas F y G son equivalentes y que la primera es transformada en la segunda por medio de la sustitucion T, las formas f y g tambien serán equivalentes, y f sera transformada en g por medio de la sustitucion adjunta a T y g en f por medio de la sustitución que surge de la transposición de la sustitución T. Pues, por estas dos sustituciones, respectivamente, la forma adjunta a F seraó transformada en la forma adjunta a G y viceversa. Estas dos formas, sin embargo, vienen de f y de g al multiplicar todos los coeficientes por D; asó que se concluye que f es transformada en g y g en f, respectivamente, por estas mismas sustituciones.

270.

Si la forma ternaria f implica a la forma ternaria f0 y f0 implica a la forma f00, entonces f tambien implicaró a f''. Pues es facil observar que si f es transformada en f0 por medio de la sustitucióon

|  |  |  |
| --- | --- | --- |
| a, | β, | γ |
| a', | β', | γ' |
| a", | β'', | γ'' |

y f en f'' por medio de la sustitución

|  |  |  |
| --- | --- | --- |
| δ, | ε, | Ζ |
| δ , |  | Ζ |
| δ , | ε'', | Ζ |

entonces f sera transformada en f'' por medio de la sustitución

αδ + βδ' + γδ' α'δ + β'δ' + γ'δ'' α δ + β δ + γ δ ,

αε + βε' + γε'', α'ε + β'ε' + γ'ε'', αε + βε + γε

αΖ + βΖ' + γΖ'' α'Ζ + β'ζ' + γ'Ζ'' α''Ζ + β''Ζ' + γ''Ζ''

Y en el caso donde f es equivalente a f' y f' a f'', la forma f tambien sera equivalente a la forma f''. Es inmediatamente obvio cómo estos teoremas funcionan con una serie de varias formas.

271.

Es aparente, a partir de lo que hemos visto, que las formas ternarias, al igual que las binarias, pueden ser distribuidas en clases, asignando formas equivalentes a la misma clase y formas no-equivalentes a clases diferentes. Las formas con determinantes diferentes, ciertamente por lo anterior, perteneceraón a clases diferentes y, por tanto, habrá un numero infinito de clases de formas ternarias. Las formas ternarias de un mismo determinante a veces producen un nuómero grande de clases y a veces un nómero pequeno, pero es una propiedad importante de estas formas el que todas las formas de un mismo determinante dado siempre constituyen un número finito de clases. Antes de que discutamos este teorema importante en detalle, debemos explicar la siguiente diferencia esencial que se obtiene entre formas ternarias.

Ciertas formas ternarias estón de tal manera construidas que pueden repre­sentar indistintamente nómeros positivos y negativos, p.ej. la forma x2 + y2 — z2. Se llamarón entonces formas indefinidas. Por otro lado, hay formas que no pueden representar a números negativos sino (excepto por el cero, el cual se obtiene haciendo cada incognita = 0) solamente nómeros positivos, p.ej. x2 + y2 + z2. Se llamarón formas positivas. Finalmente hay otras que no pueden representar nómeros positivos, p.ej. —x2 — y2 — z2. Estas serán llamadas formas negativas. Las formas positivas y negativas son ambas llamadas formas definidas. Ahora daremos un criterio general para determinar como distinguir estas propiedades de las formas.

Si se multiplica la forma ternaria

f = ax2 + a'x'2 + a'' x''2 + 2bx'x'' + 2b' xx" + 2b" xx'

de determinante D por a, y si los coeficientes de la forma que es adjunta a f se denotan como en el artículo 267 por A, A', A'', B, B', B'', tenemos

(ax + b''x' + b'x'')2 — A''x'2 + 2Bx'x'' — A'x''2 = g

y, multiplicando por A', obtenemos

A'(ax + b''x' + b'x'')2 — (A'x'' — Bx' )2 + aDx 2 = h.

Si ambos A' y aD son numeros negativos, todos los valores de h serán negativos, y evidentemente la forma f puede representar solo números cuyo signo es opuesto al de aA', v.g., identicos al signo de a u opuestos al signo de D. En este caso, f sera una forma definida y sera positiva o negativa, dependiendo de si a es positivo o negativo, o bien, según sea D negativo o positivo.

Pero si aD, A son ambos positivos, o bien, uno es positivo y el otro negativo (ninguno =0), h puede producir, ya sea, cantidades positivas o negativas mediante una escogencia adecuada de x, x' y x''. Así pues, en este caso f puede producir valores tanto del mismo signo como del signo opuesto a aA', y sera una forma indefinida. Para el caso donde A' = 0 pero a no es =0, tenemos

g = (ax + b'x' + b'x")2 — x' (A''x' — 2Bx'').

Dúndole a x' un valor arbitrario (diferente de 0) y tomando x'' de tal manera que

4^ x'' tenga el mismo signo que Bx' (esto puede lograrse dado que B no puede

ser = 0 pues tendríamos B2 — A'A'' = aD = 0, y D = 0, o sea el caso excluido), x'(A''x' — 2Bx'') serú una cantidad positiva, y luego x puede ser escogida para hacer de g una cantidad negativa. Manifiestamente todos estos valores pueden ser escogidos de tal manera que, si se desea, todos sean enteros. Finalmente, no importa que valores sean dados a x' ya x'', x puede ser tomado tan grande como para hacer a g positiva. De modo que en este caso f sería una forma indefinida.

Finalmente, si a = 0 resulta

f = a'x'2 + 2bx'x'' + a''x''2 + 2x(b''x' + b'x'').

Ahora, si tomamos x' y x" arbitrariamente, pero de tal manera que b"x' + b' x" no sea = 0 (obviamente esto puede hacerse a menos que ambos b' y b'' sean = 0; pero entonces tendríamos D = 0), es facil ver que x puede ser escogido de tal modo que f tendrá tanto valores positivos como negativos. Y en este caso tambien f será una forma indefinida.

De la misma manera que determinamos la propiedad de la forma f a partir de los námeros aD y A', tambien pueden usarse aD y A'', de modo que la forma f sea definida si ambos aD y A'' son negativos; indefinida en todos los otros casos. Se puede, para el mismo proposito, considerar los námeros a'D y A, o bien a'D y A'', o bien a''D y A, o finalmente a'D y A'.

A raíz de todo esto se sigue que, en una forma definida, los seis námeros A, A', A'', aD, a'D y a''D son todos negativos. Para la forma positiva, a, a' y a'' seráan positivos y D negativo; para la forma negativa, a, a y a seráan negativos y D positivo. De ahí que todas las formas ternarias con un determinante positivo dado pueden ser distribuidas en formas negativas y formas indefinidas; todas aquáellas con un determinante negativo, en formas positivas y formas indefinidas; y no hay formas positivas con un determinante positivo ni formas negativas con un determinante negativo. Y es facil ver que la adjunta de una forma definida es siempre definida y negativa, y la adjunta de una forma indefinida es siempre indefinida.

Dado que todos los nuámeros que son representables por una forma ternaria dada pueden tambiáen ser representados por todas las formas que son equivalentes a ella, las formas ternarias de la misma clase son todas indefinidas o todas positivas o todas negativas. Así es legítimo transferir estas designaciones tambien a clases enteras. [[192]](#footnote-193)

la forma dada es la forma ternaria f =

*a,*

*b,*

*a, b ,*

de determinante D (diferente

de cero) y que es transformada en la forma equivalente g medio de la sustitución (S):

|  |  |  |
| --- | --- | --- |
| α, | β, | γ |
| α0, | β0, | γ0 |
| α00, | β00, | γ00 |

Nos resta determinar α, β, γ, etc. de tal modo que g sea mós simple que f. Sean (β A Β") ’ (M’ M'’ M") las formas adjuntas a f y g respectivamente, y

|  |  |  |
| --- | --- | --- |
| m, | m0, | m00 |
| n, | n0, | n00 |

por

designemoslas por F y G. Entonces, por el artículo 269, F sera transformada en G por medio de una sustitución que es adjunta a S, y G sera transformada en F por medio de una sustitucion derivada de la transposicion de S. El numero

of // , / off i ft o t Ha> *q»* > f a ff

αβ γ + α β γ + α βγ — α β γ — αβ γ — α βγ

debe ser = +1 o bien = —1. Le denotaremos por k. Observamos lo siguiente:

1. Si tenemos γ = 0 , γ0 = 0 , α00 = 0 , β00 = 0 , γ00 = 1 entonces

m = αα2 + 2^αα0 + α0α02 , m0 = αβ2 + 2^0ββ0 + α0β02 , m00 = α00

n = bβ0 + ^β, η0 = bα0 + ^α, η00 = ααβ + ^0(αβ0 + βα0) + α0α0β0

Ademas αβ0 — βα0 debe ser = +1 o bien = —1. Por tanto, es evidente que la forma binaria (α, b00, α0), cuyo determinante es Β00, sera transformada por medio de la sustitución α, β, α0, β0 en la forma binaria (m, n00, m0) de determinante M00 y, dado que αβ0 — βα0 = ±1, ellas serón equivalentes y, por ende, M00 = Β00. Esto tambien puede ser confirmado directamente. A menos que, por esta razón, (α, b00, α0) ya sea la forma mas simple en esta clase, podemos determinar α, β, α0, β0 de tal manera que (m, n00, m0) sea una forma mós simple. A partir de la teoría de la equivalencia de formas binarias, es facil concluir que esto puede hacerse de tal modo que m no sea mayor que y—3Β00 si Β00 es negativo, o bien, no mayor que λ/Β00 cuando Β00 es positivo o de tal manera que m = 0 cuando Β00 = 0. Por ello, en todos los casos el valor (absoluto) de m puede hacerse menor o igual ay/ ± 3 Β00. De esta manera, la forma f es reducida a otra con un primer coeficiente menor, si esto es posible. Y la forma que es adjunta a esta tiene el mismo tercer coeficiente que la forma F que es adjunta a f. Esta es la primera reducción.

1. Pero si α = 1, β = 0, γ = 0, α' = 0, α'' = 0, resulta k = β'γ''-β''γ' = ±1; así que la sustitución que es adjunta a S sera

±1, 0, 0 0, γ'', -β''

0, -γ', β'

y por esta sustitución F será transformada en G y tendremos

m =α, n' = bb γ'' + b'' γ', n'' = b'β" + b''β' m' =α'β'2 + 2b^'' + α''β''2 m'' =α'γ'2 + 2^// + α''γ''2 η =α'β'γ' + b(β'γ'' + γ'β'') + α''β''γ''

M' =Α'γ''2 - 2Βγ'γ'' + Α''γ'2 N = - Α'β''γ'' + B (β'γ'' + γ'β'') - Α''β'γ'

M'' =Α'β''2 - 2Ββ'β'' + Α''β'2

De este modo, es claro que la forma binaria (Α'', B, Α'), cuyo determinante es Da, sera transformada por medio de la sustitucion β', - γ', - β'', γ'' en la forma (M'', N, M') de determinante Dm, y por tanto (dado que β'γ'' - γ'β'' = ±1, o bien, dado que Dα = Dm) es equivalente a ella. A menos que, por esta razon, (Α'', B, Α') ya sea la forma mas simple de su clase, los coeficientes β', γ', β'', γ'' pueden ser

determinados de tal manera que (M'', N, M') es mas simple. Y esto puede lograrse

de tal modo que, sin distingo de signo, M'' no es mayor que ^±3Do. De este manera, la forma f es reducida a otra con el mismo primer coeficiente. Pero la forma que es adjunta a esta tendrá, si es posible, un menor tercer coeficiente que la forma F, la cual es adjunta a f. Esta es la segunda reducción.

1. Ahora bien, si ni la primera ni la segunda reducción es aplicable a la

forma ternaria f, es decir, si f no puede ser transformada por ninguna de ellas hacia una forma más simple; entonces necesariamente α2 será < o = 3Α'', y Α''2 sera, o bien < o = 4oD, sin distingo de signo. Así, α4 será < o = 3fΑ''2, de modo que α4 sera < o = 24αΡ, α3 < o = 27D, y α < o = 4 ^^D; y, de nuevo, Α''2 sera

< o = 16 3D4 y Α'' < o = 3 3D2. De ahí que, toda vez que α o Α'' exceda estos

límites, una u otra de las reducciones previas necesariamente se aplica a la forma f. Pero esta conclusioán no puede ser invertida, dado que a menudo ocurre que el primer

coeficiente y el tercer coeficiente de la forma adjunta de una forma ternaria están ya por debajo de esos límites; sin embargo puede hacerse más simple por una u otra de las reducciones.

1. Si ahora aplicamos alternativamente la primera y segunda reducción a una forma ternaria dada de determinante D, es decir, si aplicamos la primera o la segunda, entonces al resultado le aplicamos la segunda o la primera, y al resultado de esto de nuevo la primera o la segunda, etc., es claro que eventualmente arribaremos a una forma a la cual ninguna puede ser aplicada. Pues la magnitud absoluta de los primeros coeficientes de las formas en sí, y de los terceros coeficientes de las formas adjuntas se mantienen igual y luego decrecen de modo que la progresiáon eventualmente parara; de otro modo, tendríamos dos series infinitas de námeros continuamente decrecientes. Tenemos por tanto este notable teorema: Cualquier

forma ternaria de determinante D puede ser reducida a una forma equivalente con la propiedad de que su primer coeficiente no sea mayor que 3 ^~D y que el tercer coeficiente de la forma adjunta no sea mayor que 3 v7D2, sin distinción de signo, siempre y cuando la forma propuesta no tenga ya estas propiedades. En lugar del primer coeficiente de la forma f y del tercer coeficiente de la forma adjunta, podríamos haber considerado exactamente de la misma manera o el primer coeficiente de la forma y el segundo de su adjunta; o el segundo de la forma y el primero o tercero de su adjunta; o el tercero de la forma y el primero o segundo de su adjunta. Eventualmente llegaremos a la misma conclusián; pero es mas ventajoso usar un metodo consistente de modo que las operaciones involucradas pueden ser reducidas hacia un algoritmo fijo. Observamos finalmente que si hubieramos separado las formas en definidas e indefinidas, habríamos fijado límites inferiores para los dos coeficientes que hemos estado tratando; pero esto no es necesario para nuestros propoísitos. [[193]](#footnote-194)

Estos ejemplos ilustran los principios previos.

*Ejemplo 1.* Sea f

|  |  |  |
| --- | --- | --- |
| 19, | 21, | 50 |
| 15, | 28, | 1 |

luego F

/-825, V 257,

-166,

573,

398

370

y D = -1. Dado que (19, 1, 21) es una forma binaria reducida y no hay otra equivalente a ella que tenga su primer termino menor que 19, la primera reduccion no es aplicable aquí; la forma binaria (A", B, A') = (-398, 257, -166), por la teoría de la equivalencia de formas binarias, puede ser transformada en una equivalente mas simple (-2, 1, 10) por medio de la sustitucion 2, 7, 3, 11. Entonces, haciendo

β = 2, γ0 = -7, β00 = -3, γ00 = 11 y aplicando la sustitución

1. 0, 0

0, 2, -7

0,

-3,

11

19, 354, 4769

a la forma f, esta será transformada en ^

El tercer

-1299, 301, -82

coeficiente de la forma adjunta es -2, y en este aspecto, f0 es mas simple que f.

La primera reduccián puede ser aplicada a la forma f0. Esto es, dado que la forma binaria (19, -82, 354) es transformada en (1, 0, 2) por medio de la sustitucián 13, 4, 3, 1, la sustitucion

**r** 13, 4, 0**1**

**l** 3, 1, 0 **J**

1. 0, 0, 1 **J**

puede ser aplicada a la forma f0 y sera transformada en

1,

95,

2, 4769

16, 0

y..f"

Puede aplicarse nuevamente la segunda reduccián a la forma f00, cuya adjunta -513, -4513, -2

-95, 32, 1520

(-1, 1, -2) por medio de la sustitucion 47, 1, -1, 0; así que la sustitucián

es

Esto es (-2, -95, -4513) será transformada

en

( 1, 0, 0 **1**

1. 0, 47, -1 **J**

**l** 0, 1, 0 **J**

;V..f000.

1, 257, 2

1, 0, 16

coeficiente de esta forma no puede ser reducido maás de esto por medio de la primera reducciáon, ni puede ser el tercer coeficiente de la adjunta reducido máas por medio de la segunda reducciáon.

' 10, 26, 2 a . (-3, -20, -244!

,7, 0, 4j.cuyaadjunta«( 70, -28, 8 )

y cuyo determinante es =2. Aplicando alternativamente la segunda y la primera

puede ser aplicada a f00 y sera transformada en

*Ejemplo 2.* Sea f =

El primer

reducción

por la sustitución

1, 0, 0

[0, -1, 0](#bookmark84)

0, 4, -1

|  |  |  |
| --- | --- | --- |
| 0, | -1, | 0**1** |
| 1, | -2, | 0 \ |
| 0, | 0, | 1 ί |
| 1, | 0, | 0 |
| 0, | -1, | 0 |
| 0, | 2, | 1 |



0,

1,

0,



transformamos a

f

*f'*

f

///

en

-110,,

2, 2

0, -4

(

(-2: (-2;

2, 2

1, 0

f00

2,

1,

2,

-1,

22

2)

La forma f0000 no puede ser reducida mas por medio de la primera o de la segunda reducción.

274.

Cuando se trata de una forma ternaria, donde su primer coeficiente y el tercer coeficiente de la forma adjunta han sido reducidos lo mós posible por medio de los metodos precedentes, el siguiente metodo suministraró una reducción adicional.

Usando la misma notación que en el artículo 272 y haciendo α = 1, α0 = 0, β0 = 1, α00 = 0, β00 = 0, γ00 = 1, a saber, usando la sustitucion 1

Tal transformación no cambia los coeficientes a y A00, los cuales fueron disminuidos por las reducciones anteriores. Resta, por tanto, encontrar una determinación adecuada de β, γ y γ0 de tal modo que los coeficientes restantes sean disminuidos. Observamos primero que si A00 = 0 podemos suponer tambien que a = 0, pues si a no fuera = 0, la primera reduccion sería aplicable una vez mas, dado que cualquier forma binaria de determinante 0 es equivalente a una forma como (0, 0, h) y su primer termino es = 0 (vease art. 215). Por una razon completamente similar, es legítimo suponer que A00 tambien sería = 0 si a = 0, y por tanto, ya sea, ambos o ninguno de los numeros a y A00 seran 0.

En el segundo caso, β, γ y γ0 pueden ser determinados de tal modo que, sin distincion de signo, n00, N, N0 no son mayores que 1 a, 2A00, 2A00 respectivamente. De

.i, i, y.../00"· cuya adjunta es (-[[194]](#footnote-195) -1

En el caso donde a = A00 = 0 y, por tanto, tambien b00 = 0 tendremos

manera que en el primer ejemplo del artículo previo la ultima forma

1, 257, 2

1, 0, 16

cuya adjunta es

-513, -2, -1

1, -1

en la forma

|  |  |  |
| --- | --- | --- |
| 32 |  |  |
| 1, | -16, | 16 |
| 0, | 1, | -1 |
| 0, | 0, | 1 |
| cuya | adjunta | es |

.

m = 0, m0 = a0, m00 = a00 + 2bγ0 + 2b0 γ + a1 γ02

n = b + a^0 + b0e, n = b0, n00 = 0

22 D = a b = m n

y luego

Es facil ver que β y γ0 pueden ser determinados de tal manera que n seró igual al residuo absolutamente mínimo de b relativo al módulo que sea el maximo comun divisor de a0 y b0; a saber, de tal modo que n no sea mayor que la mitad de su divisor, sin considerar el signo, y n seró 0 toda vez que a0 y b0 sean relativamente primos. Si β y γ0 son determinados de esta manera, el valor de γ puede ser tomado tal que m00 no sea mayor que b0 sin importar el signo. Esto, por supuesto, sería imposible si b0 = 0, pero entonces D sería 0, el cual es el caso excluido. Así que para la ultima forma en

el segundo ejemplo del artículo previo, n = — 2 — β + 2γ0, y poniendo β = -2, γ0 tendremos n = 0; más aún m" = 2 — 2γ, y poniendo γ = 1 entonces m" = 0. tenemos la sustitución

1. —2, 1

= 0, Así

0, 1, 0

0, 0, 1

mediante la cual aquella forma será transformada en ,

í°, 2, °)...f

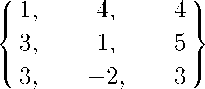
\0, —1, 0) J

275.

Si se tiene una serie de formas ternarias equivalentes f, f0, f00, f000, etc. y las transformaciones de cada una de estas formas en su sucesor: entonces, a partir de la transformacián de la forma f en f0 y de la forma f0 en f00, por el artículo 270 podemos deducir una transformacián de la forma f en f00; a partir de esto y de la transformacián de la forma f00 en f000 resultara una transformation de la forma f en f000, etc. y por medio de este proceso se puede encontrar la transformation de la forma f en cualquier otra forma de la serie. Y dado que, a partir de la transformation de la forma f en cualquier otra forma equivalente g se puede deducir una transformation de la forma g en f (S00 a partir de S, art. 268, 269), se puede, de esta manera, producir una transformacián de cualquiera de la serie f0, f00, etc. en la primera forma f. Así para las formas del primer ejemplo del artáculo previo encontramos las sustituciones

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13, | 4, | 0 | 13, | 188, | —4 | 13, | —20, | 16 |
| 6, | 2, | —7 | 6, | 87, | —2 | 6, | —9, | 7 |
| —9, | —3, | 11 | —9, | — 130, | 3 | —9, | 14, | —11 |

por medio de la cual f será transformada en f00, f000, f0000 respectivamente y, a partir de la ultima sustitucion, podemos derivar



mediante la cual f000 se transformará en f. Similarmente, tenemos las siguientes sustituciones para el ejemplo 2 del artáculo anterior.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1, | —1, | 1 | 2, | 1  CO | —1 |
| 1  co | 4, | 1  co | 3, | 1, | 0 |
| 10, | — 14, | 11 | 2, | 4, | 1 |

276.

mediante las cuales la forma

/10, 26, 2 l 7, 0, 4

se transforma en

( 0, 2, 0 λ

U -1, 0j

y vice versa.

TEOREMA. El número de clases entre las cuales se distribuyen todas las formas ternarias de un determinante dado es siempre finito.

Demostración. I. El numero de todas las formas a’ de un determinante

dado D en las cuales a = 0, b" = 0, b no es mayor que la mitad del valor del maximo común divisor de a' y b', y a" no es mayor que b', es obviamente finito. Pues, como debemos tener a'b' = D, los unicos valores posibles de b' son +1, — 1, y las raíces de cuadrados que son divisores de D (si hay otros diferentes de 1) tomadas positiva y negativamente. El numero de ellos es finito. Para cada uno de los valores de b', sin embargo, el valor de a' es dado, y por lo tanto el número de valores de b y de a" es finito.

1. Suponga que a no es = 0 ni mayor que 4 ^±D; que b''2 — aa' = A'' y que no es = 0 ni mayor que 3 ^D2; que b'' no es mayor que 3a; que ab — b'b" = B y a'b' — bb'' = B' y que ninguno es mayor que 3A''. En este caso un argumento similar

al anterior muestra que el número de todas las formas ^ ^,, de determinante D

es finito. Pues el nuúmero de todas las combinaciones de los valores de a, b , A , B y B' sera finito, y cuando se han determinado, los coeficientes restantes de la forma, a saber, a', b, b', a'' y los coeficientes de la forma adjunta

b2 — a a' = A, b'2 — aa' = A', a'b" — bb' = B''

estarán determinados por las siguientes ecuaciones:

. b''2 — A'' B2 — aD „ B'2 — a'D ..

' - A' = ——, A = - , B''

a=

BB + b D

a

b=

AB B B

A

Ba + B b

D

b' =

A

A B BB

A

Bb + B a

//

a =

A D

b'2 — A' b2 — A bb' + B''

A

a

b

Ahora, cuando se han obtenido todas las formas, si escogemos de todas las combinaciones, los valores de a, b , A , B y B que hacen que a , a , b y b sean enteros, habrá un número finito de ellos.

III. Por lo tanto, todas las formas en I y II constituyen un número finito de clases, y si algunas formas son equivalentes resultaran menos clases que formas. Por las investigaciones anteriores, cualquier forma ternaria de determinante D es necesariamente equivalente a alguna de estas formas, i.e., pertenece a alguna de las clases definidas por estas, o sea, estas clases incluirán todas las formas de determinante D, i.e., todas las formas ternarias de determinante D estaran distribuidas entre un numero finito de clases. Q. E. D.

277.

Las reglas para generar todas las formas en I y II del artículo anterior siguen en forma natural de su definición; por lo tanto basta con dar algunos ejemplos. Para D = 1, las reglas I generan las siguientes seis (tomando uno de los signos dobles a la vez):

/0, 1,0\ /0, 1, ±1\

\0, ±1, o) , \0, ±1, o)

Para las formas II, a y A" pueden asumir unicamente los valores +1 y -1, y por lo tanto para cada una de las combinaciones resultantes b", B y B' deben ser = 0 y obtenemos las formas

(1,-1, Λ (-1,1, Λ (1,1,-Λ (-1,-1,-Λ

0, 0, 0 , 0, 0, 0 , 0, 0, 0 , 0, 0, 0

Similarmente para D = -1 obtenemos seis formas I y cuatro formas II:

'0,-1,0 ! ( 0,-1, ±1'

0, 1, 0 , 0, 1, 0

(0,-1,0\ A \0, ±1,0) , 1,-1,-1 , -1,

0, 0, 0 , 0,

1,-1,-1 , -1,1,-1 0, 0, 0 , 0, 0, 0

Para D = 2 tenemos las seis formas I:

0, 2, 0

y las ocho formas II:

(1,-1,2 ( 0, 0, 0

0, 0, 0

;

-1,-1,1 0, 0, 0

,1 , 1,1,1

, 0 , 0, 0, 0

0, 2, 0 , 0, 2, ±1 0,±1,0 , 0,±1, 0

-1, 1, 2

0, 0, 0

-1, 2, 1

0, 0, 0

1,1,-2 0, 0, 0 '1, 2,-1' 0, 0, 0

-1,-1,-2 0, 0, 0

-1, -2,-1' 0, 0, 0

Pero el número de clases de formas en estos tres casos es mucho menor que el número de formas. Es facil confirmar que

I. La forma ^0’ 1’ 0^ se transforma en

/0, 1,0\ /0, 1, Λ /0, 1,— 1\ /1,1,— 1\

\0,-1, *0*) , \*0*, ±1,*0*) , *\0*, ±1, *0*) , *\0*, 0, *0*)

respectivamente mediante las sustituciones

|  |  |  |
| --- | --- | --- |
| 1 0 0 | 0 ’0 ’ i | 0’ 0’ 1 |
| 0 1 0 | 0 ’1’ -1 | 0’ 1 ’ 1 |
| 0 0 -1 | ±1 ’1’ 0 | ±1 ’-1 ’ -1 |

1’ 0’ -1

i, i, -1

0,1,1

y que la forma Q’ 0’ -0^ se transforma en ^0’ -i’ 0^ y ^-0’ 0’ 0^ por una permutaciún simple de las incognitas. Entonces, las diez formas ternarias del determinante 1 se reducen a estas dos: (0’1’ 0), (-0’ -i’ -0); para la primera, si lo prefiere, se puede

tomar Q’0 ’0^. Y puesto que la primera forma es indefinida y la segunda definida, es claro que cualquier forma ternaria indefinida de determinante 1 es equivalente a la forma x2 + 2yz y cualquier forma definida es equivalente a —x2 — y2 — z2.

1. De manera similar encontramos que cualquier forma ternaria indefinida de determinante —1 es equivalente a la forma — x2 + 2yz y cualquier forma definida a x2 + y2 + z2.
2. Para el determinante 2, la segunda, sexta y setima de las ocho formas (II) pueden rechazarse inmediatamente porque pueden obtenerse a partir de la primera por una permutación simple de las incúgnitas. Similarmente, la quinta se puede obtener a partir de la tercera y la octava a partir de la cuarta. Las tres formas restantes, junto con las seis formas I generarún tres clases; es decir ^0 ’2 ’0^ se transformarú en ^0 ’ - ’0^ mediante la sustituciún

1,

0,

0,

1,

0

0

0, 0, —1

y la forma ^0 ’ 0 ’ 0^ se transforma en

(0, 2, 1 λ (0, 2,1! (0, 2, —1! (

0, 2, —1 0, —1, 0

! í1·—1·2!

) O 0, <V

V0,1,0) , ^0, —1, 0) , ^0,1, 0) , ^

respectivamente mediante las sustituciones

|  |  |  |  |
| --- | --- | --- | --- |
| 1,0,1 | 1,0,-1 | 1,0, 0 | 1,0,0 |
| 1,2,0 | 1,2, 0 | 1,2,-1 | 1,2,1 |
| 1,1,0 | 1,1, 0 | 1,1,-1 | 1,1,1 |

1,0,0

0,1,2

0,1,1

Por lo tanto, cualquier forma ternaria de determinante 2 es reducible a una de las siguientes tres formas

/0, 2, 0\ /1, 1, -2\ (-1,-1, -2^1  
0, 1, 0 , 0, 0, 0 , 0, 0, 0

y, si lo prefiere, 0’ ^ puede reemplazar la primera. Claramente cualquier forma

ternaria definida será necesariamente equivalente a la tercera — x2 — y2 — 2z2, puesto que las dos primeras son indefinidas. Y una forma indefinida sera equivalente a la primera o segunda; a la primera, 2x2 + 2yz si sus tres primeros coeficientes son todos pares (obviamente tal forma se transformará en una forma similar mediante cualquier sustitución y por lo tanto no puede ser equivalente a la segunda forma); a la segunda forma x2 + y2 — 2z2, si sus tres primeros coeficientes no son todos pares, sino que uno, dos o todos son impares (pues la primera forma 2x2 + 2yz, no se puede transformar en esta).

Segun este argumento, pudimos haber predicho a priori en los ejemplos del artículo 273, 274 que la forma definida Q9 ^ 5°J de determinante —1 se reduciría

a x2 + y2 + z2 y que la forma indefinida ^10 ^ ^ de determinante 2 se reduciría a 2x2 — 2yz o (lo que es lo mismo) a 2x2 + 2yz. [[195]](#footnote-196)

dado por una forma ternaria dada. II. Encontrar todas las representaciones de una forma binaria dada por una forma ternaria dada. III. Juzgar si dos formas ternarias dadas del mismo determinante son equivalentes, y si lo son, encontrar todas las transformaciones de una en la otra. IV. Juzgar si una forma ternaria dada implica otra forma ternaria dada de determinante mayor, y si lo hace, asignar toda transformación de la primera en la segunda. Puesto que estos problemas son mas complicados que los problemas análogos para formas binarias, los trataremos con mas detalle en otra ocasián. Por el momento, restringiremos nuestra investigacián a mostrar como el primer problema puede reducirse al segundo y el segundo al tercero. Mostraremos como resolver el tercer problema para casos muy simples que son particularmente ilustrativos del teorema de formas binarias, y excluiremos el cuarto problema del todo.

279.

LEMA: Dados tres enteros cualesquiera *a*, *a*! y *a*" (no todos = 0), encontrar otros seis *B*, *B*', *B*'', *C*, *C* y *C*' tales que

*B C - B'C* = *a, B" C - BC* = *a, BC - B C* = *a*

Solución. Sea α el máximo comán divisor de a, a' y a" y escoja los enteros A, A! y A'' tales que

Aa + A'a' + A" a" = α

Ahora escoja arbitrariamente tres enteros C, C' y C' con la ánica restriccián de que los tres números C'A'' — C''A', C A — CA' y CA' — C'A no son todos = 0. Designaremos estos námeros por b, b' y b" respectivamente y su maximo comán divisor por β. Entonces, si se pone

*abff* *—* a*"*b' = αβΟ\ a*"*b *—* ab*'* = *αβΒ,* ab' *— ab* = αβΒ'

es claro que C, C y C' son enteros. Finalmente si escogemos enteros B, B' y B'' tales que

Bb + B' b' + B''b'' = β

poniendo

Ba + B' a' + B''a'' = h

y fijando

B = αΒ - hA, B0 = aB - hA, B00 = aB - hA"

los valores de B, B0, B", C, C0 y C00 satisfarán las ecuaciones dadas.

En efecto, se encuentra que

aB + arBr + a"B00 = 0

bA + b0A0 + b"A" = 0 y por lo tanto bB + b0B0 + b00B00 = αβ

Ahora, a partir de los valores de C0 y C00 tenemos

αβ(B0C00 - B00C0) = ab0B0 - abB0 - a00bB00 + ab00B00

= a(bB + b0B0 + b00B00) - b(aB + a0B0 + a00B00) = aea

y así B'C" - B00C0 = a; similarmente encontramos que B00C - BC00 = a' y BC0 - B0C = a00. Q. E. F. Pero debemos omitir aquí el analisis mediante el cual encontramos esta solución y el metodo para encontrar todas las demas a partir de una de ellas.

280.

Supongamos que la forma binaria

at2 + 2btu + cu2 ...φ

cuyo determinante = D es representada por la forma ternaria f con incognitas x, x' y x00, poniendo

x = mt + nu, x0 = m't + n'u, x00 = mf't + n"u

y que la adjunta de f es la forma F con incógnitas X, X' y X00. Entonces, es facil confirmar, mediante calculos, (designando los coeficientes de f y F por letras) o por deduction a partir del artículo 268.II, que el nómero D es representable por F poniendo

X = m'n" - m00n0, X0 = m00n - mn", X00 = mn0 - m'n

Se puede decir que esta representación del número D es la adjunta de la representación de la forma φ por f. Si los valores de X, X' y X'' no tienen un divisor común, para abreviar llamaremos propia esta representaciún de D, de otra manera, serú impropia y tambien daremos estas mismas designaciones a la representaciún de la forma φ por f a la cual la representaciún de D es adjunta. Ahora, el descubrimiento de todas las representaciones propias del número D por la forma F se basa en las siguientes consideraciones:

1. No hay ninguna representacion de D por la forma F que no se pueda deducir de alguna representaciúon de una forma de determinante D por la forma f, i.e. que es adjunta a tal representaciúon.

En efecto, sea X = L, X' = L', X" = L" una representaciún cualquiera de D por F; por el lema del artículo anterior escoja m, m', m", n, n' y n" tales que

m! n" — m''n' = L, m''n — mn'' = L', mn' — m'n = L''

y transforme f en la forma binaria φ = at2 + 2btu + cu2 por la sustitucion x = mt + nu, x = mt + nu, x = mt + nu

Es facil ver que D sera el determinante de la forma φ y que la representacion de D por F serúa la adjunta de la representaciúon de φ por f.

Ejemplo. Sea f = x2 + x'2 + x''2 y F = —X2 — X'2 — X''2; D = —209; su representacion por F serú X = 1, X' = 8, X'' = 12; y encontramos que los

valores de m, m', m'', n, n' y n'' son —20, 1, 1, —12, 0 y 1 respectivamente y

φ = 402t2 + 482tu + 145u2.

II. Si φ y χ son formas binarias propiamente equivalentes, cualquier representaciúon de D por F que es la adjunta de una representaciúon de φ por f serú tambien adjunta a una representacion de la forma χ por f.

Sean p y q las incúgnitas de la forma χ; transforme φ en χ mediante la sustitucion propia t = ap + βq, u = γρ + úq y sea

x = mt + nu, x' = m't + n'u, x'' = m''t + n''u... (R)

alguna representacioún de la forma φ por f. Entonces si se pone

am + qn = g, «m' + qn' = g', am'' + qn'' = g''

β^. + ún = h, β^.' + ún' = h', β^" + ún'' = h''

la forma χ estará representada por f fijando

x = gp + hq, x = g p + h'q, x" = g" p + h"q ... (R')

y mediante calculos (puesto que αδ — βγ = 1) encontramos

g'h" — g"h' = m'n" — m"n', g"h — gh" = m'n — mn" , gh' — g'h = mn' — m'n

i.e. la misma representacián de D por F es adjunta a las representaciones R y R'.

En el ejemplo anterior la forma φ es equivalente a χ = 13p2 — 10pq + 18q2 y se transforma en ella mediante la sustitución propia t = —3p + q, u = 5p — 2q; y la representacián de la forma χ por f es: x = 4q, x' = —3p + q, x'' = 2p — q. A partir de esto deducimos la misma representacion del námero —209 que teníamos antes.

1. Finalmente, si dos formas binarias φ y χ de determinante D cuyas incognitas son t, u; p, q, se pueden representar por f y si la misma representacion propia de D por F es adjunta a la representacián de cada una de estas, las dos formas deben ser propiamente equivalentes. Supongamos que φ se representa por f poniendo

x = mt + nu, x = mt + n u, x = m t + n u

y que χ se representa por f fijando

x = gp + hq, x' = g'p + h'q, x" = g''p + h" q

y que

mn — mn = gh — gh = L  
m n — mn = g h — gh = L  
mn' — m'n = gh' — g'h = L"

Ahora escoja los enteros l, l' y l" tales que Ll + Ü I' + L" l" = 1 y sea

n'l'' — n''l' = M, n''l — nl'' = M', nl' — n'l = M''  
l'm" — l" m' = N, l''m — lm'' = N', lm' — l'm = N''

y finalmente, sea

gM + g'M' + g''M'' = α, hM + h'M' + h''M'' = β  
gN + g'N' + g''N'' = γ, hN + h'N' + h''N'' = δ

A partir de esto es fácil deducir

am + γη = g — l(gL + g'L' + g"L") = g em + δη = h — l(hL + h'L' + h"L") = h

y similarmente

am0 + γη = g0, ^m0 + δη0 = h0, am00 + γη0 = g00, ^m00 + δη00 = h00

A partir de esto es claro que mt + ηη, m0t + η0η, m00t + η00 η se transformará en gp + hq, g0p + h0q, g00p + h00q, respectivamente, mediante la sustitucián

t = ap + eq, η = γρ + δq... (S)

y mediante la sustitución S, φ se transformara en la misma forma que f poniendo

x = gp + hq, x' = g0p + h0q, x00 = g00p + h00q

es decir, en χ a la cual debe, por lo tanto, ser equivalente. Finalmente, mediante las sustituciones adecuadas se encuentra que

αδ — βγ = (Ll + Ll' + L00 100 ) 2 = 1

Por lo tanto, la sustitucián S es propia y las formas φ y χ son propiamente equivalentes.

Como resultado de estas observaciones se derivan las siguientes reglas para encontrar toda representacián propia de D por F: Encontrar todas las clases de formas binarias de determinante D y de ellas seleccionar una forma arbitraria; encontrar todas las representaciones propias de cada una de estas formas por f (desechando cualquiera que no se puede representar por f) y de cada una de estas representaciones, deducir representaciones del námero D por F. Mediante I y II es claro que de esta manera se obtienen todas las representaciones propias posibles y que, por lo tanto, la solucion es completa; mediante III es claro que transformaciones de formas de diferentes clases producen representaciones diferentes.

281.

La investigación de representaciones impropias de un número dado D por la forma F puede reducirse fúcilmente al caso anterior. Es evidente que si D no es divisible por ningún cuadrado (excepto 1), no habrá ninguna representaciún de este tipo; pero si λ2, μ2, ν2, etc. son divisores cuadrados de D, todas las representaciones impropias de D por F pueden encontrarse si primero encontramos todas las representaciones propias de los numeros ^2, ^2, , etc. por esta misma

forma y se multiplican los valores de las incúgnitas por λ, μ, ν, etc. respectivamente.

Por lo tanto, el poder encontrar todas las posibles representaciones de un número dado por una forma ternaria dada, la cual es adjunta a otra forma ternaria, depende del segundo problema. Y aunque a primera vista esto parece ser un caso muy particular, los demas casos se pueden reducir a este como sigue. Sea D el numero que se quiere representar por la forma h' h") de determinante

Δ, cuya adjunta es la forma ’ h"^ = f. Entonces la adjunta de f sera

(^Ah’ Ah' ’Ah") = F, y es claro que las representaciones del numero ΔD por F (esta investigacion depende de la anterior) seran identicas a las representaciones del número D por la forma propuesta. Pero, cuando todos los coeficientes de la forma f tienen un divisor comun μ, es evidente que todos los coeficientes de la forma F seran divisibles por μ2 y así ΔD tambien debe ser divisible por μ2 (de otra manera, no habrían representaciones); y representaciones del numero D por la forma propuesta coincidirán con representaciones del numero ΔΡ por la forma que resulta de dividir cada uno de los coeficientes de F por μ2, y esta forma sera adjunta a la forma que resulta de dividir cada coeficiente por μ.

Observamos, finalmente, que la solucion del primer problema no es aplicable en el caso donde D = 0; pues en este caso, las formas binarias del determinante D no estan distribuidas entre un numero finito de clases; resolveremos posteriormente este caso, utilizando principios diferentes.

282.

La investigacion de las representaciones de una forma binaria dada de determinante distinto de 0[[196]](#footnote-197)) por una forma ternaria, depende de las siguientes

observaciones.

1. De cualquier representación propia de una forma binaria (p, q,r) = φ de determinante D por la forma ternaria f de determinante Δ se pueden deducir enteros B y B' tales que

B2 = Δρ, BB' = —Δq, B'2 ξ Δr (mod. D)

i.e. un valor de la expresion Δ(ρ, -q,r) (mod. D). Tomese la siguiente repre­

sentation propia de la forma φ por f

x = at + βη, x' = a't + β'η, x" = a"t + β"η

(donde x, x' y x''; t y η designan las incognitas de las formas f y φ); escoja enteros Y, γ' y γ'' tales que

(α'β'' — α''β')γ + (α''β — αβ'')γ' + (αβ' — α'β )γ'' = k con k = +1 o = —1. Transforme f mediante la sustitución

en la forma

resulta a = tanto

1. *a , a*
2. *b1, b”*

B E’, B'w = G. Entonces, claramente

= g, cuya adjunta es p, b'' = q, a' = r, A'' = D, y Δ el determinante de la forma g; por lo

B2 = Δp + A'D, BB' = —Δq + B''D, B'2 = Δr + AD

|  |  |  |
| --- | --- | --- |
| α, β, | | γ |
| α', | β', | γ |
| α'', | β'', | γ |

o o o D D

Entonces, por ejemplo, la forma 19t2 + 6tu + 41u2 es representada por x2 + x' + x'' poniendo x = 3t + 5u, x' = 3t — 4u, x'' = t; y fijando γ = —1, γ' = 1, γ'' = 0, tendremos B = —171, B' = 27 o sea (—171, 27) como un valor de la expresión

1. Puesto que γ, γ0 y γ00 pueden determinarse de una infinidad de maneras diferentes, resultaran diferentes valores de B y B0. Veamos que relación tendrán entre sí. Suponga que tambien hemos escogido δ, δ0 y δ00, tales que

(α0β00 — α00β0)δ + (α00β — αβ")δ' + (αβ0 — α β)δ00 = k

+1 o —1 y que la forma f se transforma mediante la sustitución

se hace

|  |  |  |
| --- | --- | --- |
| α, | β, | δ |
| α0, | β0, | δ0 |
| α00, | β00, | δ00 |

en í b’ a'’ b'w = g con adjunta ( B ’ Bg/ Bg"j = G. Entonces g y 0 serán equivalentes y así tambien G y G, y por una aplicación de los principios dados en los artículos 269 y 270[[197]](#footnote-198)) encontraremos que si se fijan

(β0γ00 — β00γ 0)δ + (β00γ — βγ00)δ0 + (βγ0 — β0γ)δ00 = Ζ (γ0α00 — γ00α0)δ + (γ00α — γα00)δ0 + (γα0 — γ0α)δ00 = η

la forma G se transformara en G mediante la sustitucion

k, 0, 0 0, k, 0

C η, k

Entonces resulta

B = nkD + kkB, B0 = Ζ kD + kkB0

y así, puesto que kk = ±1, tendremos B ξ B, B0 ξ B0 o B ξ —B, B0 ξ —B0 (mod. D). En el primer caso diremos que los valores (B,B0) y (B, B0) son equivalentes, en el segundo caso, que son opuestos; y diremos que las representaciones de la forma φ pertenecen a cualquiera de los valores de la expresion Δ(ρ, —q,r)

(mod. D) que puede deducirse mediante el metodo de I. Así pues, todos los valores a los cuales les corresponde la misma representacion, serán equivalentes u opuestos.

1. En cambio, como en I, si x = at + βη etc. es una representación de la forma φ por f, y si esta representation pertenece al valor (B,B0) del cual se deduce mediante la transformación

la misma representación tambien pertenecerá a cualquier otro valor (B, B0) que le es equivalente u opuesto; i.e., en lugar de γ, γ0 y γ00 podemos tomar otros enteros δ, δ0 y δ00 para los cuales la ecuación

|  |  |  |
| --- | --- | --- |
| α, β, | | γ |
| a0, | β0, | γ0 |
| a00, | β00, | γ00 |

(α0β00 — α00β0)δ + (α00β — αβ00)δ0 + (αβ0 — α0β )δ00 = ±1

(Ω)

tiene lugar y se escogieran tales que, si f se transforma en su forma adjunta mediante la sustitucion (S):

|  |  |  |
| --- | --- | --- |
| a, | β, | δ |
| a0, | β0, | δ0 |
| a00, | β00, | δ00 |

el cuarto y quinto coeficiente de la forma adjunta serón respectivamente = B, B0. En efecto, sea

±B = B + ηϋ, ±B0 = B0 + ζϋ

(aquí y mas adelante tomaremos el signo superior e inferior segón los valores de (B,B0) y (B, B0) sean equivalentes u opuestos); ζ y η serán enteros y mediante la sustitucióon

1. 0, ζ

0, 1,

η

0, 0, ±1

g se transformara en una forma 0 con determinante Δ. Es facil ver que los coeficientes 4 y 5 de la forma adjunta serón = B, B0 respectivamente. Sin embargo, si fijamos

αζ + βη ± γ = δ, α0ζ + β0η ± γ0 = δ0, α00ζ + β00η ± γ00 = δ00

no es difícil ver que f se transformara en 0 mediante la sustitución (S) y que la ecuacion (Ω) sera satisfecha. Q. E. D.

283.

A partir de estos principios se deduce el siguiente método para encontrar todas las representaciones propias de la forma binaria

φ = pt2 + 2qtu + ru2

de determinante D por la forma ternaria f de determinante Δ.

1. Se buscan todas los valores diferentes (i.e. no equivalentes) de la expresión \J Δ(ρ, -q, r) (mod. D). Para el caso en el cual φ es una forma primitiva y Δ y D primos relativos, la solucion fue dada en el art. 233, y los casos restantes se pueden reducir facilmente a este. Para abreviar no daremos una explicación mas completa. Simplemente indicaremos que siempre que Δ y D sean primos relativos, la expresión Δ(ρ, -q,r) no puede ser un residuo cuadrático de D a menos que φ sea una forma primitiva. En efecto, suponiendo

Δρ = B2 - DA', -Δq = BE' - DE", Δr = B'2 - DA

entonces

(DE'' - Δq)2 = (DA' + Δp)(DA + Δ^ y manipulando y sustituyendo D por q2 - pr tenemos

(q2 - pr)(B"2 - AA') - Δ(Αρ + 2B''q + A'r) + Δ2 = 0

y es fócil concluir que si ρ, q y r, tienen un divisor comón, tambien este seró un factor de Δ2; por consiguiente Δ y D no podrían ser primos relativos. Por lo tanto ρ, q y r no pueden tener un divisor comun y φ es una forma primitiva.

1. Designemos el nómero de estos valores por m y supongamos que entre ellos hay n que son opuestos a sí mismos (fijando n = 0 cuando no los hay). Entonces es claro que los restantes m - n valores estarán compuestos por parejas que son opuestas entre só (puesto que hemos supuesto que se incluyen todos los valores); ahora, si de cada par de valores opuestos rechazamos un valor arbitrariamente, nos quedaran 2 (m + n) valores en total. Asó pues por ejemplo, tenemos ocho valores de la expresión ^-1(19, -3,41) (mod. 770), a saber, (39, 237), (171,-27), (269, -83), (291,-127), (-39,-237), (-171, 27), (-269, 83) y (-291,127). Rechazamos los cuatro últimos como opuestos a los primeros. Pero es evidente que si (B,B') es un valor que es opuesto a só mismo, 2B, 2B' y tambien 2Δρ, 2Δq y 2Δr serón divisibles por D; y

por lo tanto, si Δ y D son primos relativos, 2p, 2q y 2r, también serán divisibles por D. Según I, en este caso p, q y r no pueden tener un divisor comán, entonces 2 debe ser divisible por D. Esto no puede ocurrir a menos que D sea = ±1 o = ±2. Así pues, para todos los valores de D mayores que 2, siempre resulta n = 0 si Δ y D son primos relativos.

1. Al ver esto, es evidente que cualquier representacián propia de la forma φ por f debe pertenecer a uno y sálo uno de los valores restantes. Deberíamos, por lo tanto, revisar cada uno de estos valores en orden para encontrar la representacioán que pertenece a cada uno. Para poder encontrar la representacián correspondiente a un valor dado (B, B0) debemos determinar primero la forma ternaria g = ^a 5/’ 5'/^ cuyo

determinante = Δ y en la cual a = p, b" = q, a0 = r, ab — b'b" = B, a'b' — bb" = B0;

los valores a00, b y b' se pueden encontrar con la ayuda de la ecuacián del artículo 276.II. A partir de estos es fácil ver que cuando Δ y D son primos relativos, b, b0 y a00 deben ser enteros (puesto que estos tres numeros dan valores enteros cuando son multiplicados por D y luego por Δ). Ahora, si alguno de los coeficientes b, b0 y a00 es una fracción o las formas f y g no son equivalentes, no habrá ninguna representación de la forma φ por f perteneciente a (B, B0); pero si b, b0 y a00 son enteros y las formas f y g son equivalentes, entonces, cualquier transformation de f en g, por ejemplo

|  |  |  |
| --- | --- | --- |
| a, | β, | Y |
| a0, | β0, | γ0 |
| a00, | β ", | Y00 |
| producira tal representacion, a saber, |  |  |

x = at + βυ, x0 = a0t + β0υ, x00 = a00t + β"υ

Es claro que no puede existir ninguna representation de este tipo que no se pueda deducir de alguna transformacion. Entonces aquella parte del segundo problema que se refiere a la representation propia se reduce al tercer problema.

1. Ahora, transformaciones diferentes de la forma f en la forma g siempre producen representaciones distintas, con la unica exception del caso en el cual el valor (B,B0) es opuesto a sí mismo. En este caso dos transformaciones dan una sola representacion. En efecto, suponga que f tambien se transforma en g mediante la sustitucion

|  |  |  |
| --- | --- | --- |
| a, | β, | δ |
| a0, | β0, | δ0 |
| a00, | β00, | δ00 |

(que da la misma representación que la anterior) y sean k, k, ζ y η los mismos números que en II del artículo anterior. Tendremos

B = kkB + ηΙΌ, B' = kkB' + ζ ID

Si se supone que ambas k, k = +1 o = -1, encontramos (ya que hemos excluido el caso de D = 0) que ζ = 0, η = 0 y se sigue que δ = γ, δ' = γ', δ" = γ''; estas dos transformaciones pueden ser diferentes sólo cuando uno de los números k o k es +1 y el otro -1; entonces tenemos B ξ —B, B' ξ —B' (mod. D) o el valor de (B,B') es opuesto a só mismo.

1. A partir de lo dicho anteriormente (art. 271) sobre los criterios para formas definidas e indefinidas, se sigue facilmente que si Δ es positivo, D es negativo, y φ es una forma negativa, g sera una forma negativa definida, pero si Δ es positivo y D es positivo (o bien D es negativo y φ una forma positiva), g sera una forma indefinida. Ahora, puesto que f y g definitivamente no pueden ser equivalentes, a menos que sean similares en cuanto a esto, es claro que formas binarias con determinantes positivos y formas positivas no pueden ser representadas propiamente por una forma ternaria negativa, y que formas binarias negativas no pueden representarse por formas ternarias indefinidas con determinante positivo; pero una forma ternaria del primer tipo puede representar una forma del segundo tipo, y una forma ternaria del segundo tipo puede representar una forma del primer tipo uónicamente. Similarmente, concluimos que una forma ternaria definida (i.e. positiva) con determinante negativo puede representar uónicamente formas binarias positivas, y que una forma ternaria indefinida con determinante negativo solamente puede representar formas binarias negativas y formas con determinante positivo. [[198]](#footnote-199)

alguno de los números e, e0, e00, etc. como máximo común divisor. Por esta razón decimos simplemente que una representación impropia de la forma φ pertenece al

o 2 2

divisor cuadrado e2, o e0 , o e00 , etc. Ahora se utilizan las reglas siguientes para encontrar todas las representaciones de la forma φ que pertenecen al mismo divisor dado e2 (supondremos que su raíz cuadrada e se toma positivamente). Para abreviar daremos una demostracion sintetica, pero sera facil reconstruir el analisis que produce los resultados.

Primero encuentre todas la formas binarias de determinante DJ que se transforman en φ mediante una sustitucion propia como T = χί + λu, U = μη, donde T y U son incógnitas de tal forma; ί y u incognitas de la forma φ; χ y μ enteros positivos (cuyo producto es por lo tanto = e); λ un entero positivo menor que μ (puede ser cero). Estas formas, con las transformaciones correspondientes, se pueden encontrar como sigue.

Sea χ igual, sucesivamente, a cada uno de los divisores de e tomados positivamente (incluyendo a 1 y a e) y sea μ = X; para cada uno de los valores enteros χ y μ, asigne a λ todos los valores enteros desde cero hasta μ — 1, y de seguro tendremos todas las transformaciones. Ahora podemos encontrar la forma que se transforma en φ mediante una sustitución T = χί + λη, U = μη, investigando la forma en la cual se transforma φ mediante la sustitución ί = XT — λ U, u = μ U; así se obtendrán las formas correspondientes a cada una de las transformaciones; pero sólo aquellas formas en las cuales los tres coeficientes son enteros[[199]](#footnote-200)) deben ser retenidas.

Segundo, supongamos que Φ es una de las formas que se transforma en φ mediante la sustitucion T = χί + λη, U = μη; se investigan todas las representaciones propias de la forma Φ por f (si existe alguna) y se exhiben en general por la fórmula:

x = AT + BU, x0 = AT + B0U, x00 = A00T + B00 U (R)

De cada uno de los (R) se deduce una representación

x = αί + βη, x0 = α0ί + β0η, x00 = α00ί + β00η (ρ)

mediante las ecuaciones

α = χΑ, α0 = χΑ0, α" = χΑ00 (R)

β = λΑ + μΒ, β = ΛΑ0 + μΒ0, β" = ΛΑ" + μΒ00

Al tratar de la misma manera todas las otras formas que encontramos mediante la primera regla (si hay varias), otras representaciones serán obtenidas a partir de cada representación propia de cada forma. De esta manera obtendremos todas las representaciones de la forma φ que pertenecen al divisor e2 y cada una sólo una vez.

Demostración. I. Es tan obvio que la forma ternaria f se transforma en φ por cada sustitución (ρ) que no necesita de una explicación adicional; que cada representación (ρ) es impropia y pertenece al divisor e2 es claro en vista de que los numeros

α0β00 - α"β0, α"β - αβ", αβ - α0β son = e^'B" - Α"®'), e^'B - ΑΒ00),

e^B0 - Α'Β) respectivamente y su móximo comón divisor seró e (puesto que (R) es una representacióon propia).

1. Mostraremos que a partir de cualquier representación (ρ) de la forma φ se puede encontrar una representacion propia de una forma de determinante ^2 contenida entre las formas encontradas mediante la primera regla; eso es, a partir de los valores dados α, α0, α00, β, β0 y β00 podemos deducir valores enteros χ, λ y μ con las condiciones prescritas, tanto como los valores de Α, Α0, Α00, Β, Β0 y Β00 que satisfacen unívocamente a las ecuaciones (R). Es inmediatamente claro de las tres primeras ecuaciones de (R) que para χ debemos tomar el maximo común divisor de α, α0 y α00 con signo positivo (ya que Α0Β00 - Α00Β0, Α00Β - ΑΒ00 y ΑΒ0 - Α0Β no tienen un divisor común, y Α, Α0 y Α00 tampoco); por lo tanto esrán determinados Α, Α0, Α00 y μ = χ (es fócil ver que necesariamente serón enteros). Supongamos que los tres enteros a, a0 y a00 hacen αΑ + α0Α0 + α00Α00 = 1 y para abreviar escribamos k para αΒ + α0Β0 + α00Β00. Entonces a partir de las óltimas tres ecuaciones (R) se sigue que αβ + α0β0 + α00β00 = λ + μk y de esto es inmediatamente evidente que se da solo un valor de λ entre los límites de 0 y μ - 1. Cuando hemos hecho esto, los valores de Β, Β0 y Β00 tambien se habrán determinado, asó que resta solo mostrar que siempre serán enteros. Ahora tenemos

Β

^(β - ΛΑ) μ

1

μ

1

μ

1

e

'β(1 - αΑ) - Α(α0β0 + α00β00)) + Ak α00(Α00β - Αβ00) - α0(Αβ0 - Α0β)) + Ak α00(α00β - αβ00) - α0(αβ0 - α0β)) + Ak

Es claro que B es un entero, y de la misma manera podemos mostrar que B' y B" son enteros. De estos argumentos vemos que no puede haber ninguna representación impropia de la forma φ por f que pertenezca al divisor e2 que no se pueda obtener unívocamente por el metodo que hemos utilizado.

Si tratamos los restantes divisores cuadrados de D de la misma manera y desarrollamos las representaciones pertenecientes a cada uno de ellos, tendremos todas las representaciones impropias de la forma φ por f.

A partir de esta solucion es fácil deducir que el teorema enunciado al final del artículo anterior para las representaciones propias tambien se aplica a las representaciones impropias; eso es, en general ninguna forma binaria positiva con determinante negativo puede ser representada por una forma ternaria negativa, etc. Pues, si φ fuera una forma binaria tal que de acuerdo con el teorema no pudiera ser representada propiamente por f, entonces todas las formas con determinante -§, etc. que φ implica, tampoco podrían ser representadas propiamente por f. La razán es que todas estas formas tienen determinante del mismo signo que φ, y cuando estos determinantes son negativos, todas las formas serán positivas o negativas segán φ pertenezca a formas positivas o negativas. [[200]](#footnote-201)

formas indefinidas no son equivalentes si en una los tres primeros coeficientes son todos pares y en la otra no son todos pares; en los casos restantes (los tres primeros coeficientes de ambas formas son todos pares o alguno de los tres primeros coeficientes de ambas formas es impar) las formas serán equivalentes. Podríamos mostrar muchas mas proposiciones de este carácter especial si se hubieran desarrollado mas ejemplos anteriormente (art. 277).

1. Para todos estos casos se puede encontrar una transformación de una de las formas ternarias equivalentes f y f' en la otra. Pues en todos los casos, en cualquier clase de forma ternaria hemos encontrado un nuómero suficientemente pequeño de formas tales que cualquier forma de la misma clase pueda ser reducida por metodos uniformes a una de ellas; y tambien hemos mostrado como reducirlas todas a una sola forma. Sea F esta forma de la misma clase que f y f'; por los metodos dados anteriormente se puede encontrar transformaciones de las formas f y f' en F y de la forma F en f y f'. Entonces por el artículo 270 pueden deducirse las transformaciones de la forma f en f' y de la forma f' en f.
2. Entonces solamente queda demostrar cómo obtener todas las posibles transformaciones a partir de una transformación de una forma ternaria f en otra f'. Este problema depende de un problema mas sencillo, el de encontrar todas las transformaciones de la forma ternaria f en só misma. Pues si f se transforma en só misma por varias sustituciones (τ), (τ'), (τ'0), etc. y si se transforma en f mediante la sustitución (t), es claro que se combina la transformación (t) con (τ), (τ'), (τ'0), etc. de acuerdo con la norma del artóculo 270 para producir transformaciones, cada una de las cuales llevaró f hacia f'. Mediante cólculos adicionales, es facil probar que cualquier transformacióon de la forma f en f' puede deducirse de esta manera, combinando una transformación dada (t) de f en f' junto con una (y sólo una) transformación de la forma f en só misma. Asó a partir de la combinacion de una transformación dada de f en f' con todas las transformaciones de f en só misma, se obtienen todas las transformaciones de la forma f en f', cada una de ellas sólo una vez.

Restringiremos nuestra investigacion de todas las transformaciones de la forma f en só misma al caso donde f es una forma definida cuyo 4o, 5o y 6o coeficientes son todos = 0[[201]](#footnote-202)). Por lo tanto sea f = ^0,ao,a0^, y representense las sustituciones

mediante las cuales f es transformada en sí misma por

|  |  |  |
| --- | --- | --- |
| α, | β, | γ |
| α0, | β0, | γ0 |
| α00, | β00, | γ00 |

así que las siguientes ecuaciones se cumplen

1. , t /2 . n //2

αα + αα + α α = α (Ω)

1. 2 2

αβ + αβ + α β = α

1. 2 2

αγ + αγ + α γ = α

ααβ + α'α'β0 + α"α"β" = 0 ααγ + α0α0γ0 + α00α00γ00 = 0 αβγ + α0β0γ0 + α00β00γ00 = 0

Ahora deben distinguirse tres casos:

1. Cuando α, α0 y α'0 (que tienen el mismo signo) son todos diferentes, supongamos que α < α0 y α0 < α00 (si hay un orden diferente de magnitud, las mismas conclusiones resultarán de manera similar). Entonces la primera ecuación en (Ω) evidentemente requiere que α0 = α00 = 0, por lo tanto α = ±1; entonces por las ecuaciones 4 y 5 resulta β = 0, γ = 0; similarmente de la ecuacián 2 tenemos β00 = 0 y por lo tanto β0 = ±1; ahora a partir de la ecuacion 6, γ0 = 0 y de la 3, γ00 = ±1 así pues (debido a la ambigüedad independiente de los signos) habrá en total 8 transformaciones.
2. Cuando dos de los numeros α, α0 y α00 son iguales e.g., α0 = α00 y el tercero diferente, supongamos:

Primero que α < α0. Entonces de la misma manera que en el caso anterior tendremos que α0 = 0, α00 = 0, α = ±1, β = 0, γ = 0; y a partir de las ecuaciones 2, 3 y 6 es facil deducir que o β0 = ±1, γ0 = 0, β00 = 0, γ00 = ±1 o β0 = 0, γ0 = ±1,

β00 = ±1, γ00 = 0.

Pero si, en segundo lugar, α > α0, se obtienen las mismas conclusiones de esta manera; a partir de las ecuaciones 2 y 3 resulta necesariamente β = 0, γ = 0 y ademas tenemos β0 = ±1, γ0 = 0, β00 = 0, γ00 = ±1 o β0 = 0, γ0 = ±1, β00 = ±1, γ00 = 0; en cualquier caso, a partir de las ecuaciones 4 y 5 tendremos α0 = 0, α00 = 0 y a partir de la 1, α = ±1. Y así para cada caso habrá 16 transformaciones diferentes. Los

dos restantes casos donde a = a'' o a = a' se pueden resolver de manera totalmente similar. En el primer caso necesitamos simplemente intercambiar los caracteres a, a', a" con β, β', β'' respectivamente; en el segundo caso se tienen que intercambiar con γ, γ', γ'' respectivamente.

1. Cuando todos los a, a' y a'' son iguales, las ecuaciones 1, 2 y 3 requieren que en cada uno de los tres triples α, a', a''; β, β', β''; γ, γ', γ'' dos de los números sean = 0, y el tercero = ±1. Mediante las ecuaciones 4, 5 y 6 es fúcil ver que solo uno de los tres números a, β y γ puede ser = ±1. Lo mismo es cierto de los conjuntos a', β', γ' y a'', β'', γ''. Por lo tanto solo hay seis posibles combinaciones:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| a | a | a' | a' | a'' | a'' | = ±1 |  |
| β | β'' | β | β'' | β | β' | = ±1 | Los restantes seis coeficientes serún = 0 |
| γ | γ' | γ'' | γ | γ' | γ | = ±1 |  |

y, por causa de la ambigüedad de signos, hay un total de 48 transformaciones. La misma tabla tambiúen incluye los casos anteriores, pero solamente se debe tomar la primera columna cuando a, a y a son todos diferentes; la primera y segunda cuando a' = a''; la primera y tercera cuando a = a'; la primera y sexta cuando a = a''.

En resumen, si la forma f = ax2 + a'x'2 + a''x''2 se transforma en una forma equivalente f' mediante la sustitución

x = óy + ey' + (y", x' = ó'y + ε'y' + ('y'', x'' = δ''y + e''y' + (''y'' toda transformaciúon de la forma f en f estaraú comprendida en el siguiente esquema:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| x | x' | x' | x' | x'' | x'' | = ±(óy + ey' + (y'') |
| x | x'' | x | x'' | x | x' | = ±(ó'y + e'y' + ('y'') |
| x | x' | x'' | x | x' | x | = ±(ó''y + e''y' + (''y'') |

con esta diferencia: que las seis columnas serán utilizadas en su totalidad cuando a = a' = a''; las columnas 1 y 2 cuando a' = a'' con a distinto; 1 y 3 cuando a = a'; 1 y 6 cuando a = a''; y la primera sola cuando a, a' y a'' son todos diferentes. En el primer caso, el número de transformaciones serú 48, en el segundo, tercero y cuarto 16, y en el quinto 8.

ALGUNAS APLICACIONES A LA TEORIA DE LAS FORMAS BINARIAS.

Encontrar una forma cuya duplicación produce una forma dada del género principal.

Puesto que los elementos básicos de la teoría de formas ternarias se han desarrollado de manera concisa, procederemos a algunas aplicaciones especiales. Entre ellas, el siguiente problema merece el primer lugar.

286.

PROBLEMA. Dada una forma binaria F = (A, B, C) de determinante D que pertenece al género principal: encontrar una forma binaria f cuya duplicacion nos da F.

Solucion. I. Sea F' la opuesta de la forma F. Se busca una representacián propia de F' = AT2 - 2BTU + CU2 por la forma ternaria x2 — 2yz. Suponga que es

x = aT + βυ, y = aT + β'υ, z = a''T + β"υ.

Es claro que esto se puede realizar a partir de la teoría anterior sobre formas ternarias, ya que, por hipótesis, F pertenece al genero principal, así que hay un valor para la expresión yj(A, B,C) (mod. D), a partir del cual se puede encontrar una forma ternaria φ de determinante 1 en la cual (A, —B,C) será una parte y todos sus coeficientes serán enteros. Es igualmente obvio que φ será una forma indefinida (pues por hipótesis F ciertamente no es una forma negativa); y por lo tanto será necesariamente equivalente a la forma x2 — 2yz. Por consiguiente, se podrá encontrar una transformacion de esa a φ, la cual da una representacián propia de la forma F' por la forma x2 — 2yz. Como resultado

A = a2 — 2a'a", —B = αβ — α'β'' — α''β', C = β2 — 2β'β"

ademas, designando los námeros αβ' — a'β, a' β" — a" β', a" β — aβ'' por a, b, c respectivamente, estos no tendrán un divisor comán y D = b2 — 2ac.

II. Con la ayuda de la áltima observacion del artículo 235, es facil concluár que F, mediante la sustitucion 2β', β, β, β'';2α', a, a, a'', se transformará en el producto de la forma (2a, —b, c) con ella misma, y por la sustitucián β', β, β, 2β''; a', a, a, 2a'', en el producto de la forma (a, — b, 2c) con ella misma. Ahora el maximo comán divisor de los námeros 2a, 2b y 2c es 2; por lo tanto si el námero c es

impar, los números 2a, 2b y c no tendrán un divisor común, así (2a, —b, c) será una forma propiamente primitiva; similarmente si a es impar (a, —b, 2c) será una forma propiamente primitiva. En el primer caso F será obtenida a partir de la duplicacián de la forma (2a, —b, c) y en segundo caso a partir de una duplicación de la forma (a, —b, 2c) (ver conclusion 4, art. 235). Ciertamente uno de estos casos siempre se cumplirá. En efecto, si ambas a y c fueran pares, b sería necesariamente impar; ahora es facil confirmar que β"a + βb + β'c = 0, a"a + ab + a'c = 0 y se sigue que βb y ab serán pares y así tambien lo serán a y β. De esto seguiría que A y C son pares pero esto contradice a la hipáotesis seguán la cual F es una forma del gáenero principal y asá de orden propiamente primitiva. Pero puede ocurrir que a y c sean impares. En este caso inmediatamente habraá dos formas que produciráan F mediante su duplicacioán.

Ejemplo. Propongase la forma F = (5, 2, 31) con determinante —151. Un valor de la expresion \J(5,2,31) sera (55,22); por los metodos del artículo 272 encontramos que la forma ternaria φ = 30’ es equivalente a la forma Q’

í 2- 2’ Ί

y esta se transformará en φ mediante la sustitucián ) 1, —6, —2 ); y con la

10, 3, 1J

ayuda de las transformaciones dadas en el artículo 277 encontramos que ^\_Q’ 0’ 0^

r 3, —7, —21

es transformada en φ por la sustitucion ) 2, —1, 0 ). Así pues a = 11, b = —17,

l 1, —9, —3),

c = 20; por lo tanto puesto que a es impar, F se obtendrá de la duplicacion de la forma (11, 17, 40) y se transformara en el producto de esta forma con ella misma por la sustitucion —1, —7, —7, —18; 2, 3, 3, 2.

287.

Agregamos las siguientes observaciones sobre el problema que se resolvio en el artículo anterior.

1. Si la forma F es transformada en un producto de las dos formas (h, i, k) y (h',i',k') por la sustitucion p, p, p'', p'''; q, q', q'', q''' (supongamos que cada una se toma propiamente) se tendran las siguientes ecuaciones que son facilmente deducidas de la conclusión 3 del artículo 235:

p''hn' — p'h'n — p(in' — i'n) = 0 (p'' — p')(in' + i'n) — p(kn' — k'n) + p'''(hn' — h'n) = 0

pkn — p kn — p (in — i n) = 0

y tres mas que se derivan de estas intercambiando los numeros p, p', p'', p''' y q, q', q'', q'''; n y n' son las raíces cuadradas positivas que resultan de la division de los determinantes de las formas (h,i,k) y (h',ir,k') por el determinante de la forma F. Así, si estas formas son identicas, eso es, n = n', h = h', i = i', k = k, las ecuaciones seran

(p'' — p' )hn = 0, (p'' — p' )in = 0, (p'' — p' )kn = 0

y necesariamente p' = p'' y similarmente q' = q''. Por lo tanto, asignando a las formas (h,i,k) y (h',ir,k') las mismas incognitas t y u y designando las incognitas de F por T y U, entonces F sera transformada por la sustitucion

T = pt2 + 2p'tu + p'''u2, U = qt2 + 2q'tu + q'''u2 en (ht2 + 2itu + ku2)2

1. Si la forma F se obtiene a partir de una duplicacion de la forma f, sera tambien obtenida a partir de una duplicacion de cualquier otra forma contenida en la misma clase que f; eso es, la clase de la forma F se obtendrá a partir de una duplicacion de la clase de la forma f (ver art. 238). Así en el ejemplo del artículo anterior, (5, 2, 31) tambien se obtendrá de una duplicacion de la forma (11, —5, 16) la cual es propiamente equivalente a la forma (11, 17, 40). A partir de una clase que por duplicacion produce a la clase de la forma F, se encuentran todas (si hay mas que una) aquellas clases con la ayuda del problema 260; en nuestro ejemplo no hay ninguna otra clase positiva porque existe solo una clase ambigua positiva propiamente primitiva de determinante —151 (la clase principal); y puesto que, a partir de la composicion de la unica clase ambigua negativa (—1, 0, —151) con la clase (11, —5, 16) resulta la clase (—11, —5, —16), esta sera la unica clase negativa y de su duplicacion resulta la clase (5, 2, 31).
2. Puesto que por la solucion del problema del artículo anterior queda claro que cualquier clase propiamente primitiva (positiva) de formas binarias perteneciendo al genero principal se puede obtener de la duplicacion de alguna clase propiamente primitiva del mismo determinante, podemos ampliar el teorema del artículo 261. Este teorema afirmaba que podríamos estar seguros de que al menos la mitad de todos los

caracteres asignables para un determinante no cuadrado D no pueden corresponder a generos propiamente primitivos (positivos). Ahora podemos decir que exactamente la mitad de todos estos caracteres corresponden a tales generos y ninguno de los de la otra mitad puede corresponder a ellos (ver demostración del teorema). En el artículo 264 distribuimos todos esos caracteres entre dos grupos iguales P y Q. Se probo que ninguno de los de Q puede corresponder a formas propiamente primitivas (positivas). Aón se dudaba de si había generos que correspondían a cada uno de los caracteres de

P. Ahora la duda se ha aclarado y estamos seguros de que entre el conjunto completo de caracteres de P no hay ninguno que no corresponda a un genero. Se mostró en el artículo 264, I que para un determinante negativo es imposible para P y sólo posible para Q el tener miembros en un orden negativo propiamente primitivo. Mostraremos en efecto que todos los miembros de Q son posibles. Si K es cualquier carácter en

Q, f una forma arbitraria en el orden de formas negativas propiamente primitivas de determinante D, y K' su carócter, entonces K' estará en Q; a partir de esto es fócil ver que el carácter compuesto por K y K' (según la norma del art. 246) pertenece a P y entonces hay formas propiamente primitivas positivas de determinante D que le corresponden. La composición de esta forma con f da raíz a una forma propiamente primitiva negativa de determinante D cuyo carácter sera K. De manera similar se prueba que aquellos caracteres en un orden impropiamente primitivo, que seguón los metodos de los artículos 264 II, III resultan ser los únicos posibles, son realmente del todo posibles, independientemente de si pertenecen a P o a Q. Creemos que estos teoremas esrán entre los mós bellos de la teoría de las formas binarias, especialmente porque, a pesar de ser sumamente simples, son tan profundos que sus demostraciones rigurosas requieren de muchas otras investigaciones.

La teoría de la descomposicion de números y formas binarias en tres cuadrados.

Veamos ahora otra aplicación de la divagación anterior, la descomposición de nómeros y formas binarias en tres cuadrados. Empezamos con lo siguiente. [[202]](#footnote-203)

Solución. Designemos por Ω el conjunto de todos los caracteres particulares que dan las relaciones del número 1 tanto a los divisores primos (impares) de M como a los numeros 8 o 4 cuando divide a M. Estos caracteres serán Rp, Rp0, Rp", etc., donde p, p0, p00, etc. son los divisores primos, y 1, 4 cuando 4 divide a M; 1,8 cuando 8 divide a M. Ademas utilizaremos las letras P y Q con el mismo significado que en el artículo anterior y en el artículo 264. Ahora distinguimos los siguientes casos.

1. Cuando M es divisible por 4, Ω serú un carácter completo, y es claro por el artículo 233 V que 1 puede ser un número característico solamente de aquellas formas cuyo carúcter es Ω. Pero es claro que Ω es el carácter de la forma principal (1, 0,M) y así pertenece a P y no puede resultar de una forma propiamente primitiva negativa; por lo tanto, puesto que no hay formas impropiamente primitivas para este determinante, en este caso no habrá formas primitivas negativas que sean residuos de M.
2. Cuando M ξ 3 (mod. 4) el mismo razonamiento es valido con la excepciún de que en este caso existe un orden impropiamente primitivo negativo en el cual los caracteres P serún posibles o no según M ξ 3 o M ξ 7 (mod. 8) (ver art. 264 III). En el primer caso habrá un genero para este orden cuyo carácter es Ω, asú 1 sera el numero característico de todas las formas contenida en ella; en el segundo caso no puede haber ninguna forma negativa con esta propiedad.
3. Cuando M ξ 1 (mod. 4), Ω aún no es un carácter completo, pero debemos agregarle una relacioún con el nuúmero 4; es claro sin embargo, que Ω debe pertenecer al caraúcter de una forma cuyo nuúmero caracterústico es 1, y recúprocamente cualquier forma cuyo carácter es o Ω; 1, 4, o Ω; 3, 4, tiene 1 como número caracterústico. Ahora Ω; 1, 4 es claramente el caraúcter del gúenero principal que pertenece a P y por lo tanto es imposible dentro de un orden propiamente primitivo negativo; por la misma razón Ω; 3, 4 pertenecerá a Q (art. 263). Por esto habrá un gúenero correspondiente al orden propiamente primitivo negativo de todas aquellas formas que tendraún 1 como nuúmero caracterústico. En este caso, tal como en el siguiente no habrá ningun orden impropiamente primitivo.
4. Cuando M ξ 2 (mod. 4) debemos agregarle a Ω una relaciún con 8 para obtener un carúcter completo. Estas relaciones serán 1 y 3,8ú5 y 7, 8 cuando M ξ 2 (mod. 8); y ú 1 y 7, 8 ú 3 y 5, 8 cuando M ξ 6 (mod. 8). En el primer caso el carúcter Ω; 1 y 3, 8 evidentemente pertenecerán a P y asú Ω; 5 y 7, 8 a Q. Como consecuencia de esto, habrá un genero propiamente primitivo negativo que le corresponde. Por una razón similar, en el segundo caso habrá un genero en el orden

propiamente primitivo negativo, cuya forma tiene la propiedad prescrita; eso es, su carácter es Ω; 3 y 5, 8.

A partir de todo eso se sigue que no hay formas primitivas negativas de determinante — M con número característico 1 excepto cuando M es congruente con uno de los números 1, 2, 3, 5 ú 6 segun el modulo 8 y ellos pertenecerún a solo un genero, que es impropio cuando M = 3; no hay tales formas cuando M = 0, 4 ú 7 (mod. 8). Pero si (—a, —b, —c) es una forma primitiva negativa con número característico +1, (a, b, c) sera una forma primitiva positiva con número característico — 1. De esto es claro que en los cinco casos anteriores (cuando M ξ 1, 2, 3, 5, 6) hay un genero primitivo positivo cuyas formas tienen número característico —1, y es impropio si M ξ 3; sin embargo en el último de los tres casos (cuando M ξ 0, 4, 7) no hay tales formas positivas.

289.

En cuanto a las representaciones propias de las formas binarias por la forma ternaria x2 + y2 + z2 = f, podemos obtener lo siguiente a partir de la teoría general del artúculo 282.

1. La forma binaria φ no se puede representar propiamente por f a menos que sea una forma positiva primitiva y —1 (i.e., el determinante de la forma f) sea su numero característico. Asú para un determinante positivo y ademas para un determinante negativo —M, cuando M es divisible por 4 o es de la forma 8n + 7, no hay formas binarias propiamente representables por f.
2. Ahora si φ = (p,q,r) es una forma positiva primitiva de determinante —M, y —1 es un numero característico de la forma φ y tambien de la forma opuesta (p, —q,r), habra una representación propia de la forma φ por f que pertenece a cualquier valor de la expresion ^ — (p, —q,r). Eso es, todos los coeficientes de la forma ternaria g de determinante —1 (art. 283) necesariamente serán enteros, la forma g serú definida y asú equivalente a f (art. 285.I).
3. Por el artículo 283.III el número de representaciones que pertenecen al mismo valor de la expresión yj — (p, —q, r) en todos los casos, excepto cuando M = 1 y M = 2, es igual en magnitud al numero de transformaciones de la forma f en g, y asú, por el artículo 285, = 48; asú si se conoce una representacion que pertenece a un valor dado, los 47 restantes se pueden obtener a partir de ella permutando los valores de x, y, z en todas las maneras posibles y cambiando sus signos; como resultado,

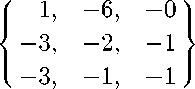
las 48 representaciones presentarán una sola descomposición de la forma φ en tres cuadrados, si consideramos los cuadrados en si y no su orden o el signo de sus raíces.

1. Sea μ el nómero de todos los enteros primos impares diferentes que dividen a M; no es difícil concluir del artículo 233 que el nómero de valores diferentes de la expresión \J — (p, -q,r) (mod. M) seró = 2μ, donde, segun el artículo 283, necesitamos considerar solo la mitad de estos (cuando M > 2). Por lo tanto el nómero de todas las representaciones propias de la forma φ por f sera = 48 · 2μ-1 = 3 · 2μ+3; pero el número de descomposiciones diferentes en tres cuadrados es = 2μ-1.

Ejemplo. Sea φ = 19t2 + 6tu + 41u2, de modo que M = 770; aquí se debe considerar (art. 283) los cuatro valores siguientes de la expresion —(19, —3,41)

(mod. 770): (39, 237), (171, —27), (269, —83), (291, —127). Para encontrar las

representaciones que pertenecen a los valores (39, 237), debemos determinar la forma ternaria ^3’ 4β’ 3) = V Mediante los metodos de los artículos 272 y 275, encontramos que f se transformara en esta forma por la sustitucion



y la representacion de la forma φ por f es:

x = t — 6u, y = —3t — 2u, z = —3t — u

Por razones de brevedad no escribiremos las 47 representaciones restantes que pertenecen a ese mismo valor, las cuales resultan de las permutaciones de estos valores y el cambio de signos. Todas las 48 representaciones producen la misma descomposicion de la forma φ en tres cuadrados

t2 — 12tu + 36u2, 9t2 + 12tu + 4u2, 9t2 + 6tu + u2.

De manera similar el valor (171, —27) dará una descomposicion en cuadrados (3t + 5u)2, (3t — 4u)2, t2; el valor (269, —83) dará (t + 6u)2 + (3t + u)2 + (3t — 2u)2; y finalmente el valor (291, —127) dará (t + 3u)2 + (3t + 4u)2 + (3t — 4u)2; cada una de estas descomposiciones es equivalente a 48 representaciones. Fuera de estas 192 representaciones o cuatro descomposiciones no hay otras, puesto que 770 no es divisible por ningun cuadrado y por lo tanto no puede haber ninguna representacion impropia.

290.

Las formas de determinante —1 y —2 están sujetas a ciertas excepciones, así que diremos un poco sobre ellas como caso particular. Empezamos con la observacián general de que si φ y φ' son dos formas binarias equivalentes cualesquiera, (Θ) una transformación dada de la primera en la segunda, entonces combinando cualquiera de las representaciones de φ por la forma ternaria f con la sustitucion (Θ), se obtiene una representacián de la forma φ' por f. Además a partir de las representaciones propias de φ obtenemos las representaciones propias de la forma φ', a partir de representaciones distintas de φ obtenemos representaciones distintas de φ0 y si tomamos todas las representaciones de la primera obtendremos todas las representaciones de la segunda. Todo esto se puede comprobar mediante cálculos muy sencillos. Por lo tanto una de las formas φ y φ' es representable por f de tantas maneras distintas como lo es la otra.

1. Primero sea φ = t2 + u2 y φ' una forma binaria positiva cualquiera de determinante —1, a la cual φ es equivalente. Sea t = at' + βν!, u = yt' + δη' la sustitucián que transforma φ en φ'. La forma φ se representa por la forma ternaria f = x2 + y2 + z2, poniendo x = t, y = u, z = 0; permutando x, y, z resultan seis representaciones, y a partir de cada una de estas, cuatro mas cambiando los signos de t y u. Así pues habrá en total 24 representaciones que corresponden a solo una descomposicián en tres cuadrados. Es facil ver que no habra ninguna otra representacián salvo estas. Y se concluye que la forma φ' se puede descomponer en tres cuadrados de solo una manera, a saber, (at' + βΥ)2, (yt' + δΥ)2 y 0. Esta descomposicián sera equivalente a las 24 representaciones.
2. Sea φ = t2 + 2u2, φ' cualquier otra forma binaria positiva de determinante —2, en la cual se transforma φ mediante la sustitucián t = at' + β^, u = yt' + δ^. Entonces de manera similar que en el caso anterior concluimos que φ y tambien φ' se pueden descomponer en tres cuadrados de manera única, a saber, φ en t2 + u2 + u2 y φ' en (at' + β^)2 + (yt' + δ^)2 + (yt' + δ^)2; es obvio que esta descomposicion es equivalente a las 24 representaciones.

De todo esto se sigue que las formas binarias de determinante —1 y —2 en cuanto al námero de representaciones por la forma ternaria x2 + y2 + z2 son completamente iguales a las otras formas binarias; puesto que en ambos casos tenemos μ = 0, la fármula dada en IV del artículo anterior dará las 24 representaciones. La razoán para esto es que las dos excepciones a las cuales estáan sujetas estas formas se compensan mutuamente.

Por razones de brevedad omitiremos la aplicación, a la forma x2 + y2 + z2, de la teoría general respecto a representaciones impropias dada en el artículo 284.

291.

El problema de encontrar todas las representaciones propias de un número positivo M por la forma x2 + y2 + z2 se reduce primeramente en el artículo 281 a la investigación de las representaciones propias del nómero — M por la forma

—x2 — y2 — z2 = f; por los metodos del artículo 280 estas se pueden encontrar

de la siguiente manera.

1. Encontramos todas las clases de formas binarias de determinante — M

cuyas formas se pueden representar propiamente por X2 + Y2 + Z2 = F (la cual tiene a f como adjunta). Cuando M ξ 0, 4 o 7 (mod. 8), por el artículo 288 no

hay tales clases y entonces M no se puede descomponer en tres cuadrados que no

tienen un divisor comón [[203]](#footnote-204)). Pero cuando M ξ 1, 2, 5 o 6, habrá un genero positivo propiamente primitivo, y cuando M ξ 3 uno impropiamente primitivo que incluye todas aquellas clases. Designemos el nómero de estas clases por k.

1. Ahora escoja arbitrariamente una forma de cada una de estas k clases y llamelas φ, φ', φ'', etc.; investigue todas las representaciones propias de cada una de estas por F. El numero de ellas será 3 · 2μ+3k = K, donde μ es el número de factores primos (impares) de M; finalmente a partir de cada una de estas representaciones, tales como

X = mt + nu, Y = m't + n'u, Z = m"t + n"u

derivamos la siguiente representación de M por x2 + y2 + z2:

x = m'n'' — m''n', y = m''n — mn'', z = mn' — m'n

Todas las representaciones de M esrán contenidas en el conjunto, que designaremos por Ω, de estas K representaciones.

1. Sólo queda determinar si hay algunas representaciones en Ω que sean idénticas; y puesto que del artículo 280.III esta claro que aquellas representaciones

en Ω que se obtienen de diferentes formas, e.g., de φ y φ' deben ser distintas, la única pregunta que queda es si diferentes representaciones de la misma forma e.g., φ por F pueden dar lugar a representaciones identicas del número M por x2 + y2 + z2. Ahora es inmediatamente evidente que si entre las representaciones de φ encontramos

X = mt + nu, Y = mt + n'u, Z = m't + n''u (r)

tambien encontraremos entre las mismas representaciones

X = —mt — nu, Y = -m't — n'u, Z = —m'' t — n'u (r')

y a partir de cada una podemos obtener la misma representación de M que llamaremos (R); examinemos por lo tanto si la representaciún (R) puede obtenerse todavía de otras representaciones de φ. A partir del artículo 280.III, si hacemos que χ = φ y si exhibimos todas las transformaciones de la forma propia φ en sí misma por

t = at + ^u, u = yt + Su

podemos deducir que todas aquellas representaciones de la forma φ a partir de la cual se obtiene R serúan expresadas por

x = (am + yn)t + (^m + Sn)u y = (am' + yn )t + (^m' + Sn')u z = (am'' + yn")t + (^m'' + Sn")u

Pero de la teoría de la transformacion de formas binarias con determinante negativo como se explico en el artículo 179, se sigue que en todos los casos, excepto cuando M = 1 y M = 3, hay solo dos transformaciones propias de la forma φ es sí misma, a saber, α, β, y, S = 1, 0, 0, 1 y = —1, 0, 0, —1 respectivamente (pues como φ es una forma primitiva, el número que designamos en el artículo 179 por m sera ú 1 ú 2 y así, excepto en los casos que se excluyeron, 1) ciertamente sera aplicable). Por lo tanto (R) puede aparecer súlo a partir de r, r' y cada una de las representaciones propias del número M se encontrarú dos veces, y no mas en Ω; y el numero de representaciones propias de M será 2K = 3 · 2^+2k.

En cuanto a los casos que se excluyeron, el numero de transformaciones propias de φ en sí misma, con base en el artículo 179 serán 4 para M = 1 y 6 para M = 3; y es facil comprobar que el numero de representaciones propias de los números 1 y

1. es ^K y 6K respectivamente; eso es cada número se puede descomponer en tres cuadrados de una manera única, 1 en 1 + 0 + 0, 3 en 1 + 1 + 1. La descomposición de 1 proporciona seis, la descomposiciún de 3, ocho representaciones diferentes, ahora para M = 1 tenemos K = 24 (aquí μ = 0, k = 1) y para M = 3 tenemos K = 48 (aquí μ = 1, k = 1).

Sea h el número de clases en el genero principal. Por artículo 252 sera igual al número de clases en cualquier otro genero propiamente primitivo. Observamos que k = h para M ξ 1, 2, 5 o 6 (mod. 8), pero k = 1 h para M ξ 3 (mod. 8), excepto en el caso de M = 3 (donde k = h = 1). Así, el numero de representaciones, en general, de numeros de la forma 8n + 3 es = 2^+2h, puesto que para el numero 3 las dos excepciones se compensan entre sí.

292.

Hemos distinguido la descomposicion de numeros (y tambien de formas binarias) en tres cuadrados por representaciones de la forma x2+y2+z2, de tal manera que en el primero nos preocupamos unicamente por la magnitud de los cuadrados y en el segundo tambien consideramos el orden de las raíces y sus signos. Así, consideramos que las representaciones x = a, y = b, z = c y x = a!, y = b', z = c' son distintas a menos que a = a', b = b', c = c' simultaneamente; y tomamos las descomposiciones en a2 + b2 + c2 y en a' + b' + c' como la misma si, sin considerar el orden, los cuadrados en una son iguales a los cuadrados en la otra. De esto es claro:

1. Que la descomposicion del numero M en a2 + b2 + c2 es equivalente a 48 representaciones si ninguno de los cuadrados es = 0 y si todos son distintos entre sí; pero sólo a 24 si alguno es = 0 y los otros son distintos entre sí, o ninguno es = 0 y dos son iguales. Sin embargo, si en la descomposicion de un numero dado en tres cuadrados dos de los cuadrados = 0, ó uno = 0 y los restantes iguales entre sí, o todos son iguales entre sí, la descomposicion sera equivalente a 6 o 12 o 18 representaciones; pero esto no puede suceder a menos que tengamos el caso especial de M = 1 o 2 o 3, respectivamente, por lo menos si se quiere que las representaciones sean propias. Excluyendo estos tres casos, supongamos que el numero de descomposiciones de un número M en tres cuadrados (que no tienen un divisor común) es E, y que entre ellas tenemos e descomposiciones en las cuales un cuadrado es 0, y e' en las cuales dos cuadrados son iguales; el primero se puede considerar como descomposiciones en dos cuadrados y el segundo como descomposiciones en un cuadrado y dos veces un cuadrado. Entonces el numero de representaciones propias del numero M por

9 9 9 '

x + y + z9 sera

= 24(e + e0) + 48(E - e - e0) = 48E - 24(e + e0)

Pero de la teoría de formas binarias es facil ver que e sera = 0 o = 2μ-1, según — 1 sea un no residuo o sea un residuo cuadrútico de M, y que e0 serú 2μ-1 ú = 0 segun —2 sea o no un residuo de M. Aquí μ es el número de factores primos (impar) de M (ver art. 182; omitimos aquú una exposición mas completa). De todo esto tenemos

E = 2^-9k, si ambos —1 y —2 son no residuos de M;

E = 2^-9(k + 2), si ambos números son residuos;

E = 2^-9(k +1), si uno es un residuo y el otro un no residuo.

En los casos excluidos donde M = 1 y M = 2 esta fúrmula haría que E = 3, mientras que debio haber sido E = 1. Sin embargo, para M = 3 obtenemos el valor correcto, E = 1, porque las excepciones se compensan mutuamente.

Por lo tanto si M es un número primo, resulta μ = 1 y asú E = 9¡(k + 2)

cuando M ξ 1 (mod. 8); E = 9¡ (k + 1) cuando M ξ 3 o M ξ 5. Estos teoremas

especiales fueron descubiertos por el ilustre Legendre por métodos de inducciún y fueron publicados por el en aquel comentario esplendido que hemos citado a menudo, Hist. de l’Ac. de Paris 1785, p. 530 y siguientes. Si lo presentú de manera un poco distinta es porque no distinguio entre equivalencias propias e impropias y asú mezclo clases opuestas.

1. Para encontrar todas las descomposiciones de un número M en tres cuadrados (sin un divisor común) no es necesario obtener todas las representaciones propias de todas las formas φ, φ' y φ". En efecto, es facil comprobar que todas las (48) representaciones de la forma φ que corresponden al mismo valor de la expresión \J—(p, —q, r) (donde φ = (p,q,r)) darán la misma descomposiciún del número M, asú es suficiente si tenemos una de ellas, o lo que es lo mismo, si conocemos todas las descomposiciones [[204]](#footnote-205)) diferentes de la forma φ en tres cuadrados. Lo mismo es cierto para las restantes φ', φ00, etc. Ahora si φ pertenece a una clase no ambigua, es permitido ignorar la forma que fue escogida de la clase opuesta; eso es, es suficiente considerar súolo una de las dos clases opuestas. Pues, ya que es completamente arbitrario cuúal forma seleccionamos de una clase, supongamos que se escoge la forma

φ' de la clase opuesta a la que contiene φ, la cual es opuesta a la forma φ. Entonces no es difícil mostrar que si se representan las descomposiciones propias de la forma φ por la expresión general

(gt + hu)2 + (g't + h'u)2 + (g''t + h''u)2

todas las descomposiciones de la forma φ0 seróan expresadas por

(gt — hu)2 + (g't — h'u)2 + (g"t — h''u)2

y la misma descomposición del nómero M se obtendró de ambas. Finalmente, para el caso en el cual φ es de una clase ambigua, pero no de la clase principal ni equivalente a la forma (2, 0, ^M) o (2, 1, 2(M + 1)) (segón M sea par o impar), es permitido omitir la mitad de los valores de la expresion \J — (p, —q,r); pero para brevedad no daremos los detalles de esta simplification. Tambien podemos utilizar estas simplificaciones cuando queremos todas las representaciones propias de M por x2 + y2 + z2, puesto que esto se puede obtener muy fóacilmente a partir de las descomposiciones.

Como ejemplo investigaremos todas las descomposiciones del nómero 770 en tres cuadrados. Aquí μ = 3, e = e' = 0 y así E = 2k. Puesto que es facil utilizar las normas del artóculo 231 para clasificar las formas binarias positivas de determinante —770, omitiremos esta operation para brevedad. Encontramos que el nómero de clases positivas es = 32. Todas ellas son propiamente primitivas y estan distribuidas entre ocho generos de modo que k = 4 y E = 8. El genero cuyo nómero característico es —1 claramente tiene los caracteres particulares R5; N7; N11 con respecto a los numeros 5, 7 y 11, y por el artículo 263 concluimos que su carácter respecto al numero 8 debe ser 1 y 3, 8. Ahora, en el genero con carácter 1 y 3, 8; R5; N7; N11 encontramos cuatro clases. De ellas escogemos las siguientes como representantes (6, 2,129), (6, —2,129), (19, 3,41), (19, —3,41) y rechazamos la segunda y cuarta puesto que son opuestos de la primera y tercera. En el artículo 289 dimos cuatro descomposiciones de la forma (19, 3,41). A partir de estas obtenemos las descomposiciones del numero 770 en 9 + 361 + 400; 16 + 25 + 729, 81 + 400 + 289, 576 + 169 + 25. Similarmente podemos encontrar cuatro descomposiciones de la forma 6t2 + 4tu + 129u2 en

(t — 8u)2 + (2t + u)2 + (t + 8u)2, (t — 10u)2 + (2t + 5u)2 + (t + 2u)2

(2t — 5u)2 + (t + 10u)2 + (t + 2u)2, (2t + 7u)2 + (t — 8u)2 + (t — 4u)2

Estos provienen directamente de los valores (48,369), (62, -149), (92, -159), (202, 61) de la expresión yj-(6, -2, 129). Como resultado tenemos la descomposición del número 770 en 225 + 256 + 289, 1 + 144 + 625, 64 + 81 + 625, 16 + 225 + 529. Y no hay descomposiciones fuera de estas ocho.

En cuanto a la descomposición de números en tres cuadrados que tienen divisores comunes, se sigue tan facilmente a partir del teorema general del artículo 281 que no hace falta recordarlo aquó.

Demostración de los Teoremas de Fermat: todo entero  
puede descomponerse en tres números triangulares o cuatro cuadrados.

293.

Los argumentos anteriores tambien proveen una demostracion de aquel famoso teorema: cualquier entero positivo puede descomponerse en tres numeros triangulares que fue descubierto por Fermat, pero cuya prueba rigurosa se deseaba hasta ahora. Es claro que cualquier descomposición del número M en números triangulares

1. x(x + 1) + 1 y(y + 1) + 1 z(z + 1)

producirá la descomposicion del número 8M + 3 en tres cuadrados impares

(2x + 1)2 + (2y + 1)2 + (2z + 1)2

y vice versa. Por la teoría anterior, cualquier entero positivo 8M + 3 se puede resolver en tres cuadrados que necesariamente serán impares (ver nota del artúculo 291); y el número de resoluciones depende tanto del número de factores primos de 8M + 3 como del nuúmero de clases entre las cuales estúan distribuidas las formas binarias de determinante -(8M + 3). Habrá el mismo número de descomposiciones del número M en tres números triangulares. Sin embargo, hemos supuesto que para cualquier valor entero de x el numero 2x(x+1) se ve como un número triangular; y si preferimos excluir al cero el teorema debe cambiarse como sigue: Cualquier entero positivo es o triangular o resoluble en dos o tres números triangulares. Un cambio similar se tendría que realizar en el siguiente teorema si quisieramos excluir al cero como un cuadrado.

A partir de los mismos principios se demuestra otro teorema de Fermat que dice que cualquier entero positivo se puede descomponer en cuatro cuadrados. Si

restamos de un número de la forma 4n + 2 cualquier cuadrado (menor que el número), de un numero de la forma 4n + 1 un cuadrado par, de un numero de la forma 4n + 3 un cuadrado impar, el residuo en todos estos casos sera resoluble en tres cuadrados, y el numero dado, por lo tanto, en cuatro. Finalmente, un número de la forma 4n puede representarse como 4PN de tal manera que N pertenezca a una de las tres formas anteriores; y cuando N estú resuelto en cuatro cuadrados, 4PN serú tambien resoluble. Podríamos tambien remover de un número de la forma 8n + 3 el cuadrado de un raíz ξ 0 (mod. 4), de un numero de la forma 8n + 7 el cuadrado de un raíz ξ 2 (mod. 4), de un número de la forma 8n + 4 un cuadrado impar y el residuo sera resoluble en tres cuadrados. Pero este teorema ya ha sido probado por el ilustre Lagrange, Nouv. Mém. de l’Ac. de Berlin, 1770, p. 123. Y el ilustre Euler lo explico mucho mas completamente (de manera diferente de la nuestra) en Acta Ac. Petr. II, p. 48. Hay otros teoremas de Fermat que son como continuaciones de los anteriores. Dicen que cualquier entero es resoluble en cinco números pentagonales, seis hexagonales, siete heptagonales, etc. Pero auún les hace falta la prueba y parecen necesitar principios distintos para su resoluciúon.

Solución de la ecuación ax2 + by2 + cz2 = 0.

294.

TEOREMA. Si los numeros a, b y c son primos relativos y ninguno = 0 ni es divisible por un cuadrado, la ecuacion

ax2 + by2 + cz2 = 0 ... (Ω)

no se puede resolver con enteros (excepto cuando x = y = z = 0, lo cual no vamos a considerar), a menos que -bc, -ac y -ab respectivamente sean residuos cuadréticos de a, b y c y estos números tengan signos diferentes; pero cuando estas cuatro condiciones se cumplen, (Ω) se podrá resolver con enteros.

Demostracion. Si (Ω) es realmente resoluble por enteros, será tambien resoluble por valores de x, y y z que no tienen un divisor común; pues cualesquiera valores que satisfacen la ecuaciún (Ω) tambien la satisfarán si se dividen por su maximo comun divisor. Ahora supongamos que ap2 + bq2 + cr2 = 0 y que p, q y r no tienen un divisor común, tambien serán primos relativos dos a dos, pues si q y r tuvieran un divisor comun μ, sería primo relativo a p, pero μ2 dividiría a ap2 y así tambien a a, contrario a la hipótesis, similarmente p, r; p, q deben ser primos relativos. Por esto

—ap2 se representa por una forma binaria by2 + cz2 asignando a y y z los valores q y r, primos relativos; así su determinante — bc será un residuo cuadrático de ap2 y así tambien de a (art. 154); de la misma manera tendremos —acRb, —abRc. En cuanto a la condición de que (Ω) no admite una resolución si a, b y c tienen el mismo signo, es tan obvio que no necesita una explication.

Para demostrar la proposition inversa que constituye la segunda parte del teorema, mostraremos primero, como encontrar una forma ternaria que sea equivalente a ^0’ 0’ 0^ ...f y escogida tal que los coeficientes segundo, tercero y cuarto sean divisibles por abc; y segundo, deduciremos una solution de la ecuacion (Ω) a partir de esto.

1. Se buscan tres enteros A, B y C que no tengan un divisor comán y escogidos de tal manera que A sea primo relativo a b y c; B sea primo relativo a a y c y C primo relativo a a y b. Entonces aA2 + bB2 + cC2 sera divisible por abc segán se ve de lo siguiente. Sean A, B y C respectivamente valores de las expresiones V—bc (mod. a ), —ac (mod. b) y V—ab (mod. c) que necesariamente serán primos relativos a a, b y c respectivamente. Ahora escoja tres enteros arbitrarios a, b y c con la unica condicián de que sean primos relativos a a, b y c respectivamente (e.g. sean todos = 1) y determine A, B y C tales que

A = bc (mod. b) y = cC (mod. c)

B = ca (mod. c) y = aA (mod. a)

C = ab (mod. a) y = bB (mod. b)

Entonces resulta

aA2 + bB2 + cC2 = a2(bA2 + cb2) = a2(bA2 — A2b) = 0 (mod. a)

Así será divisible por a y similarmente por b y por c y tambien por abc . Ademas es evidente que A necesariamente es primo relativo a b y c; B a a y c;y C a a y b. Ahora, si los valores A, B y C resultan tener un (maximo) comun divisor μ, este necesariamente sera primo relativo a a, b y c, y tambien a abc; por lo tanto si dividimos estos valores por μ obtendremos nuevos valores que no tienen un divisor comun y que producirán un valor de aA2 + bB2 + cC2 que aun sera divisible por abc, y así satisface a todas las condiciones.

1. Si determinamos los numeros A, B y C de esta manera, los numeros Aa, Bb y Cc tampoco tendran un divisor comun. Pues si tuvieran un divisor comun μ,

necesariamente tendría que ser primo relativo a a (el cual, de hecho, es primo relativo a Bb y Cc) y similarmente a b y c; por lo tanto μ tambien tendría que ser divisor de A, B y C contrario a la hipótesis. Por lo tanto podrán encontrarse enteros α, β y γ tales que aAa + βBb + γCc = 1. Ademas, básquense seis enteros α0, β0, γ0, α00, β00 y γ00 tales que

βγ — γβ = Aa, γα — αγ = Bb, αβ — βα = Cc

Ahora f se transformara por la sustitucion

|  |  |
| --- | --- |
| α0, | α00 |
| β0, | β00 |
| „ / |  |
| γ, | γ00 |

α,

β,

γ,

en m = g (que será equivalente a f) y digo que m0, m00 y n serán divisibles por abc. Pues, sea

β00γ — γ 00β = A0,

βγ0 — γβ0 = A00,

γ00α — α00γ = B0, γα0 — αγ0 = B00,

α00β — β00 α = C0 αβ0 — βα0 = C00

y tendremos

α0 = B00Cc — C00Bb, α00 = C0Bb — B0Cc,

β0 = C00Aa — A00Cc, β00 = A0Cc — C0Aa,

γ0 = A00Bb — B00Aa γ00 = B0Aa — A0Bb

Si sustituimos estos valores en las ecuaciones

0 02 , 7 /702 , 02

m = ao + bβ + cγ [[205]](#footnote-206)

i.e. m', m" y n serán divisibles por a; de manera similar se muestra que los mismos números son divisibles por b y por c y así que son divisibles por abc Q. E. P.

1. Pongamos, por razones de elegancia, d igual al determinante de las formas f y g, i.e. el numero —abc. Entonces

md = M, m = M'd, m'' = M''d, n = Nd, n = N', n" = N''

Esta claro que f se transforma por la sustitución (S)

ad, α', α''

βd, β', β" γ , γ"

en la forma ternaria NN" = g de determinante d3 que por lo tanto estará

contenida en f. Ahora digo que la forma 0 0^ = g" es necesariamente equivalente

claro que ( M M/’ tN/rá = g"' es una forma ternaria de determinante 1;

a g. Pues es

ademas, puesto que por hipotesis a, b y c no pueden tener el mismo signo, f sera una forma indefinida y facilmente se concluye que g' y g" tambien deben ser indefinidas; por lo tanto g''' sera equivalente a la forma Q’ 0’ 0^ (art. 277), y se podra encontrar una transformacion (S') de g"' en sí misma; es claro sin embargo que (S') dará una transformation de g' en g". Por lo tanto g'' tambien estará contenida en f y mediante una combination de las sustituciones (S) y (S') se deduce una transformacion de f en g''. Si esta transformacion es

δ, δ', δ''

ε, ε*'*, ε*''*

ζ, ζ*'*, ζ*''*

claramente tenemos una doble solution de la ecuacion (Ω), a saber x = δ', y = ε', z = ζ' y x = δ'', y = ε'', z = ζ''; de manera similar es claro que no todos estos valores pueden ser = 0 a la vez, puesto que debemos tener

δε*'*ζ*''* + δ*'*ε*''*ζ + δ*''*εζ*'* — δε*''*ζ*'* — δ*'*εζ*''* — δ*''*ε*'*ζ = d *Q*. *E*. *S*.

Ejemplo. Sea 7x2 — 15y2 + 23z2 = 0 la ecuacion propuesta. Es resoluble porque 345R7, —161R15, 105R23. Aquí los valores A, B y C serán 3, 7 y 6;

haciendo a = b = c = 1 encontramos que A = 98, B = -39 y C = -8. De

( 3, 5, 22

esto obtenemos la sustitución < -1, 2, — 28 ^ mediante la cual f se transforma

1. 8, 25, -7.

|  |  |  |  |
| --- | --- | --- | --- |
| , 14490, , -1246, | -7245 λ 4735 J = g. | Y | como r |
|  | r 7245, | 5, | 22 |
| (S ) = | 1 -2415, | 2, | -28 |
|  | 1 19320, | 25, | -7 |
| g000 se | transforma | en | 11, 0, 0 λ 1, 0, 0 |

(-2

en

3670800, 6, -3'

-1, -1246, 4735

|  |  |  |
| --- | --- | --- |
| 3, | 5, | 1 |
| 2440, | -4066, | -813 |
| 433, | 722, | 144 |

Si combinamos esto con (S) obtenemos:

r 9, ii, 1 -1, 9,



que transformará f en g''. Tenemos entonces una solucion doble de la ecuación propuesta x = 11, y = 9, z = 4 y x = 12, y = -9, z = 3; la segunda solucion se simplifica dividiendola por su divisor comán 3 y tenemos x = 4, y = -3, z = 1.

295.

La segunda parte del teorema de la seccion anterior tambien se puede resolver como sigue. Se busca un entero h tal que ah = C (mod. c) (le asignamos los mismos significados a los caracteres A, B y C, que en el artículo anterior) y resulta ah2 + b = ci. Es facil ver que i es un entero y que -ab es el determinante de la forma binaria (ac, ah, i) ...φ. Ciertamente esta forma no será positiva (puesto que como por hipótesis a, b y c no tienen el mismo signo, ab y ac no pueden ser positivos simultaneamente); además tendrá el numero característico -1, que mostramos sinteticamente como sigue. Determine los enteros e y e' tales que

e = 0 (mod. a) y = B (mod. b); ce' = A (mod. a) y = hB (mod. b)

y (e,e0) será un valor de la expresión y — (ac, ah, i) (mod. — ab). Pues según el modulo a tenemos

2

e = 0 ξ —ac, ee ξ 0 ξ —ah

*ξ A2* *= —*bc = *—c2i* entonces e/2 ξ —i

2 /2

*ce*

y segUn el modulo b tenemos

e2 ξ B2 ξ —ac, cee0 ξ hB2 ξ -

ach entonces ee0 = entonces e/2 ξ —i

ah

1. 2 2 2 2 2 c2e = h2B2 = *—*ach2 = —c2i

y las mismas tres congruencias que son vólidas según cada uno de los módulos a y b por separado tambien serán vólidos según el modulo ab. Entonces, por el teorema de formas ternarias, es fócil concluir que φ es representable por la forma ^ 0 ^.

Suponga entonces que

act2 + 2ahtu + iu2 = —(at + βη)2 + 2(qt + óu)^t + ζη)

Multiplicando por c obtenemos

a(ct + hu)2 + bu2 = —c(at + βη)2 + 2c(qt + óu)^t + ζη)

Ahora si le damos a t y u valores tales que o qt + úu o εt + Zu sea = 0, habró una solución de la ecuación (Ω) que seró satisfecha por

x = úc — qh, y = γ, z = αδ — βγ

y por

x = Zc — εh, y = ε, z = αζ — βε

Es evidente que no todos los valores en cualquiera de los dos conjuntos puede ser = 0 simultóneamente, pues si úc — qh = 0, γ = 0, tendríamos tambien δ = 0 y φ = — (at + eu)2, resultando ab = 0, contrario a la hipótesis y similarmente para los otros valores. En nuestro ejemplo encontramos que la forma φ es (161, —63, 24), que el valor de la expresion — φ (mod. 105) = (7, —51), y que la representacion de la forma φ por 0 0^ es

φ = —(13t — 4u)2 + 2(11t — 4u)(15t — 5u)

Esto nos da las soluciones x = 7, y = 11, z = -8; x = 20, y = 15, z = -5, o dividiendo por 5 e ignorando el signo de z, x = 4, y = 3, z = 1.

De los dos metodos para resolver la ecuación (Ω), el segundo es preferible porque utiliza numeros pequeños con mas frecuencia; el primero, sin embargo, que puede acortarse mediante varios artificios que omitiremos aquí, parece ser mas elegante, especialmente porque los nómeros a, b y c se tratan de la misma manera y los calculos no se alteran al permutarlos. Por otra parte, es en el segundo metodo donde tenemos los calculos mas convenientes si dejamos que a sea el menor y c el mayor de los tres nómeros, como hicimos en nuestro ejemplo.

Sobre el método con el cual Legendre trato de demostrar su teorema fundamental.

296.

El elegante teorema que hemos explicado en los artículos anteriores fue descubierto por primera vez por el ilustre Legendre, Hist. de l’Ac. de Paris, 1785, p. 507, y lo justifico con una demostración bella (enteramente diferente de las dos nuestras). A la vez este geometra sobresaliente trato de obtener a partir de ello una demostracion de proposiciones que se ajustan al teorema fundamental de la seccion anterior, pero ya hemos dicho en el artículo 151 que parecía no ser apropiado para este proposito. Entonces, este es el lugar para explicar esta demostracion (extremadamente elegante en sí) de manera breve y dar las razones de nuestra opinion. Empezamos con la siguiente observation: si los némeros a, b y c, son todos = 1 (mod. 4), la ecuacién ax2 + by2 + cz2 =0... (Ω) no es resoluble. En efecto, es facil ver que en este caso el valor de ax2 + by + cz2 necesariamente sera o ξ 1, o ξ 2, o ξ 3 (mod. 4), excepto si todos los x, y y z son pares a la vez; por lo tanto, si Ω fuera soluble, esto no podría suceder excepto por valores pares de x, y y z, Q. E. A., puesto que cualesquiera que sean los valores que satisfacen la ecuacion Ω la seguiran satisfaciendo al dividirse por su maximo comun divisor, así que por lo menos uno de los valores debe ser impar. Ahora se obtienen los diferentes casos del teorema por demostrar mediante las consideraciones siguientes.

1. Si p y q son numeros primos (diferentes y positivos) de la forma 4n + 3, no podemos tener pRq y qRp a la vez. En efecto, si fuera posible, claramente al poner que 1 = a, - p = b, - q = c, todas las condiciones para resolver la ecuacion ax2 + by2 + cz2 = 0 se cumplirán (art. 294); pero mediante la observation anterior, esta ecuacion no tiene solution; por lo tanto, nuestra suposicion es inconsistente. De esto sigue inmediatamente la proposition 7 del artículo 131.
2. Si p es un número primo de la forma 4n +1 y q es un número primo de la forma 4n + 3, no se puede tener simultáneamente qRp y pNq. En efecto, tendríamos —pRq y la ecuación x2 + py2 — qz2 = 0 sería resoluble. De esto obtenemos los casos 4 y 5 del artículo 131.
3. Si p y q son numeros primos de la forma 4n + 1, no se puede tener simultaneamente pRq y qNp. Sea r otro número primo de la forma 4n + 3 que sea un residuo de q y del cual p sea un no residuo. Entonces por los casos (II) ya demostrados tendremos qRr y rNp. Por lo tanto, si tenemos pRq y qNp tendríamos qrRp, prRq, pqNr y luego —pqRr. Esto haría que la ecuacion px2 + qy2 — rz2 = 0 fuera resoluble, contrario a la observation anterior; y la suposiciún sería inconsistente. De esto siguen los casos 1 y 2 del artículo 131.

Este caso se puede tratar mías elegantemente de la siguiente manera. Sea r un nímero primo de la forma 4n+3 para el cual p sea un no residuo. Entonces tendremos rNp y por lo tanto (suponiendo pRq, qNp) qrRp; ademas, tenemos —pRq, —pRr, y así tambien —pRqr y la ecuacion x2 + py2 — qrz2 = 0 sería resoluble contrario a la observation anterior, etc.

1. Si p es un nímero primo de la forma 4n + 1 y q un primo de la forma 4n + 3, no se puede tener pRq y qNp simultaneamente. Sea r un nímero primo auxiliar de la forma 4n +1 que es un no residuo de ambos p y q. Entonces tendremos (por II) qNr y (por III) pNr; por lo tanto pqRr; por lo tanto si pRq, qNp tambien tendríamos prNq, —prRq, qrRp; así pues la ecuacion px2 — qy2 + rz2 = 0 sería resoluble, Q. E. A. De esto obtenemos los casos 3 y 6 del artículo 131.
2. Si p y q son nímeros primos de la forma 4n + 3, no podemos tener pNq y qNp simultaneamente. En efecto, si se supone que esto es posible y se toma un nímero primo auxiliar r de la forma 4n +1 que sea un no residuo de ambos p y q, tendremos qrRp, prRq; ademís (por II) pNr, qNr y por lo tanto pqRr y —pqRr; así que la ecuacion —px2 — qy2 + rz2 = 0 es posible, contrario a la observation anterior. De esto obtenemos el caso 8 del artículo 131. [[206]](#footnote-207)

suposiciones son tan aparentes que parecen no requerir una demostración, y aunque ciertamente dan el mas alto grado de probabilidad al teorema que estamos tratando de demostrar, no obstante, si queremos rigor geometrico no podemos simplemente aceptarlas de manera gratuita. En cuanto a la suposición en IV y V de que existe un nómero primo r de la forma 4n +1 que es un no residuo de los otros primos dados p y q, es facil concluir de la Seccion IV que todos los nómeros menores que 4pq y primos relativos con el (su nómero es 2(p — 1)(q — 1)) se pueden distribuir equitativamente en cuatro clases. Una de ellas contendrá los no residuos de p y q y las tres restantes los residuos de p que son no residuos de q, los no residuos de p que son residuos de q y los residuos de ambos p y q; y en cada clase la mitad de los nómeros serán de la forma 4n + 1 y la otra mitad de la forma 4n + 3. Entre ellos por lo tanto habrá 4 (p — 1)(q — 1) que son no residuos de p y q de la forma 4n +1. Los designaremos por g, g', g", etc., y los restantes 4(p — 1)(q — 1) nómeros por h, h', hff, etc. Todos los nómeros contenidos en las formas 4pqt + g, 4pqt + g', 4pqt + g'', etc. ... (G) tambien serán no residuos de p y q de la forma 4n +1. Ahora esta claro que para establecer nuestra suposicion es necesario solamente establecer que las formas (G) contienen números primos. Y esto parece ser muy plausible puesto que estas formas junto con las formas 4pqt + h, 4pqt + h', etc. ... (H) contienen todos los nómeros que son primos relativos a 4pq y son por lo tanto todos nómeros primos absolutos (excepto 2, p y q); y no hay razon por la cual pensar que esta serie de nómeros primos no sea distribuida equitativamente entre las formas de modo que un octavo pertenezca a (G) y el resto a (H). Pero obviamente este razonamiento esta lejos del rigor geometrico. El ilustre Legendre mismo confeso que la demostración de un teorema que asegura que nómeros primos ciertamente esrán contenidos en una forma kt + l (donde k y l son nómeros primos relativos dados y t indefinido) es bastante difícil y sugiere un metodo que puede ser útil. Nos parece que son necesarias muchas investigaciones preliminares antes de poder llegar a una demostracion rigurosa por este camino. En cuanto a la otra suposicion (III, segundo metodo) de que existe un numero primo r de la forma 4n + 3 del cual otro numero primo dado p de la forma 4n +1 sea un no residuo, Legendre no agrega nada. Hemos mostrado anteriormente (art. 129) que ciertamente hay numeros primos para los cuales p es un no residuo, pero nuestro metodo no parece idoneo para mostrar que existen tales numeros primos que sean ademas de la forma 4n+3 (como se requiere aquí pero no en nuestra primera demostracion). Sin embargo, podemos probar facilmente la validez de esta proposition como sigue. Por el artículo 287 existe un genero positivo de formas binarias de determinante —p cuyo carácter es 3,4; Np. Sea (a,b,c) tal forma y a impar (esto es permitido). Entonces a sera de

la forma 4n + 3 y primo en si o al menos divisible por un factor primo r de la forma 4n + 3. Sin embargo, tenemos -pRa y así tambien —pRr y como resultado pNr. Pero debemos notar cuidadosamente que las proposiciones de los artículos 263 y 287 dependen del teorema fundamental, y así tendríamos un círculo vicioso si basaramos alguna parte de esta discucion en ellos. Finalmente, la suposición del primer metodo en III es tanto mas gratuita que no hay razon por la cual añadir mas sobre ella aquí.

Agreguemos una observacion sobre el caso V que verdaderamente no ha quedado suficientemente comprobado por el metodo anterior; sin embargo sera resuelto satisfactoriamente por lo que sigue. Si pNq y qNp fueran verdaderos simultaneamente, tendríamos —pRq y —qRp, y es facil verificar que —1 es un numero característico de la forma (p, 0,q) que podría entonces (segun la teoría de formas ternarias) ser representada por la forma x2 + y2 + z2. Sea

pt2 + qu2 = (at + βη)2 + (α'ί + β0η)2 + (a"t + β00η)2 o

1. 2 2 2 2 2

a + α + α — p, β + β + β — q, αβ + αβ + αβ — 0

y tendremos de las ecuaciones 1 y 2 que todos los numeros α, α0, α", β, β0 y β00 son impares; pero entonces la tercera ecuacion no puede ser consistente. El caso II se puede resolver de una manera similar a esta. [[207]](#footnote-208)

Demostración. Sean bc = Aa2, ac = Bβ2,αb = Cj2. A, B y C serán enteros libres de factores cuadrados y A = BC, B = AC, C = AB; como resultado ABC = (ABC)2 y así ABC = AA = BB = CC es necesariamente un entero. Sea m el máximo común divisor de los námeros A y AA. Entonces A = gm, AA = hm y g será primo relativo a h y (puesto que A está libre de factores cuadrados) a m. Ahora tenemos h2m = gA2A = gBC así que g divide a h2m, lo cual es obviamente imposible a menos que g = ±1. Así A = ±m, A = ±h y por lo tanto son enteros y como consecuencia B y C tambien serán enteros. Q. E. P. Puesto que A = BC no tiene factores cuadrados, B y C deben ser primos relativos; y similarmente, A sera primo relativo a C ya B. Q. E. S. Finalmente si X = P, Y = Q, Z = R satisfacen la ecuacián (Ω), la ecuación (ω) sera satisfecha por x = aP, y = βQ, z = jR; en cambio si (ω) es satisfecha por x = p, y = q, z = r, (Ω) será satisfecha por X = βγρ, Y = ajq, Z = aβr y así si una es resoluble lo será tambien la otra. Q. E. T.

Representaciones de cero por formas ternarias cualesquiera

299.

PROBLEMA. Dada la forma ternaria

f = ax2 + a'x'2 + a''x''2 + 2bx' x" + 2b' xx" + 2b" xx'

determinar si cero es representable por esta forma (sin que todas las incógnitas sean = 0 simultáneamente).

Solución. I. Cuando a = 0 los valores de x' y x'', se pueden tomar arbitrariamente y es claro de la ecuaciáon

22

a x + 2bx x + a x = —2x(b x + b x )

que x tomará un valor racional determinado; cuando obtenemos una fraccion como valor de x, solo debemos multiplicar los valores de x, x' y x'' por el denominador de la fraccion para obtener enteros. Los ánicos valores de x' y x'' que se deben excluir son aquellos que hacen que b'x'' + b''x' = 0 a menos que tambien satisfagan a'x' +2bx'x'' + a''x'' = 0, en cuyo caso x es arbitrario. Así se pueden obtener todas las posibles soluciones. Pero el caso donde b' = b'' = 0 no se contempla aquí pues entonces x no participaría en la determinacion de f; esto es, f es una forma binaria y la posible representacion de cero por f debe decidirse a partir de la teoría de tales formas.

1. Cuando tenemos a = 0, la ecuación f = 0 será equivalente a

(ax + b''x' + b'x")2 - A''x'2 + 2Bx'x'' - A'x''2 = 0

al poner

b''2 - aa' = A', ab - b'b" = B, b'2 - aa" = A.

Ahora, cuando A = 0 y B = 0 es claro que si tomamos ax + b''x' + b'x'' y x'' arbitrariamente, x y x' serán námeros racionales y cuando no son enteros se pueden hacer enteros mediante una multiplicacián apropiada. Para un valor de x'', a saber x'' = 0, el valor de ax + b''x' + b'x'' no es arbitrario pero debe ser tambien = 0; pero el x' se puede tomar con completa libertad y producirá un valor de x racional. Cuando A' y B = 0 simultáneamente, es claro que si A es un cuadrado = k2, la ecuacion f = 0 se reduce a las siguientes dos ecuaciones lineales (donde una u otra debe tener lugar)

ax + b''x' + (b' + k)x'' = 0, ax + b''x' + (b' - k)x'' = 0

pero si (bajo la misma hipátesis) A no es un cuadrado, la solucion de la ecuacián propuesta depende de las siguientes (ambas deben cumplirse) x'' = 0 y ax + b'x' = 0.

Sera apenas necesario notar que el metodo de I es aplicable cuando a' o a'' = 0 y el metodo de II cuando A = 0.

1. Cuando ni a ni A'' = 0, la ecuacián f = 0 sera equivalente a

A'(ax + b''x' + b'x'')2 - (A''x' - Bx'')2 + Dax''2 = 0

donde D es el determinante de la forma f y Da es el número B2 - A'A''. Cuando D = 0 tendremos una solucián como la del final del caso anterior; eso es, si A'' es un cuadrado = k2, la ecuacion propuesta se reduce a estas:

kax + (kb'' - A')x' + (kb' + B)x'' = 0, kax + (kb'' + A'')x' + (kb'' - B)x'' = 0

pero si A no es un cuadrado, se debe tener

ax + b''x' + b'x'' = 0, A''x' - Bx'' = 0

Sin embargo, cuando D no es = 0 se nos reduce a la ecuacioán

A''t2 - u2 + Dav2 = 0

una posibilidad que se puede decidir mediante el artículo anterior. Si esta ecuación no se puede resolver excepto para t = 0, u = 0 y v = 0, la ecuación propuesta no admite ninguna solución salvo x = 0, x' = 0 y x" = 0; pero si tiene como solución cualquier otro conjunto de enteros t, u y v podemos mediante las ecuaciones

ax + b"x' + b'x'' = t, A''x' — Bx'' = u, x'' = v

obtener por lo menos valores racionales de x, x' y x''. Si estas incluyen fracciones, podemos hacerlas enteros mediante una multiplicacion apropiada.

Tan pronto se encuentra una solución de la ecuacion f = 0 por enteros, el problema se reduce al caso I y todas las soluciones se pueden encontrar de la siguiente manera. Sean α, a' y a'' algunos valores de x, x' y x'' que satisfacen la ecuacion f = 0. Supongamos que no tienen factores comunes. Ahora (por art. 40, 279) escoja enteros β, β', β'', γ, γ' y γ'' tales que

α(β'γ'' — β''γ') + α' (β''γ — βγ'') + α''(βγ' — β'γ) = 1 y la forma f se transformaró, por la sustitución

x = ay + βν + γ^'', x' = a'y + βΥ + γΥ', x'' = a" y + β'Υ + γ'Υ' (S)

en la forma

g = cy+ cy + cy + 2dy y + 2d yy + 2d yy

Entonces se tendrá c = 0 y g seró equivalente a f, de donde se concluye facilmente que todas las soluciones por enteros de la ecuación f = 0 pueden obtenerse (por S) de todas las soluciones de g = 0. Y por I todas las soluciones de la ecuacion g = 0 estan contenidas en las fórmulas

y = —z(c'p2 + 2dpq + c''q2), y' = 2z(d''p2 + d'pq), y'' = 2z(d''pq + d'q2)

donde p y q son enteros cualesquiera , z un número cualquiera que puede ser una fraccion siempre y cuando y, y' e y'' sean enteros. Si sustituimos estos valores de y, y' e y'' en (S), se tendrán todas las soluciones de la ecuacion f = 0 por enteros. Así, por ejemplo, si

f = x2 + x'2 + x''2 — 4x'x'' + 2xx'' + 8xx'

y una solución de la ecuación f = 0 es x = 1, x' = — 2, x" = 1; haciendo β, β', β'', γ, γ', γ'' = 0, 1, 0, 0, 0, 1 tenemos

/2 a 2 ^///,10 H

g = y + y - 4yy + 12yy

Todas las soluciones de la ecuación g = 0 por enteros estarán contenidas en la fórmula

y = —z(p2 — 4pq + q2), y' = 12zpq, y'' = 12zq2

y todas las soluciones de la ecuacion f = 0 en las fórmulas

x = —z(p2 — 4pq + q2) x' = 2z(p2 + 2pq + q2) x'' = —z(p2 — 4pq — 11q2)

Solución general por racionales de ecuaciones de segundo grado en dos variables.

300.

A partir del problema del artículo anterior se obtiene inmediatamente la solucióon de la ecuacióon indeterminada

ax2 + 2bxy + cy2 + 2dx + 2ey + f = 0

si se buscan sólo valores racionales. Ya la hemos resuelto para valores enteros (art. 216 y siguientes). Todo valor racional de x e y puede representarse por V y u, donde t, u y v son enteros. Así pues, es claro que la solucion de esta ecuacion por nómeros racionales es identica a la solucion por enteros de la ecuacion

at2 + 2btu + cu2 + 2dtv + 2euv + fv2 = 0

y esto coincide con la ecuacion tratada en el artículo anterior. Excluimos solo aquellas soluciones donde v = 0; pero no puede ocurrir ninguna de este tipo cuando b2 — ac es un nómero no cuadrado. Así pues, e.g., toda solución por nómeros racionales de la ecuación (resuelta de modo general por enteros en el art. 221)

x2 + 8xy + y2 + 2x — 4y +1=0

estará contenida en la fórmula

p2 — 4pq + q2 2p2 + 4pq + 2q2

p2 — 4pq — 11q2 ’ ^ p2 — 4pq — 11q2

donde p y q son enteros cualesquiera. Pero aquí hemos tratado brevemente estos dos problemas que están íntimamente conectados dejando por fuera muchas observaciones pertinentes para no hacernos demasiado prolijos. Tenemos otra solucián del problema del artículo anterior basada en principios generales, sin embargo se tratará en otra ocasioán puesto que requiere de un estudio maás profundo de las formas ternarias.

Del número promedio de géneros.

301.

Regresemos ahora al estudio de las formas binarias de las cuales tenemos aán muchas propiedades notables que examinar. Primero le agregaremos algunas observaciones sobre el nuámero de clases y gáeneros en un orden propiamente primitivo (positivo si el determinante es negativo) y para brevedad restringiremos nuestra investigation a estas.

El número de generos en los cuales se distribuyen todas las formas (propia­mente primitivas positivas) de determinante ±D positivo o negativo es siempre 1, 2, 4 o una potencia mayor de 2 cuyo exponente depende de los factores de D y que se puede encontrar a priori mediante el argumento presentado anteriormente. Ahora, puesto que en una serie de námeros naturales los námeros primos están mezclados con nuámeros máas o menos compuestos, sucede que para muchos determinantes suce­sivos ±D, ±(D + 1), ±(D + 2), etc. el námero de generos crece y decrece de manera desordenada. Sin embargo, si sumamos los námeros de generos correspondientes a muchos determinantes sucesivos

±D, ±(D + 1), ... ± (D + m)

y dividimos la suma por el námero de determinantes, obtenemos el número promedio de géneros. Se puede considerarlo como si correspondiera al determinante central ±(D + 2m) de la serie y establece una progresián muy regular. Supongamos no sálo que m es suficientemente grande sino tambien que D sea mucho mayor, de modo que la razán de los determinantes extremos D, D + m no difiera mucho de la igualdad. La regularidad de esta progresián debe entenderse asá: si D0 es un numero mucho mayor

que D, el número promedio de determinantes alrededor de D0 será notablemente mayor que alrededor de D; y si D y D0 no difieren por mucho, el número promedio de generos alrededor de D y D0 sera aproximadamente igual. Pero el número promedio de generos alrededor del determinante positivo +D siempre sera aproximadamente igual al número de generos alrededor del correspondiente determinante negativo y entre mayor sea el valor de D, mas cierto sera lo anterior mientras que para valores pequeños el número de generos correspondiente al determinante positivo sera un poco mayor que el del determinante negativo. Estas observaciones quedaran ilustradas mejor por los siguientes ejemplos tomados de la tabla que clasifica a las formas binarias para mas de 4000 determinantes. Entre los cien determinantes de 801 a 900 hay 7 que corresponden a un único genero, 32, 52, 8, 1, que corresponden respectivamente a 2, 4, 8, 16 generos. Hay en total 359 generos y un número promedio de 3,59. Los cien determinantes negativos de -801 a -900 producen 360 generos. Los siguientes ejemplos se toman con determinantes negativos. En la centena 16 (desde -1501 a -1600) el número promedio de generos es 3,89; en la centena 25 es 4,03; en la centena 51 es 4,24; para los 600 determinantes desde -9401 a -10000 es 4,59. De estos ejemplos es claro que el número promedio de generos crece mucho mas lentamente que los determinantes mismos, pero se busca la ley que describe esta progresión. Mediante una discusión teórica bastante difícil, cuya explicación sería demasiado larga para presentar aquí, se encontró que el número promedio de generos alrededor de +D o -D puede calcularse aproximadamente por la fórmula

a log D + β

donde α y β son cantidades constantes y de hecho

4

a = -= = 0,4052847346 π2

(π es la mitad de la circunferencia de un cúrculo de radio unitario),

1. 1

β = 2ag + 3a2h a log 2 = 0,8830460462

6

donde g es el valor de la serie

1. - log(1 + 1) + - - log(1 + -) + - - log(1 + -) + etc. = 0,5772156649
2. 2 3 3

(ver Euler, Inst. Calc. Diff. p. 444) y h es el valor de la serie

1 log 2 + 1 log 3 + :1 log 4 + etc.

1. 9 16

que es aproximadamente = 0,9375482543. A partir de esta formula es claro que el número promedio de generos aumenta en una progresión aritmetica si los determinantes aumentan en una progresión geometrica. Los valores que nos proporciona esta formula para D = 8502, 15502, 24501, 50502, 97001 resultan ser 3,617; 3,86; 4,046; 4,339; 4,604; los cuales difieren poco de los valores presentados anteriormente. Entre mayor sea el determinante central y el nuómero de determinantes a partir de los cuales se calcula el promedio, menor seróa la diferencia entre el valor real y el que se obtiene con la formula. Con la ayuda de esta fórmula, tambien se puede encontrar la suma aproximada del nuómero de góeneros que corresponden a determinantes sucesivos ±D, ±(D + 1), ... ±(D + m) sumando el número promedio correspondiente a cada uno sin importar que tan separados esten D y D + m. Esta suma seróa

= a (logD + log(D + 1)+ etc. + log(D + m)) + e(m + 1) o con bastante exactitud

= a ((D + m)log(D + m) — (D — 1) log(D — 1)) + (β — a)(m + 1)

De esta manera la suma del número de generos para los determinantes —1a —100 resulta ser 234,4, mientras que su valor real es 233; similarmente desde —1a —2000 la fórmula nos da 7116,6 mientras que el valor real es 7112; de —9001 a —10000 el valor real es 4595 y el aproximado por la formula 4594,9, una aproximación mejor de lo que se podría esperar.

Del número promedio de clases.

302.

En cuanto al número de clases (siempre asumimos que son propiamente primi­tivas positivas) los determinantes positivos se comportan de una manera completa­mente diferente a los determinantes negativos; por lo tanto los consideraremos sep­aradamente. Concuerdan en el hecho de que para un determinante dado hay igual

número de clases en cada género, y por lo tanto el número de clases es igual al producto del número de generos por el número de clases en cada uno.

Primero, con respecto a los determinantes negativos, el número de clases que corresponde a varios determinantes sucesivos —D, — (D + 1), — (D + 2), etc. genera una progresión que es tan irregular como el número de generos. El numero promedio de clases, sin embargo, (no hace falta una definicion) aumenta de manera muy regular como se notará en los siguientes ejemplos. Los cien determinantes de —500 a —600 proporcionan 1729 clases y así el número promedio es 17,29. Similarmente en la centena #15 el número promedio de clases es 28,26; para la #24 y #25 se calcula 36,28; para la #61, #62 y #63 resulta 58,50; para las cinco centenas de #91 a #95 se encuentra 71,56; finalmente para las cinco de 96 a 100 se tiene 73,54. Estos ejemplos muestran que el número promedio de clases crece mas lentamente que los determinantes pero mucho mús rápidamente que el numero promedio de generos; con una leve atenciún se puede ver que crece casi exactamente en proporciún a la raíz cuadrada del determinante central. De hecho hemos encontrado mediante una investigaciúon teúorica que el nuúmero promedio de clases cerca del determinante — D se puede expresar aproximadamente como

γ YD — δ

donde

2π

*Ye*

+ etc. 2

π2

γ = 0,7467183115

donde e es la suma de la serie

1111 1 + 8 + 27 + 64+125

δ = 0,2026423673 =

Los valores promedios obtenidos mediante la formula difieren poco de los valores tomados de la tabla de clasificaciones mencionada arriba. Con la ayuda de esta fúrmula tambien se puede aproximar el número de clases (propiamente primitivas positivas) que corresponden a los determinantes sucesivos — D, — (D + 1), — (D + 2), ... — (D + m — 1), sin importar la separaciún de los extremos, sumando los números promedios correspondientes a estos determinantes, obtenidos según la fúrmula. Se encuentra una suma

= γ (YD + λ/D + 1 + etc. + YDYm —1) — δm

3

-[[208]](#footnote-209) [[209]](#footnote-210)) 2 2;

o aproximadamente

2

3

Y

(D + m

(D

3

^2 2;

*óm*

Así pues, e.g., por medio de la fórmula la suma de los cien determinantes —la -100 será 481,1, mientras que el valor real es 477; los mil determinantes entre —1 y —1000 segun la tabla proporcionan 15533 clases, mientras que el valor que nos da la formula es 15551,4; en el segundo milenio segán la tabla hay 28595 clases, y segán la formula 28585,7. Similarmente el tercer milenio realmente tiene 37092 clases; la fórmula da 37074,3; el decimo milenio posee 72549 segán la tabla y 72572 segán la formula.

303.

La tabla de determinantes negativos ordenados segán varias clasificaciones ofrece muchas otras observaciones notables. Para determinantes de la forma — (8n+3) el numero de clases (tanto el námero total como el námero de clases contenido en cada genero propiamente primitivo) es siempre divisible por tres, con la ánica excepción del determinante —3, como se puede concluir del artículo 256, VI. Para aquellos determinantes cuyas formas estaán contenidas en un solo gáenero, el nuámero de clases es siempre impar, puesto que para estos determinantes hay una ánica clase ambigua, la principal, las restantes clases siempre estan opuestas en parejas y el námero de ellas es por lo tanto par, lo cual hace impar el námero total de clases. Esta áltima propiedad es tambien válida para determinantes positivos. Además, la serie de determinantes que corresponden a una clasificacion dada (i.e. un námero dado de generos y de clases) parece siempre finita e ilustramos esta observacioán notable con los siguientes ejemplos. (El numeral romano indica el námero de generos propiamente primitivos positivos, el numeral aráabigo el nuámero de clases en cada gáenero, luego sigue la serie de determinantes que corresponde a esta clasificacion. Por razones de brevedad omitimos el signo negativo.)

II. 2 ... 14,17, 20,32, 34, 36,39,46,49, 52, 55,63, 64, 73,82, 97,100,142,148,193

1. 1... 21,24,30,33,40,42,45,48, 57, 60, 70, 72, 78,85, 88, 93,102,112,130,133,

177, 190, 232, 253

1. 1... 105,120,165,168, 210, 240, 273, 280, 312, 330, 345, 357, 385,408,462,

520, 760

XVI. 1... 840,1320,1365,1848

Similarmente, se encuentran 20 determinantes (el mayor = -1423) que corresponden a la clasificación I. 9; 4 (el mayor = -1303) que corresponden a la clasificación I. 11 etc; a las clasificaciones II. 3, II. 4, II. 5, IV. 2, corresponden no mós de 48, 31, 44 y 69 determinantes respectivamente, donde los mayores son -652, -862, -1318 y -1012. Puesto que la tabla de la cual obtuvimos estos valores se ha extendido mucho mas alla que el mayor determinante que aparece aquí[[210]](#footnote-211)) y puesto que no proporciona ningún otro que pertenezca a estas clases, no hay duda de que las series anteriores terminan, y por analogóa es permitido extender la conclusioón a cualquier otra clasificacióon. Por ejemplo, puesto que en todo el decimo milenio de determinantes, no hay ninguno que corresponde a menos de 24 clases, es muy probable que las clasificaciones I. 23, I. 21, etc. II. 11, II. 10, etc. IV. 5, IV. 4, IV. 3; VIII. 2 estan todas completas antes de llegar al nuómero - 9000 o que por lo menos tienen muy pocos determinantes mayores que -10000. Sin embargo, probar rigurosamente estas observaciones parece ser muy difícil. Es tambien notable que todo determinante cuyas formas se distribuyen entre 32 o mas generos tiene por lo menos dos clases en cada genero y, por lo tanto, que las clasificaciones XXXII. 1, LXIV. 1 etc. no existen del todo (el determinante menor entre estos es -9240 y corresponde a la clasificación XXXII. 2); y parece ser muy probable que cuando crece el numero de generos mas clasificaciones desaparecen. En este aspecto los 65 determinantes mencionados anteriormente, aquellos de las clasificaciones I. 1, II. 1, IV. 1, VIII. 1, XVI. 1, son bastante excepcionales, y es facil ver que solo ellos gozan de dos propiedades notables: todas las clases de las formas que pertenecen a ellos son ambiguas y todas las formas contenidas en el mismo genero son a la vez propia e impropiamente equivalentes. El ilustre Euler en Nouv. Mém. de l’Ac. de Berlin, 1776, p. 338 ya ha determinado estos 65 numeros (bajo un aspecto ligeramente diferente que mencionaremos luego, y con un criterio que es facil de demostrar).

304.

El número de clases propiamente primitivas que corresponden a formas bina­rias con un determinante cuadrado positivo k2 puede determinarse completamente a priori; hay tantas clases como números primos relativos a 2k y menores que el. De este hecho y siguiendo un razonamiento facil, que omitimos aquí, deducimos que el número promedio de clases alrededor de k2 que pertenecen a tales determinantes es aproximadamente . Al respecto, sin embargo, determinantes positivos no cuadra­dos presentan fenómenos singulares. A saber, hay solo un numero pequeno de clases para determinantes pequeños negativos o cuadrados, e.g., clasificacion I. 1 o I. 3 o II. 1 etc., y la serie termina rápidamente; al contrario, para determinantes positivos no cuadrados, siempre y cuando no sean muy grandes, la gran mayoría de ellos pro­ducen clasificaciones en las cuales solo una clase esta contenida en cada genero. Así pues, clasificaciones como I. 3, I. 5, II. 2, II. 3, IV. 2, etc. son muy raras. Por ejemplo, entre los 90 determinantes inferiores a 100 encontramos 11, 48 y 27, que correspon­den a las clasificaciones I. 1, II. 1, IV. 1 respectivamente; solo uno (37) tiene I. 3; dos (34 y 82) tienen II. 2; uno (79) tiene II. 3. Sin embargo, al aumentar los de­terminantes, aparecen numeros mayores de clases y lo hacen con mayor frecuencia; así pues, entre los 96 determinantes no cuadrados entre 101 y 200, dos (101, 197) tienen la clasificacion I. 3; cuatro (145, 146, 178, 194) tienen II. 2; tres (141, 148, 189) tienen II. 3. Entre los 197 determinantes de 801 a 1000, tres tienen I. 3; cuatro II. 2; catorce tienen II. 3; dos tienen II. 5; dos tienen II. 6; quince tienen IV. 2; seis tienen

1. 3; dos tienen IV. 4; cuatro tienen VIII. 2. Los 145 restantes tienen una clase en cada genero. Es curioso y sería digno de un geometra, investigar la ley que justifique el hecho de que los determinantes con una clase por cada genero se hacen menos frecuentes. Hasta el momento no podemos asegurar teoricamente ni conjeturar por observacion si hay un numero finito de ellos (esto es poco probable) o si se hacen infinitamente raros o que su frecuencia tiende a un límite fijo. El numero promedio de clases aumenta por una razon ligeramente mayor que la razon con que varía el número de generos y mas lentamente que las raíces cuadradas de los determinantes. Entre 800 y 1000 se encuentra 5, 01. Se puede agregar a estas observaciones otra que apoya la analogía entre los determinantes negativos y positivos. Hemos encontrado que para un determinante positivo D, no es el numero de clases sino este numero multiplicado por el logaritmo de t + u\J~D (t y u son los numeros menores, diferentes de 1 y 0, que satisfacen la ecuacion t2 — Du2 = 1) el que es analogo al numero de clases para un determinante negativo. No podemos explicar esto mas a fondo, pero el valor promedio de ese producto es dado aproximadamente por una formula

como m\/ü — n. Pero aun no hemos podido determinar teóricamente los valores de las constantes m y n. Si se permite llegar a una conclusion valida con base en la comparación de unas cuantas centenas, parece que m es aproximadamente 2^. Reser­vamos para otra ocasion una discusion mós completa de los principios detras de la discusioón anterior sobre los valores promedios de cantidades que no siguen una ley analítica, sino que se aproximan asintoticamente a una ley analítica. Pasamos ahora a otra investigacion, la comparacion de diferentes clases propiamente primitivas de un mismo determinante y asó terminaraó esta larga seccioón.

Algoritmo singular para clases propiamente primitivas; determinantes regulares, etc.

305.

TEOREMA. Si K es la clase principal de formas de un determinante dado D, y C es otra clase cualquiera del género principal del mismo determinante; y si 2C, 3C, 4C, etc. son las clases que resultan (como en art. 249) de la duplicación, triplicación, cuadruplicación, etc. de la clase C; entonces si continuamos la progresion C, 2C, 3C, etc. lo suficiente, finalmente obtendremos una clase que es idóntica a K; y suponiendo que mC es la primera que es idóntica a K y que el numero de clases en el gónero principal = n, entonces tendremos que m = n o que m seró un factor de n.

Demostracion. I. Puesto que todas las clases K, C, 2C, 3C, etc., necesariamente pertenecen al genero principal (art. 247), las primeras n +1 clases de la serie K, C, 2C, 3C, ...nC no pueden ser todas diferentes. Entonces, K seró identica a alguna de las clases C, 2C, 3C, ...nC o al menos dos de ellas serán identicas entre sí. Sea rC = sC y r > s; se tendró tambien

(r — 1)C = (s — 1)C, (r — 2)C = (s — 2)C etc. y (r + 1 — s)C = C

por lo tanto (r — s)C = K. Q. E. P.

II. Tambien sigue directamente de esto que m = n o que m < n, y solo queda demostrar que en el segundo caso m es un factor de n. Puesto que las clases

K, C, 2C, ... (m — 1)C

las cuales designaremos como C, no agotan el genero principal, sea C0 una clase de este genero que no estó contenida en C. Ahora sea C0 el conjunto de clases que resulta de la composicion de C0 con las clases individuales de C, a saber

C0, C0 + C, C0 + 2C, C0 + (m — 1)C

Ahora, obviamente todas las clases en C' serán diferentes entre sí, serán diferentes de todas las clases en C y pertenecerán al genero principal; si C y C' agotan completamente este genero, entonces tendremos n = 2m; si no, 2m < n. En el segundo caso sea C'' cualquier clase del genero principal que no esta comprendida ni en C ni en C' y designaremos por C ' el conjunto de clases que resulta de la composición de la clase C" con las clases individuales de C; i.e.

1. C + C, C + 2C, ...C" + (m - 1)C

y es claro que todas estas son diferentes entre sí y diferentes de todas las clases en CyC0, y pertenecen al genero principal. Ahora, si C, C' y C ' agotan este genero, tendremos que n = 3m; si no, n > 3m. En este caso hay otra clase C'" del genero principal que no está comprendida en C, C', C". De manera similar encontramos que n = 4m o n > 4m y así sucesivamente. Ahora puesto que n y m son finitos, el genero principal debe agotarse eventualmente y n sera un multiplo de m, o m un factor de n. Q. E. S.

Ejemplo. Sea D = -356, C = (5, 2, 72)[[211]](#footnote-212)). Se encuentra 2C = (20, 8, 21), 3C = (4, 0, 89), 4C = (20, -8, 21), 5C = (5,-2, 72), 6C = (1,0, 356). Aquí m = 6 y para este determinante n = 12. Si tomamos (8, 2, 45) como la clase C' las restantes cinco clases de C' serán (9, -2,40), (9, 2,40), (8,-2,45), (17,1, 21) y (17,-1, 21).

306.

La demostracion del teorema anterior es análoga a las demostraciones en los artículos 45 y 49, y de hecho la teoría de multiplicacián de clases es muy afín con el argumento dado en la seccion III. Pero las limitaciones de este trabajo no permiten proseguir el tratamiento mas profundo que merece esta teoría y solo agregaremos algunas observaciones, dejando para otra ocasioín aquellas demostraciones que requieren mucho detalle.

I. Si la serie K, C, 2C, 3C, ...etc. se extiende mís allí de (m - 1)C, obtendremos las mismas clases de nuevo.

mC = K, (m + 1)C = C, (m + 2)C = 2C etc.

y en general (tomando K como 0C), las clases gC y g'C serán idénticas o diferentes según g y g0 sean congruentes o no respecto al módulo m. Por lo tanto la clase nC siempre será identica a la clase principal K.

1. El conjunto de clases K, C, 2C, ... (m — 1)C que designamos

anteriormente como C se llamara el período de la clase C. Esto no debe confundirse con los períodos de formas reducidas de un determinante no cuadrado positivo como se tratá en el artículo 186 y siguientes. Es claro por lo tanto que la composicián de cualquier numero de clases contenidas en el mismo período dará una nueva clase que tambien estará comprendida en el mismo período

gC + g'C + g"C etc. = (g + g0 + g00 + etc.)C

1. Puesto que C +(m — 1)C = K, las clases C y (m — 1)C serán opuestas, así tambien 2C y (m — 2)C, 3C y (m — 3)C etc. Por lo tanto, si m es par, la clase 2mC será opuesta a sí misma y asá, ambigua; reciprocamente si en C aparece alguna clase además de K que sea ambigua, por ejemplo gC, tendremos gC = (m — g)C y así g = m — g = ^m. Se sigue que si m es par no puede haber una clase ambigua en C excepto K y ^mC; si m es impar, ninguna excepto K.
2. Si suponemos que el período de cualquier clase hC contenida en C es

K, hC, 2hC, 3hC, ... (m0 — 1)hC

es claro que m0h es el menor multiplo de h divisible por m. Entonces, si h y m son primos relativos, se tendrá m0 = m y ambos períodos contendrán las mismas clases pero en orden diferente. En general, si μ es el máximo común divisor de m y h, será m0 = m. Así es claro que el námero de clases comprendidas en el período de cualquier clase de C sera m o un factor de m; de hecho habrá tantas clases en C de período m como námeros en la serie 0, 1, 2, ...m — 1 que son primos relativos a m, o sea <^>m, utilizando la simbología del artículo 39, y en general, habrá tantas clases en C con período m como námeros de la serie 0, 1, 2, ...m — 1 que tienen a μ como el maximo comán divisor de ellos y m. Es fácil ver que el námero de ellas será φm. Si por lo tanto m = n o sea el genero principal completo esta contenido en C, habrá φη clases en este genero cuyos períodos incluyen todo el genero y φ« clases cuyos períodos son de e terminos, donde e es cualquier divisor de n. Esta conclusion es verdadera cuando existe una clase del genero principal cuyo período es de n terminos.

1. Bajo la misma suposición, la mejor manera de hacer un arreglo de un sistema de clases del genero principal es tomar como base una clase de período n, colocando las clases del genero principal en el mismo orden con el que aparecen en este período. Ahora, si le asignamos el índice 0 a la clase principal, 1 a la que tomamos como base y así sucesivamente, entonces con sólo sumar los índices, se puede determinar cual clase resultaró de la composición de cualquiera de las clases del genero principal. Aquí sigue un ejemplo para el determinante -356, donde tomamos la clase (9, 2, 40) como la base:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | (1, | 0, | 356) | 4 | (20, | 8, 21) | 8 | (20, | -8, 21) |
| 1 | (9, | 2, | 40) | 5 | (17, | 1, 21) | 9 | ( 8, | 2, 45) |
| 2 | (5, | 2, | 72) | 6 | ( 4, | 0, 89) | 10 | ( 5, | -2, 72) |
| 3 | (8, | -2, | 45) | 7 | (17, | -1, 21) | 11 | ( 9, | -2, 40) |

1. Aunque tanto una analogía con la sección III como una inducción con mas de 200 determinantes negativos y aún mas determinantes positivos no cuadrados parecen justificar que la suposicion es valida para todo determinante, tal conclusion sería falsa y se refutaría por una extension de la tabla de clasificaciones. Para brevedad llamaremos regulares a aquellos determinantes para los cuales el genero principal completo puede incluirse en un período, e irregulares a aquellos para los que esto no es posible. Podemos ilustrar con sólo unas pocas observaciones este asunto, el cual depende de los misterios mas profundos de la aritmetica superior e involucra una investigacion difícil. Empezaremos con la siguiente relacion general.
2. Si C y C' son clases del genero principal con períodos de m y m' clases, y si M es el menor nómero divisible por m y m', entonces habró clases en el mismo genero cuyos períodos serón de M terminos. Resuelva M en dos factores r y r' primos entre só, donde uno (r) divide a m, y el otro (r') divide a m' (ver art. 73), y la clase mC + mC' = C'' tendra la propiedad deseada. Pues, supongamos que el período de la clase C'' consiste de g terminos, resultara

K = grC'' = gmC + ^C = K + ^C

r' r'

*grm*0

C0

de donde debe ser divisible por m' o gr por r' y asó g por r'. De modo semejante se encuentra que g sera divisible por r y por lo tanto por rr' = M. Pero, puesto que MC'' = K, M seró divisible por g, y necesariamente M = g. Se sigue que el mayor nómero de clases (para un determinante dado) contenido en algón período esdivisible por el número de clases en cualquier otro período (de una clase del mismo género principal). Aquí tambien puede determinarse un metodo para encontrar la clase que tiene el mayor período (para un determinante regular este período incluye todo el genero principal). Este metodo es completamente anúlogo al de los artículos 73 y 74, pero en la prúctica puede acortarse el trabajo mediante algunos artificios. El cociente del numero n por el número de clases en el período mayor serú 1 para determinantes regulares y un entero mayor que 1 para determinantes irregulares, y este cociente es apropiado para expresar los diferentes tipos de irregularidades. Por esta razón se llamarú el exponente de irregularidad.

1. Hasta el momento no hay una regla general mediante la cual puedan distinguirse a priori determinantes regulares de irregulares, en especial porque entre el segundo grupo hay tanto números primos como compuestos; serú suficiente entonces agregar algunas observaciones particulares. Cuando se encuentran mas de dos clases ambiguas en el genero principal, el determinante es irregular y el exponente de irregularidad es par; pero cuando el genero tiene sólo uno o dos, el determinante sera regular o al menos el exponente de irregularidad sera impar. Todos los determinantes negativos de la forma — (216k + 27), excepto -27, son irregulares y el exponente de irregularidad es divisible por 3; lo mismo es valido para los determinantes negativos de la forma — (1000k + 75) y — (1000k + 675), con la exception de —75, y para una infinidad de otros. Si el exponente de irregularidad es un número primo p, o por lo menos divisible por p, n sera divisible por p2, de donde sigue que si n no admite divisor cuadrado, el determinante es de seguro regular. Es solo para determinantes positivos cuadrados e2 que puede determinarse a priori si son regulares o irregulares; son regulares si e es 1 ú 2 o un numero primo impar o una potencia de un numero primo impar; en todos los otros casos son irregulares. Para determinantes negativos, conforme aumentan los determinantes, los irregulares se hacen mas frecuentes; e.g., entre los primeros mil encontramos 13 irregulares (omitiendo el signo negativo) 576, 580, 820, 884, 900 cuyo exponente de irregularidad es 2, y 243, 307, 339, 459, 675, 755, 891, 974 cuyo exponente de irregularidad es 3; en el segundo millar hay 13 con exponente de irregularidad 2 y 15 con exponente de irregularidad 3; en el decimo millar hay 31 con exponente de irregularidad 2 y 32 con exponente de irregularidad 3. Todavía no podemos decidir si determinantes con exponente de irregularidad mayor que 3 aparecen debajo de —10000; mas alla de este límite puede encontrarse determinantes de cualquier exponente dado. Es muy probable que conforme aumenta el tamaño del determinante, la frecuencia de determinantes negativos irregulares tiende a una razon constante respecto a la frecuencia de los

regulares. La determinación de esta razón sería realmente digna de las habilidades de un geometra. Para determinantes positivos no cuadrados, los irregulares son mucho mas escasos; ciertamente hay un nómero infinito cuyos exponentes de irregularidad son pares (e.g., 3026 para el cual es 2); y parece haber sin duda algunos cuyos exponentes de irregularidad es impar, aunque debemos confesar que no hemos encontrado ninguno hasta el momento.

1. Por brevedad, no se puede tratar aquí la disposición mas cómoda del sistema de clases contenida en un góenero principal con determinante irregular; soólo observamos que, puesto que una base no es suficiente, hay que tomar dos o mós clases, y a partir de su multiplicacion y composición producir todas las demas. Así nacen 'índices dobles o múltiples que tendrán la misma funcion que los óndices simples en el caso de determinantes regulares. Pero trataremos este tema en otra ocasión con mas detalle.
2. Finalmente hacemos notar que, puesto que todas las propiedades conside­radas en este articulo y el anterior dependen especialmente del numero n, el cual juega un papel similar al de p — 1 en la Seccion III, este numero merece atencion cuidadosa. Es muy deseable por lo tanto determinar la relacion general entre este numero y el determinante al cual pertenece. No debemos desesperarnos para encontrar la respuesta, puesto que ya hemos logrado establecer (art. 302) la formula del valor promedio del producto de n por el número de generos (que puede determinarse a priori), por lo menos para determinantes negativos.

307.

Las investigaciones de los artículos anteriores solo toman en cuenta las clases del genero principal y así, son suficientes para determinantes positivos cuando hay solo un genero y para determinantes negativos cuando hay solo un genero positivo si no queremos considerar el genero negativo. Solo queda agregar unos cuantos comentarios respecto a los generos restantes (propiamente primitivos).

I. Cuando G0 es un genero diferente del genero principal G (del mismo determinante) con alguna clase ambigua, habrá tantas en este como en G. Sean L, M, N, etc. las clases ambiguas en G (entre las cuales estará la clase principal K) y L0, M0, N0, etc., las de G0 y designe el primer conjunto por A y el segundo por A0. Puesto que es claro que todas las clases L + L0, M + L0, N + L0, etc., son ambiguas y diferentes entre sí y pertenecen a G0, y así tambien deben estar contenidas en A0,

el número de clases en A0 no puede ser menor que el número en A, y similarmente, puesto que las clases L0 + L0, M' + L0, N0 + L0 etc., son diferentes entre si y ambiguas y pertenecen a G, y por lo tanto estan contenidas en A, el número de clases en A no puede ser menor que el número en A0; por esto el número de clases en A y A0 son necesariamente iguales.

1. Puesto que el número de todas las clases ambiguas es igual al número de generos (art. 261, 287.III), es claro que si hay solo una clase ambigua en G, debe haber una clase ambigua en cada genero; si hay dos clases ambiguas en G, habrá dos en la mitad de todos los generos y ninguna en los restantes; finalmente si hay varias clases en G, digamos a de ellas[[212]](#footnote-213)), la α-esima parte de todos los generos contendrá clases ambiguas, el resto no contendrá ninguna.
2. En el caso donde G contiene dos clases ambiguas, sean G, G0, G00, etc., los generos que contienen dos, y H, H0, H00, etc., los generos que no contienen ninguna, y designe el primer conjunto por G y el segundo por H. Puesto que siempre obtenemos una clase ambigua a partir de la composición de dos clases ambiguas (art. 249), no es difícil ver que la composicion de dos generos de G siempre da un genero de G. Ademas, la composicion de un genero de G con un genero de H da un genero de H; pues, si por ejemplo G0 + H no pertenece a H sino a G, G0 + H + G0 debe estar en G Q. E. A. , puesto que G0 + G0 = G y así G0 + H + G0 = H. Finalmente los generos G + H, G0 + H, G00 + H, etc. y H + H, H0 + H, H00 + H, etc. son todos diferentes y asú, tomados juntos, deben ser identicos con G y H; pero por lo que acabamos de mostrar los generos G + H, G0 + H, G00 + H, etc. pertenecen todos a H y agotan este conjunto; por lo tanto, necesariamente los restantes H + H, H0 + H, H00 + H, etc. todos pertenecerán a G: i.e., la composiciún de dos generos de H siempre da un gúenero de G.
3. Si E es una clase del genero V, diferente del genero principal G, es claro que 2E, 4E, 6E, etc. todos pertenecen a G y 3E, 5E, 7E, etc. a V. Si, por lo tanto, el período de la clase 2E contiene m terminos, es claro que en la serie E, 2E, 3E, etc. la clase 2mE, y ninguna antes que ella, sera identica a K; eso es, el período de la clase E contendrá 2m terminos. Asú pues, el número de terminos en el período de cualquier clase de un genero que no sea el principal sera 2n o un factor de 2n, donde n representa el numero de clases en todos los generos.
4. Sea C una clase dada del género principal G y E una clase del género V que da C cuando se duplica (siempre hay una, art. 286), y sean K, K0, K00, etc. clases ambiguas (propiamente primitivas del mismo determinante). Luego E(= E + K), E + K', E + K", etc. serán todas las clases que producen C cuando se duplican; este último conjunto se llamara Ω. El número de estas clases será igual al número de clases ambiguas o sea el número de generos. Habrá tantas clases en Ω que pertenecen al genero V como clases ambiguas en G. Por lo tanto, representando este número por a, en cada genero habrá a clases de Ω o bien ninguna. Como resultado, cuando a = 1, cada genero contendrá una clase de Ω; cuando a = 2, la mitad de todos los generos contendrá dos clases de Ω, el resto ninguna. De hecho, la mitad coincidirá totalmente con G ( según el significado planteado en III) y la segunda mitad con H o vice versa. Cuando a es mayor, la arásima parte de todos los generos incluirá clases de Ω (a clases en cada uno).
5. Supongamos ahora que C es una clase cuyo período contiene n terminos. Es obvio que en el caso donde a = 2 y n es par, ninguna clase de Ω puede pertenecer a G (puesto que esta clase estaría contenida en el período de la clase C; si fuera = rC, eso es 2rC = C, se tendría 2r ξ 1 (mod. n) Q. E. A. ). Por lo tanto, puesto que G pertenece a G, todas las clases de Ω deben distribuirse entre los generos H. De aquú, puesto que (para un determinante regular) hay en total φη clases en G con períodos de n terminos, para el caso cuando a = 2 habrá en total 2φη clases en cada genero de H con períodos de 2n terminos que incluirán tanto su propio genero como el genero principal. Cuando a = 1 habrá φn de estas clases en cada genero excepto el principal.
6. Dadas esas observaciones, ahora establecemos el siguiente metodo para construir el sistema de todas las clases propiamente primitivas para cualquier deter­minante regular dado (puesto que hemos descartado los determinantes irregulares). Escoja arbitrariamente una clase E con período de 2n terminos. Este período incluirá tanto su propio genero que llamamos V como el genero principal G; distribuya las clases de estos dos generos como se presentan en aquel período. El trabajo estará terminado cuando no hay otros generos salvo estos dos, o cuando no parece ser nece­sario agregar el resto de ellos (e.g., para un determinante negativo que posee solo dos generos positivos). Pero cuando hay cuatro o mas generos, los restantes se trataran de la siguiente manera. Sea V0 uno cualquiera de ellos, y V + V0 = V00. En V0 y V00 habrá dos clases ambiguas (una en cada uno o dos en uno y ninguna en el otro). Seleccione una de estas, A, de manera arbitraria y es claro que si A se compone con

cada una de las clases en G y V, se producen 2n clases distintas que pertenecen a V' y V'' que agotaran completamente estos generos; por lo tanto estos generos tambien se pueden ordenar. Si hay otros generos además de estos cuatro, sea V''' uno de los restantes y V'''', V''''' y V'''''' los generos que resultan de la composición de V''' con V, V' y V''. Estos cuatro generos V''' ...V"'"' contendrán cuatro clases ambiguas, y si una de ellas, A', se selecciona y se compone con cada una de las clases en G, V, V' y V'', se obtendrán todas las clases en V''' ...V"'"'. Si aun hay más generos restantes, contináe de la misma manera hasta que todos desaparezcan. Obviamente si el námero de generos construidos es 2μ, necesitaremos μ — 1 clases ambiguas en total, y cada clase de estos generos se puede generar mediante una multiplicacion de la clase E o componiendo una clase que resulta de tal multiplicacion con una o mas de las clases ambiguas. Siguen dos ejemplos de este procedimiento; no diremos mas sobre el uso de tal construction o de los artificios mediante los cuales se puede facilitar el trabajo.

I. El determinante —161.

Cuatro generos positivos, cuatro clases cada uno

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | G |  |  |  | V |  |  |
|  | 1, | 4; R7; | R23 |  | 3,4 | ; N7; R23 | |  |
| (1, | 0, | 161) | = K | (3, | 1, | 54) = | E |  |
| (9, | 1, | 18) | = 2E | (6, | —1, | 27) = | 3E |  |
| (2, | 1, | 81) | = 4E | (6, | 1, | 27) = | 5E |  |
| (9, | —1, | 18) | = 6E | (3, | —1, | 54) = | 7E |  |
|  |  | V |  |  |  | V |  |  |
|  | 3, | 4; R7; | N 23 |  | 1,4 | N7; N23 | |  |
| (7, | 0, | 23) | =A | (10, | 3, | 17) = | A+ | E |
| (11, | —2, | 15) | = A + 2E | (5, | 2, | 33) = | A+ | 3E |
| (14, | 7, | 15) | = A + 4E | (5, | —2, | 33) = | A+ | 5E |
| (11, | 2, | 15) | = A + 6E | (10, | —3, | 17) = | A+ | 7E |

II. El determinante -546  
Ocho generos positivos; tres clases en cada uno

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | G |  |  | V |
|  | 1 y 3, 8; R7; R7; Rl3 |  | 5 y 7, 8; N3; N7; N13 | |
| (1, | 0, 546) = K | (5, | 2, | 110) = E |
| (22, | -2, 25) = 2E | (21, | 0, | 26) = 3E |
| (22, | 2, 25) = 4E | (5, | -2, | 110) =5E |
|  | V0 |  |  | V00 |
|  | 1 y 3, 8; N3; R7; N13 |  | 5 y 7, 8; R3; N7; R13 | |
| (2, | 0, 273) = A | (10, | 2, | 55) = A + E |
| (11, | -2, 50)= A + 2E | (13, | 0, | 42) = A + 3E |
| (11, | 2, 50) = A + 4E | (10, | -2, | 55) = A + 5E |
|  | V 000 |  |  | V0000 |
|  | 1 y 3, 8; N3; N7; Rl3 |  | 5 y 7, 8; R3; R7; N13 | |
| (3, | O  00 | (15, | -3, | 37) = A0 + E |
| (17, | 7, 35) = A0 + 2E | (7, | 0, | 78) = A0 + 3E |
| (17, | -7, 35) = A0 + 4E | (15, | 3, | 37) = A0 + 5E |
|  | V00000 |  |  | V000000 |
|  | 1 y 3, 8; R3; N7; N13 |  | 5 y 7, 8; N3; R7; R13 | |
| (6, | 0, 91)= A + A0 | (23, | 11, | 29) = A + A0 + E |
| (19, | 9, 33) = A + A0 + 2E | (14, | 0, | 39) = A + A0 + 3E |
| (19, | -9, 33) = A + A0 + 4E | (23, | -11, | 29) = A + A0 + 5E |

Sección Sexta

APLICACIONES VARIAS DE LAS INVESTIGACIONES PRECEDENTES.

308.

A menudo hemos indicado cuán fructífera puede ser la aritmética superior para hechos que pertenecen a otras ramas de la matematica. Por esto vale la pena discutir algunas aplicaciones que merecen mas amplio desarrollo, sin embargo, sin intentar agotar un tema que puede facilmente llenar varios volúmenes. En esta sección trataremos primero de la descomposicion de fracciones en otras más simples y de la conversion de fracciones comunes en decimales. Explicaremos luego un metodo de exclusián que será átil para la solucián de ecuaciones indeterminadas de segundo grado. Finalmente, daremos nuevos metodos reducidos para distinguir námeros primos de nuámeros compuestos y para encontrar los factores de estos uáltimos. En la seccion siguiente estableceremos la teoría general de una clase especial de funciones que tiene mucha importancia en todo el analisis y que está estrechamente vinculada con la aritmetica superior. En particular agregaremos nuevos resultados a la teoría de secciones de un cárculo. Hasta ahora sálo los primeros elementos de esta teoría han sido conocidos.

*De la descomposición de fracciones en otras más simples*

309.

PROBLEMA. *Descomponer la fraccián* f*, cuyo denominador n es el producto de dos números primos relativos a y b en otras dos cuyos denominadores son a y b.*

Solución. Sean X e y las fracciones deseadas; se debe tener bx + ay = m; entonces x sera una raíz de la congruencia bx = m (mod. a) que puede ser encontrada por los metodos de la Sección II. Ademas y sera = .

Es claro que la congruencia bx = m tiene infinitas raíces, todas conguentes relativas a a; pero hay únicamente una que es positiva y menor que a. Tambien es posible que y sea negativo. Es apenas necesario hacer notar que podemos tambien encontrar y por la congruencia ay = m (mod. b) y x por la ecuación x = m j)ay. Por ejemplo, dada la fracción ||, 4 seró un valor de la expresión |γ (mod. 7), por tanto || se descompondrá en 7 + jj.

310.

Si se propone la fracción m con un denominador n, el cual es el producto de cualquier número de factores a, b, c, d, etc. primos entre sí, entonces por el artículo precedente se puede primero resolver en dos fracciones cuyos denominadores seróan a y bcd, etc.; luego la segunda de estas en dos fracciones con denominadores b y cd, etc.; la ultima de estas en otras dos y asó sucesivamente hasta que toda la fracción dada es reducida a la forma

*m*

*n*

α

*a*

β Y

+ y + - +  
bc

δ

- + etc. d

Evidentemente se pueden tomar los numeradores α, β, γ, δ, etc., positivos y menores que sus denominadores, excepto para el uóltimo, el cual ya no es arbitrario cuando los restantes han sido determinados. Este puede ser negativo o mayor que su denominador (si no presuponemos que m < n). En tal caso la mayoría de las veces seró ventajoso ponerlo en la forma | ^ k donde ε es positivo y menor que e y k es un entero. Y finalmente a, b, c, etc. pueden ser tomados como nómeros primos o como potencias de nómeros primos.

Ejemplo. La fracción cuyo denominador = 4 · 3 · 7 · 11 es resuelta de esta

manera en 4 + ; 2§T en f — ff; -f¡r en 7 — jj y escribiendo jj — 1 por — jj, tenemos

391 = 1 + 2 + 1+JL\_ 1 924 = 4 + L + 7 + Π 1

311.

La fracción — puede descomponerse de una única manera, en la forma θα + f + etc. ^ k tal que α, β, etc., sean positivos y menores que a, b etc.; esto es, suponiendo que

*m*

*n*

α β γ

+-—\ + etc. ^ k

*a b c*

α' β0

+ Τ

*ab*

Υ ,

+ + etc. ^ k'

c

y si α', β', etc., son tambien positivos y menores que a, b, etc., tendremos necesariamente α = α', β = β', γ = γ', etc., k = k'. Porque si multiplicamos por n = abc etc., tenemos m ξ αbcd etc. ξ α'bcd etc. (mod. a) y así, puesto que bcd etc. es primo relativo a a, necesariamente α ξ α' y por lo tanto α = α' y entonces β = β', etc., de donde inmediatamente k = k'. Ahora, puesto que es completamente arbitrario cual denominador es tomado primero, es evidente que todos los numeradores pueden ser investigados tal como se hizo con α en el artículo precedente, a saber, β por la congruencia βαcd etc. ξ m (mod. b), γ por γabd etc. ξ m (mod. c) etc. La suma de todas las fracciones así encontradas seró igual a la fracción — o la diferencia seró el entero k. Esto nos da un medio de verificar el cólculo. Así en el artículo precedente los valores de la expresión (mod. 4), (mod. 3), (mod. 7), 391 (mod. 11), proporcionaran inmediatamente los

numeradores 1, 2, 1 y 4 correspondientes a los denominadores 4, 3, 7 y 11 y la suma de estas fracciones excederó a la fracción dada en una unidad.

La conversión de fracciones comunes en decimales.

312.

Definición. Si una fraccion común es convertida en un decimal, a la serie de cifras decimales [[213]](#footnote-214)) (excluyendo la parte entera si la hay), tanto si es finita o infinita, la llamaremos mantisa de la fraccion. Aquó hemos tomado una expresion, que hasta ahora ha sido usada solamente para logaritmos, y extendido su uso. Asó, e.g., la mantisa de la fracción 1 es 125, la mantisa de la fraccion y| es 1875, y la de la fracción 37 es 054054 ... infinitamente repetida.

De la definicion, es inmediatamente claro que fracciones del mismo denomi­nador - y — tendrón la misma o diferente mantisa de acuerdo con que los numeradores n J n n

l y m sean o no congruentes según n. Una mantisa finita no cambia si se le agrega cualquier número de ceros a la derecha. La mantisa de la fracción 10m se obtiene desechando de la mantisa de la fracción m la primera cifra y en general la mantisa de la fracción 10nm se encuentra omitiendo las primeras ν cifras de la mantisa de

m. La mantisa de la fraccion n comienza inmediatamente con una cifra significativa (i.e. diferente de cero) si n no es > 10; pero si n > 10 y no igual a una potencia de 10, el nómero de cifras de las cuales estó formada es k, las primeras k — 1 cifras de la mantisa de n serán ceros y la krásima sera significativa. Por lo tanto, si n y m tienen mantisas diferentes (i.e. si l y m no son congruentes segón n), ellas de hecho no pueden tener las primeras k cifras idóenticas, sino que deben diferir al menos en la k-esima.

313.

PROBLEMA. Dado el denominador de la fracción m y las primeras k cifras de su mantisa, encontrar el numerador m, asumiendo que es menor que n.

Solución. Consideremos las k cifras como un entero. Multiplique por n y divida el producto por 10k (u omita las ultimas k cifras). Si el cociente es un entero (o todas las cifras omitidas son ceros), sera evidentemente el numero buscado y la mantisa dada estaraó completa; de otra forma el numerador que buscamos seraó el siguiente entero móas grande, o el cociente aumentado en una unidad, despuóes de omitir las siguientes cifras decimales. La razóon de esta regla se entiende tan fóacilmente a partir de lo establecido al final del articulo precedente que no es necesaria una explicación mas detallada.

Ejemplo. Si se constata que las dos primeras cifras de la mantisa de una fracción que tienen un denominador 23, es 69, tenemos el producto 23 · 69 = 1587. Desechando las últimas dos cifras y agregando una unidad, se produce el número 16 para el numerador buscado.

314.

Comenzamos con una consideracioón de fracciones cuyos denominadores son primos o potencias de primos, y posteriormente reduciremos las demóas a este caso. Observamos inmediatamente que la mantisa de la fracción pj (suponemos que el numerador a no es divisible por el nómero primo p) es finita y consiste de μ cifras cuando p = 2 o = 5; en el primer caso esta mantisa, considerada como un entero será = 5μα, en el ultimo caso = 2μα. Esto es tan obvio que no necesita explicación.

Pero si p es otro námero primo, 10rα nunca sera divisible por ρμ, no importa cuán grande tomemos a r, y por lo tanto, la mantisa de la fraccion F = Ρμ debe ser infinita. Supongamos que 10e es la menor potencia del námero 10 que es congruente con la unidad relativo al mádulo ρμ (cf. Seccion III, donde probamos que e es o igual al numero (p — 1)ρμ-1 o a un divisor de el.) Obviamente 10ea es el primer námero en la serie 10a, 100a, 1000a, etc., que es congruente a a relativo al mismo modulo. Ahora ya que, de acuerdo con el artículo 312, obtenemos las mantisas de las fracciones γμ, γβτ,... suprimiendo la primera cifra de la fraccián F, luego

las dos primeras cifras, etc., hasta que se hayan suprimido las e primeras cifras, es evidente que unicamente despues de las e primeras cifras, y no antes, las mismas se repetirán. Llamaremos a estas primeras e cifras que forman la mantisa por repeticián infinita de ellas mismas el período de esta mantisa o de la fraccion F. La magnitud del período, i.e. el numero e de cifras en el, es completamente independiente del numerador a y es determinado solo por el denominador. Así, e.g., el período de la fraccion γγ es 09 y el período de la fraccion 7 es 428571[[214]](#footnote-215)).

315.

Así cuando se conoce el período de alguna fraccion, se puede obtener la mantisa con tantas cifras como queramos. Ahora, si b = 10^a (mod. ρμ), podemos conseguir el período para la fraccion Ρμ si se escriben las primeras λ cifras del período de la fraccion F (suponiendo que λ < e, lo cual es permisible) despues de las restantes e — λ. Así, junto con el período de la fraccion F, tendremos al mismo tiempo los períodos de todas las fracciones cuyos numeradores sean congruentes a los numeros 10a, 100a, 1000a, etc., relativos al denominador ρμ. Así, e.g., ya que 6 = 3 · 102 (mod. 7), el período de la fraccián 7 se puede deducir inmediatamente del período de la fraccion 3, y el es 857142.

Por lo tanto, siempre que 10 es una raíz primitiva (art. 57 y 89) para el modulo ρμ, del per iodo de la fraccián Ρμ puede deducirse inmediatamente el per lodo de cualquiera otra fraccion ρμ (cuyo numerador m no es divisible por p), tomando de la izquierda y escribiendo a la derecha tantas cifras como unidades tenga el índice de

m cuando el número 10 es tomado como base. Así, es claro por que en este caso el número 10 se tomo siempre como base en la Tabla 1 (ver art. 72).

Cuando 10 no es una raíz primitiva, los Unicos períodos de fracciones que pueden ser derivados del período de la fracciún pj son aquellos cuyos numeradores son congruentes a alguna potencia de 10 segun ρμ. Sea 10e la mas pequeña potencia de 10 que es congruente a la unidad según ρμ; sea (p— 1)ρμ— = ef y tome como base una raíz primitiva r de modo que f sea el índice del número 10 (art. 71). En este sistema, los numeradores de las fracciones cuyos períodos pueden ser derivados del período de la fracción pj tendrán como índices f, 2f, 3f, ...ef — f; similarmente, del período de la fraccion pj, podemos deducir períodos para fracciones cuyos numeradores 10r, 100r, 1000r, etc. correspondan a índices f + 1, 2f + 1, 3f + 1, etc.; del período de la fracciún con numerador r2 (cuyo índice es 2) podemos deducir los períodos de las fracciones cuyos numeradores tienen índices f + 2, 2f + 2, 3f + 2, etc.; y en general, del período de la fracción con numerador r\* podemos derivar los períodos de fracciones cuyos numeradores tengan índices f + i, 2f + i, 3f + i, etc. Así, si únicamente se conocen los períodos de las fracciones cuyos numeradores son 1, r, r2, r3, ... , rf-1, se puede obtener todos los otros por transposition sola con la ayuda de la siguiente regla: Sea i el índice del numerador m de una fracciún dada pj en un sistema donde r es tomado como base (suponemos que i es menor que (p — 1)p^-1); dividiendo por f encontramos i = af + β, donde a y β son enteros positivos (o 0) y β < f; teniendo esto, podemos encontrar el período de la fracciún pj a partir del período de la fraccion cuyo numerador es re (es 1 cuando β = 0), poniendo las primeras a cifras despues de la restantes (cuando a = 0 mantenemos el mismo período). Esto explica como en la construction de la Tabla 1 seguimos la regla establecida en el artículo 72.

316.

De acuerdo con estos principios hemos construido una tabla para todos los denominadores de la forma ρμ menores que 1000, que publicaremos íntegramente o incluso con extensiones posteriores si una ocasiún se presenta. Por ahora damos como una muestra la Tabla III, que se extiende unicamente hasta 100 y no necesita explicaciún. Para denominadores que tienen 10 como una raíz primitiva, la tabla da los períodos de las fracciones con numerador 1 (a saber, para 7, 17, 19, 23, 29, 47, 59, 61, 97); para los demús, da los f períodos correspondientes a los numeradores 1, r, r2, ... , rf— que se denominan por los numeros (0), (1), (2), etc.; para la base r hemos tomado siempre la misma raíz primitiva que en la Tabla I. El período de cualquier

fracción cuyo denominador está contenido en esta tabla puede ser calculado por las reglas dadas en el artículo precedente. Pero, para denominadores muy pequeños podemos ejecutar lo mismo sin la Tabla 1, si por división ordinaria computamos tantas cifras iniciales de la mantisa, de acuerdo con el artículo 313, como sean necesarias para distinguirla de todas las otras del mismo denominador (por la Tabla III no son necesarias mas de 2). Ahora examinamos todos los períodos correspondientes al denominador dado, hasta que encontremos estas cifras iniciales, las cuales marcaran el inicio del período. Conviene advertir que estas cifras pueden ser separadas de modo que una (o mas) aparezcan al final de un período y las otras al comienzo.

Ejemplo. Bósquese el período de la fraccion 19. Para el modulo 19, por Tabla I tenemos ind. 12 = 2 ind. 2 + ind. 3 = 39 ξ 3 (mod. 18) (art. 57). Ya que para este caso existe unicamente un período correspondiente al numerador 1, es necesario transponer las primeras tres cifras al final y resulta el período buscado: 631578947368421052. Habría sido igualmente facil encontrar el comienzo del período por las primeras dos cifras, 63.

Si uno desea el período de la fracciín ||, ind. 45 = 2 ind. 3 + ind. 5 = 49, para el modulo 53. El nímero de períodos aquí es 4 = f y 49 = 12f + 1. De esta forma, del período marcado (1) es necesario transponer las primeras 12 cifras a la posicion final y el período buscado es 8490566037735. Las cifras iniciales, 84, estan separadas en la tabla.

Observaremos aquí, como prometimos en el artículo 59, que con la ayuda de la Tabla III podemos tambien encontrar el nímero que corresponde a un índice dado para un mídulo dado (en la tabla el modulo se lista como un denominador). Por esto es claro, de lo que precede, que se puede encontrar el período de una fracciín a cuyo numerador (si bien desconocido) corresponde el índice dado. Es suficiente tomar tantas cifras iniciales de este período como cifras haya en el denominador. De esto, por el artículo 313 se encuentra el numerador o el numero correspondiente al índice dado.

317.

Por el metodo precedente, la mantisa de cualquier fracciín cuyo denominador es un numero primo o una potencia de un nímero primo dentro de los límites de la tabla, se puede determinar sin calculo. Pero con la ayuda del resultado del comienzo de esta seccion, podemos extender el uso de esta tabla mas alla e incluir todas las fracciones cuyos denominadores son productos de primos o potencias de primos

situados dentro de sus límites. Pues, ya que tal fracción puede ser descompuesta en otras cuyos denominadores son estos factores, y estas pueden ser convertidas en fracciones decimales con cualquier numero de cifras, solamente necesitamos combinar todas ellas en una suma. Es apenas necesario hacer notar que la última cifra de la suma puede evidenciar ser poco menos de lo que debiera, pero evidentemente los errores no agregan hacia arriba tantas unidades como fracciones individuales hayan sido agregadas, así, sera apropiado computarlas a mas cifras que las que se buscan para la fracciún dada. Por ejemplo, consideremos la fraccion 1271808720 = F[[215]](#footnote-216)), cuyo denominador es el producto de los números 16, 9, 5, 49, 13, 47 y 59. Por las reglas dadas arriba encontramos que F = 1 + + 9 + 5 + 22 + \_5\_ + \_¡7 + 52. estas fracciones

individuales se convierten en decimales como sigue:

1

1

0.6875

0.8

|  |  |  |
| --- | --- | --- |
| 0.4444444444 | 4444444444 | 44 |
| 0.4489795918 | 3673469387 | 75 |
| 0.3846153846 | 1538461538 | 46 |
| 0.1489361702 | 1276595744 | 68 |
| 0.8813559322 | 0338983050 | 84 |
| 4.7958315233 | 1271954166 | 17 |

11

16

4

1. 4 9

22

49

13

\_7

47

52

59

F

El error en esta suma es ciertamente menor que cinco unidades en la vigesima segunda cifra y así las primeras veinte son exactas. Llevando los calculos a mas cifras, encontramos en lugar de las últimas dos cifras, 17, el número 1893936... . Sera obvio para todos que este metodo de convertir fracciones comunes en decimales es especialmente útil cuando buscamos una gran cantidad de cifras decimales; cuando

unas pocas bastan, la división ordinaria o los logaritmos pueden ser usados con igual facilidad.

318.

De esta manera, ya que hemos reducido la resolucion de tales fracciones con denominador compuesto de varios números primos diferentes al caso en que el denominador es primo o una potencia de un primo, necesitamos agregar solamente unas pocas notas concernientes a sus mantisas. Si el denominador no contiene los factores 2 y 5, la mantisa tambien consistirú de períodos, porque en este caso la serie 10, 100, 1000, etc. llegarú eventualmente a un termino que es congruente a la unidad segun el denominador. A la vez el exponente de este termino, que puede facilmente determinarse por los metodos del artículo 92, indicara el tamaño del período independientemente del numerador, siempre que sea primo relativo al denominador. Si el denominador es de la forma 2α5βN, donde N designa un número primo relativo a 10, α y β números de los cuales al menos uno no es 0, la mantisa de la fraccion llegara a ser periodica despues de las primeras α o β cifras (el que sea mayor) y los períodos tendrún la misma longitud que los períodos de fracciones que tienen denominador N. Esto es facil de ver, ya que la fraccion es resoluble en otras dos con denominadores 2α 5e y N, y la primera de ellas cesa enteramente despues de las primeras α o β cifras. Podemos facilmente agregar muchas otras observaciones concernientes a este asunto, especialmente en lo que se refiere a artificios para la construccion de una tabla como la III. Sin embargo omitiremos esta discusion, por motivos de brevedad y porque una gran cantidad de esto ha sido ya publicado por Robertson (loc. cit.) y por Bernoulli (Nouv. Mém de l’Ac. de Berlin, 1771, p. 273).

Solución de la congruencia x2 = A por el método de exclusion.

319.

Con respecto a la congruencia x2 = A (mod. m), la cual es equivalente a la ecuaciún indeterminada x2 = A + my, en Seccion IV (art. 146) hemos tratado su posibilidad de una manera que no parece requerir ninguún estudio adicional. Para encontrar la incognita misma, sin embargo, observamos antes (art. 152) que los metodos indirectos son preferibles a los directos. Si m es un número primo (los otros casos pueden ser reducidos fúcilmente a este), podemos usar la tabla de úndices I (combinada con la III de acuerdo con la observación del art. 316) para este propósito, como lo demostramos más generalmente en el artículo 60, pero el método estará restringido por los límites de la tabla. Por estas razones esperamos que el siguiente metodo general y conciso placera a los aficionados de la aritmetica.

Primero observamos que es suficiente conocer solamente aquellos valores de x que son positivos y no mayores que 2m, ya que los otros serán congruentes modulo m a uno de estos, tomado ya sea positiva o negativamente. Para un tal valor de x, el valor de y esta necesariamente contenido dentro de los límites —A y 1 m — A. Por ende el máetodo obvio consiste en esto, para cada valor de y contenido dentro de estos límites (denotamos al conjunto de ellos por Ω) computamos el valor de A + my (llamamos a este, V) y retenemos solamente aquellos valores para los cuales V es un cuadrado. Cuando m es un numero pequeño (e.g. abajo de 40), el numero de pruebas es tan pequeno que apenas se necesita de un atajo; pero cuando m es grande, la labor puede ser acortada tanto como usted quiera por el siguiente método de exclusión.

320.

Sea E un entero arbitrario primo relativo a m y mayor que 2; y sean a, b, c, etc. todos sus no residuos cuadraticos diferentes (i.e. no congruentes segun E); y sean α, β, γ, etc. las raíces de las congruencias

A + my = a, A + my ξ b, A + my ξ c, etc.

segun el modulo E, con todas estas raíces positivas y menores que E. Si y es un valor congruente a uno de los numeros α, β, γ, etc., entonces el valor resultante de V = A + my sera congruente a uno de los numeros a, b, c, etc. y así sera un no residuo de E y no podra ser un cuadrado. Así, inmediatamente, pueden excluirse como inservibles todos los valores en Ω que estan contenidos en las formas Et + α, Et+β, Et + γ, etc.; sera suficiente examinar a los demas y llamaremos a este conjunto Ω0. En esta operación el numero E puede llamarse numero excluyente.

Tomando otro numero excluyente E0 apropiado, del mismo modo se encuen­tran tantos numeros α0, β0, γ0, etc. como no residuos cuadraticos diferentes haya; y no puede ser congruente a ellos segun el modulo E0. Ahora se puede remover de nuevo de Ω0 todos los numeros contenidos en las formas E0t + α0, E0t + β0, E0t + γ0, etc. De esta manera se puede continuar excluyendo numeros hasta que aquellos contenidos en Ω sean reducidos hasta el punto que no haya mas dificultad en examinar los restantes que en construir nuevas exclusiones.

Ejemplo. Dada la ecuación x2 = 22 + 97y, los límites de los valores de y serán —97 y 241 — 97. Así (ya que el valor 0 es obviamente inótil) Ω incluiró los nómeros 1, 2, 3, ... 24. Para E = 3 hay ónicamente un no residuo, a = 2; así α = 1. Excluyendo de Ω todos los nómeros de la forma 3t + 1, Ω0 contendrá los 16 nómeros restantes. Similarmente, para E = 4 resulta a = 2, b = 3, y asó α = 0, β = 1; y debemos desechar los nómeros de la forma 4t y 4t + 1. Los ocho nómeros restantes son 2, 3, 6, 11, 14, 15, 18 y 23. Igualmente, para E = 5 se debe desechar los nómeros de la forma 5t y 5t + 3 y se quedan 2, 6, 11 y 14. Tomando E = 6, se deben remover los nómeros de la forma 6t +1 y 6t + 4, pero estos ya habóan sido removidos (ya que son nómeros de la forma 3t + 1). Tomando E = 7, desechamos los nómeros de la forma 7t + 2, 7t + 3, 7t + 5 y se dejan 6, 11 y 14. Si sustituimos y por estos, dan V = 604, 1089 y 1380 respectivamente. Unicamente el segundo valor es un cuadrado, asó x = ^33.

321.

Como la operación con el nómero excluyente E desecha de los valores de V correspondientes a los valores de y en Ω, todos aquóellos que son no residuos cuadráticos de E, pero no toca los residuos del mismo nómero, es obvio que el efecto de usar E y 2E no difiere si E es impar, ya que en este caso E y 2E tienen los mismos residuos y no residuos. Asó, si usamos sucesivamente los nuómeros 3, 4, 5, etc. como excluyentes, podemos omitir los nómeros ξ 2 (mod. 4), es decir 6, 10, 14, etc., como superfluos. La doble operation, usando E y E0 como excluyentes, remueve todos aquellos valores de V que son no residuos de ambos E y E0 o de uno de ellos y deja todos los que son residuos de ambos. Ahora, ya que en el caso en que E y E0 no tienen un divisor comón, los nómeros desechados son todos no residuos y los que permanecen son residuos del producto EE0, es evidente que, usando el excluyente EE0, se obtendrá en efecto el mismo resultado que usando los dos E y E0 y su uso es, por lo tanto, superfluo. Asó, es permisible omitir todos aquellos nuómeros excluyentes que pueden ser resueltos en dos factores relativamente primos, y es suficiente usar aquellos que son o primos (no divisores de m) o potencias de primos. Finalmente es claro que, despues de usar el nómero excluyente ρμ que es una potencia del nómero primo p, los nómeros excluyentes p y pv con ν < μ son superfluos. Pues, ya que ρμ deja solamente sus residuos de entre los valores de V, ciertamente no habrá no residuos de p o de una potencia menor pv. Si p o pv fueron usados antes que p^, el ultimo evidentemente puede desechar solamente aquellos valores de V que son al

mismo tiempo residuos de p (o pv) y no residuos de ρμ; por lo tanto es suficiente tomar para a, b, c, etc., Unicamente tales no residuos de ρμ.

322.

El calculo de los números α, β, γ, etc. correspondientes a cualquier excluyente dado E, puede ser en gran parte abreviado por las siguientes observaciones. Sean A, B, C, etc. raíces de las congruencias my = a, my = b, my = c, etc. (mod. E) y k una raíz de my = —A. Es claro que α = A + k, β = B + k, γ = C + k, etc. Ahora, si fuera necesario encontrar A, B, C, etc. resolviendo estas congruencias, este metodo de encontrar α, β, γ, etc. no sería mas corto que el que hemos mostrado antes; pero esto no es necesario de ningún modo. En efecto, si E es un número primo y m es un residuo cuadratico de E, es claro por el artículo 98 que A, B, C, etc., i.e., los valores de las expresiones J, Jl , JL, etc. (mod. E), son no residuos diferentes de E y así son identicos con α, β, γ, etc., si no prestamos atención a su orden, el cual de todas formas no importa aquí. Si en la misma suposicion m es un no residuo de E, los números A, B, C, etc., son identicos con todos los residuos cuadraticos, excluyendo el 0. Si E es el cuadrado de un número primo (impar), = p2, y p ya ha sido usado como excluyente, es suficiente, de acuerdo con el artículo precedente, tomar para a, b, c, etc. aquellos no residuos de p2 que son residuos de p, i.e. los números p, 2p, 3p, ...p2 — p (todos los numeros menores que p2 que son divisibles por p, excepto 0); entonces para A, B, C, etc., debemos obtener exactamente los mismos números pero en diferente orden. Similarmente, si se pone E = p3 despues de aplicar los números excluyentes p y p2, sera suficiente tomar para a, b, c, etc. los productos de cada uno de los no residuos de p por p2. Como un resultado obtendremos para A, B, C, etc., o los mismos numeros o los productos de p2 con cada residuo de p excepto 0, según sea m un residuo o un no residuo de p . En general, tomando para E cualquier potencia de un número primo, digamos prí, despues de aplicar todas las potencias menores, obtendremos para A, B, C, etc. los productos de p^-1 por todos los números menores que p excepto 0, cuando μ es par, o por todos los no residuos de p que sean menores que p cuando μ es impar y mRp, o por todos los residuos cuando mNp. Si E = 4 y a = 2, b = 3 tenemos para A, B, o 2 y 3 o 2 y 1, según sea m = 1 ó = 3 (mod. 4). Si despues de usar el excluyente 4, ponemos E = 8 tendremos α = 5 y A sería 5, 7, 1, 3 segun sea m = 1, 3, 5, 7 (mod. 8). En general, si E es una potencia mús alta de 2, digamos 2μ, y todas las potencias menores ya han sido aplicadas, debe ponerse a = 2μ-1, b = 3 · 2μ-2 cuando μ es par. Esto nos da A = 2μ-1 y B = 3 · 2μ-1 o

= 2μ-2 según sea m = 1o ξ 3. Pero cuando μ es impar, debemos poner a = 5 · 2μ-3 y A sera igual al producto del número 2μ-3 por 5, 7, 1 o 3 según sea m = 1, 3, 5 o 7 (mod. 8).

Pero un matematico experto fúcilmente encontrara un metodo para desechar mecánicamente los valores de y inservibles que estan en Ω despues de computar los números α, β, γ, etc. mediante tantas exclusiones como parezcan necesarias. Pero no tenemos espacio para discutir este u otro artificio de economía de trabajo.

Solución de la ecuación indeterminada mx2 + ny2 = A por exclusiones.

323.

En la sección V dimos un metodo general para encontrar todas las representa­ciones de un A dado por la forma binaria mx2+ny2 o sea para encontrar las soluciones de la ecuacion indeterminada mx2 + ny2 = A. El metodo no deja nada que desear desde el punto de vista de brevedad si ya tenemos todos los valores de la expresioún \J-mn según el módulo A mismo y según A dividido por sus factores cuadrados. Para el caso, no obstante, en que mn es positivo, daremos una solucion que es mucho mas corta que la directa cuando aquellos valores no hayan sido computados. Supong­amos que los nuúmeros m, n y A son positivos y primos entre sú, ya que el otro caso puede fúcilmente ser reducido a este. Serú suficiente deducir valores positivos de x e y, ya que los otros pueden ser reducidos a estos por un sencillo cambio de signos.

Claramente x debe ser tal que A , el cual designaremos por V, es positivo,

X.

entero, y cuadrado. La primera condiciún requiere que x no sea mayor que y χχ; la segunda se tiene cuando n = 1, de otro modo requiere que el valor de la expresiún d (mod. n) sea un residuo cuadrático de n. Si designamos todos los diferentes valores

(mod. n) por ±r, ±r0, etc., x deberá estar contenido en una de

de la expresiúon

las formas nt + r, nt — r, nt + r0, etc. La manera mas simple serú sustituir x por todos los números de estas formas abajo del límite (llamaremos a este conjunto Ω) y conservar unicamente aquellos para los cuales V es un cuadrado. En el siguiente artúculo mostraremos como reducir el número de estas pruebas tanto como deseemos.

324.

El metodo de exclusiones por el cual efectuamos esto, tal como en la discusiún precedente, consiste en tomar arbitrariamente varios nuúmeros que nuevamente llamaremos números excluyentes, en buscar los valores de x para los cuales el valor

* se convierte en un no residuo de estos números excluyentes y en desechar de Ω estos valores de x. El razonamiento aquí es totalmente analogo al del artículo 321, y así deberemos usar como números excluyentes solamente aquellos que son primos o potencias de primos, y en el último caso necesitamos desechar solamente aquellos no residuos, entre los valores de V, que son residuos de todas las potencias inferiores del mismo nuúmero primo, si es que comenzamos la exclusiúon con úestas.

Por lo tanto, sea E = pA el numero excluyente (incluyendo tambien el caso donde μ = 1) con p un número primo que no divide m, y supongamos [[216]](#footnote-217)) que pv es la mayor potencia de p que divide a n. Sean a, b, c, etc. no residuos cuadraticos de E (todos ellos cuando μ = 1; los necesarios, i.e. aquellos que son residuos de potencias inferiores, cuando μ > 1). Compute las raíces α, β, γ, etc. de las congruencias mz = A — na, mz = A — nb, mz = A — nc, etc. (mod. Epv = pμ+ν). Es facil ver que si para algun valor de x resulta x2 = α (mod. Epv), el correspondiente valor de

* serú = a (mod. E), esto es, un no residuo de E y similarmente para los restantes

números β, γ, etc. Recíprocamente, es igualmente facil ver que si un valor de x produce V = a (mod. E), para el mismo valor se hace x2 = α (mod. Epv). Asú, todos los valores de x para los cuales x2 no es congruente a alguno de los números α, β, γ, etc. (mod. Epv) producirán valores de V que no son congruentes a ninguno de los números a, b, c, etc. (mod. E). Ahora se seleccionan de entre los números α, β, γ, etc. todos los residuos cuadrúticos g, g, g", etc. de Epv. Compute los valores de las expresiones ^/g, -^/g7, , etc. (mod. Epv) y desígnelos como ±h, ±h7, ±h", etc.

Habiendo hecho esto, todos los numeros de las formas Epvt ± h, Epvt ± h7, Epvt ± h", etc. pueden, sin peligro, ser desechados de Ω, y los valores de V contenidos en las formas Eu + a, Eu + b, Eu + c, etc. no pueden corresponder a ningún valor de x en Ω despues de esta exclusion. Ademas es evidente que valores de x en Ω no pueden producir tales valores de V cuando ninguno de los numeros α, β, γ, etc. es un residuo cuadrútico de Epv. En este caso, por consiguiente, el número E no puede ser usado como excluyente. De esta manera se pueden usar tantos números excluyentes como deseemos y consecuentemente disminuir los numeros en Ω a voluntad.

Veamos ahora si es permisible usar primos que dividen a m o potencias de tales numeros primos como numeros excluyentes. Sea B un valor de la expresión An (mod. m); es claro que V serú siempre congruente a B segun el múd^o m, no importa que valor se tome para x. Asú, para que la ecuaciún propuesta sea posible, es necesario que B sea un residuo cuadratico de m. Si p es un divisor primo e impar de

m, por hipótesis, no divide a n o a A y por eso no divide a B. Para cualquier valor de x, V sera un residuo de p y así tambien de cualquier potencia de p; por lo tanto, ni p ni cualquiera de sus potencias pueden ser tomados como excluyentes. Similarmente, cuando m es divisible por 8, para hacer posible la ecuacion propuesta, se requiere que B ξ 1 (mod. 8) y así, para cualquier valor de x, V sera ξ 1 (mod. 8) y las potencias de 2 no serán idoneas como excluyentes. Sin embargo, cuando m es divisible por 4 pero no por 8, por la misma razon debemos tener B ξ 1 (mod. 4) y el valor de la expresion 3 (mod. 8) sera o 1 o 5 y lo designaremos por C. Para un valor par de x tendremos V ξ C; para un valor impar V ξ C + 4 (mod. 8). Y así, los valores pares deben ser desechados cuando C = 5, y los valores impares cuando C = 1. Finalmente, cuando m es divisible por 2 pero no por 4, sea C como antes, un valor de la expresion 3 (mod. 8) que sera 1, 3, 5 o 7; y sea D un valor de 33 (mod. 4) el cual sera 1 o 3. Ahora, ya que el valor de V es siempre ξ C — 2Dx2 (mod. 8) y así para x par, ξ C, para x impar, ξ C — 2D, se sigue que todos los valores impares de x deben ser desechados cuando C = 1, todos los valores pares cuando C = 3 y D = 1o C = 7 y D = 3. Todos los valores restantes producirán V ξ 1 (mod. 8); es decir, V es un residuo de alguna potencia de 2. En los casos restantes, a saber, cuando C = 5, o C = 3 y D = 3, o C = 7y D = 1, tenemos V ξ 3, 5 o 7 (mod. 8), no importa si x es impar o par. Se sigue en estos casos que la ecuacion propuesta no tiene solucion del todo.

Ahora, de la misma forma en que encontramos x por el metodo de exclusion, podemos tambien encontrar y. Así, hay siempre dos maneras de aplicar el metodo de exclusion para la solucion de un problema dado (a menos que m = n = 1, cuando los dos coinciden). Deberíamos usualmente escoger aquel para el cual el numero de terminos Ω es menor, lo que se puede estimar facilmente por adelantado. Es apenas necesario observar que si, despues de un numero de exclusiones, todos los numeros en Ω son desechados, esto debe ser considerado como una indicacion segura de la imposibilidad de la ecuacion propuesta.

325.

Ejemplo. Sea la ecuacion dada 3x2 + 455y2 = 10857362. La resolveremos de dos maneras, primero investigando los valores de x y luego los valores de y. El límite en x aquí es ^3619120 3, el cual cae entre 1902 y 1903; el valor de la expresion 3 (mod. 455) es 354 y los valores de la expresion V354 (mod. 455) son ±82, ±152, ±173, ±212. Así Ω consiste de los siguientes 33 números: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. El número 3 no puede ser usado, en este caso, para exclusion porque divide a m. Para el número excluyente 4, tenemos a = 2, b = 3 así α = 0, β = 3, g = 0y los valores de la expresiún yjg (mod. 4) son 0 y 2; así, todos los numeros de la forma 4t y 4t + 2, i.e. todos los números pares, deben ser desechados de Ω; denotaremos los 16 restantes por Ω0. Para E = 5, el cual tambien divide a n, las raíces de las congruencias mz = A — 2n y mz = A — 3n (mod. 25) son 9 y 24, ambos residuos de 25. Los valores de las expresiones -\/9 y \/24 (mod. 25) son ±3, ±7. Cuando desechamos de Ω' todos los números de las formas 25t ± 3, 25t ± 7, allú permanecen estos diez (Ω00): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Para E = 7 las raíces de las congruencias mz ξ A — 3n, mz ξ A — 5n, mz ξ A — 6n (mod. 49) son 32, 39, 18, todas ellas residuos de 49, y los valores de las expresiones -\/32, -\/39, \/Ϊ8 (mod. 49) son ±9, ±23, ±19. Cuando desechamos de Ω" los números de las formas 49t ± 9, 49t ± 19 y 49t ± 23, estos cinco (Ω000) permanecen: 537, 737, 1083, 1213, 1517. Para E = 8 tenemos a = 5, asú α = 5, un no residuo de 8; por lo tanto el excluyente 8 no puede ser usado. El número 9 debe ser desechado por la misma razón que 3. Para E =11 los numeros a, b, etc. se convierten en 2, 6, 7, 8, 10; ν = 0; asú los números α, β, etc. = 8, 10, 5, 0, 1. Tres de ellos, 0, 1, 5 son residuos de 11 y por esta razon desechamos de Ω'" los números de las formas 11t, 11t ± 1, 11t ± 4. Permanecen los números 537, 1083, 1213. Usando estos obtenemos para V los valores 21961, 16129, 14161 respectivamente. Solamente el segundo y el tercero son cuadrados. Asú la ecuación dada admite solamente dos soluciones con valores positivos de x e y: x = 1083, y = 127 y x = 1213, y = 119.

Segundo. Si preferimos encontrar la otra incognita de esta misma ecuacion por exclusiones, intercambiamos x e y y la escribimos como 455x2 + 3y2 = 10857362, asú que podemos retener la notaciún de los artúculos 323 y 324. El Emite para los valores de x cae entre 154 y 155; el valor de la expresiún ^ (mod. n) es 1; los valores de -\/I (mod. 3) son +1 y —1. Por lo tanto Ω contiene todos los números de las formas 3t + 1 y 3t — 1, es decir, todos los números hasta 154 inclusive que no son divisibles por 3, de los cuales hay 103. Aplicando las reglas dadas arriba para excluir 3, 4, 9, 11, 17, 19 y 23, debemos desechar los números de las formas 9t ±4; 4t, 4t ± 2, o sea todos los pares; 27t ± 1, 27t ± 10; 11t, 11t ± 1, 11t ± 3; 17t ± 3, 17t ± 4, 17 ± 5, 17t ± 7; 19t ± 2,

19t ± 3, 19t ± 8, 19t ± 9; 23t, 23t ± 1, 23t ± 5, 23t ± 7, 23t ± 9, 23t ± 10. Despues de que todos estos han sido suprimidos, hemos dejado los numeros 119 y 127, que dan

a V un valor cuadrado y producen las mismas soluciones que obtuvimos arriba.

326.

Los metodos precedentes son ya tan concisos que dejan muy poco que desear. No obstante hay muchos artificios, para acortar la operación, de los cuales podemos tocar aquí solamente unos pocos. Por lo tanto restringiremos nuestra discusion al caso en el que el número excluyente es un primo impar que no divide a A, o una potencia de un tal primo. Los casos restantes pueden ser tratados de modo analogo o reducidos a este. Suponiendo primero que el número excluyente E = p es un primo que no divide ni a m ni a n y los valores de las expresiones É, — na, — TÉ, — nc, etc. (mod. p) son k, A, B, C, etc. respectivamente, se obtienen los numeros α, β, γ, etc. de las congruencias α = k + A, β = k + B, γ = k + C, etc. (mod. p). Los números A, B, C, etc. pueden ser determinados, sin calcular las congruencias, por un artificio muy parecido al que usamos en el artículo 322, y serán identicos con todos los no residuos o con todos los residuos de p (excepto 0), de acuerdo con el valor de la expresion — É (mod. p), o (lo que es la misma cosa) segun sea el numero —mn un residuo o un no residuo de p. Así, en el ejemplo II del artículo precedente, para E = 17 tenemos k = 7; —mn = —1365 = 12 es un no residuo de 17; así, los numeros A, B, etc. serán 1, 2, 4, 8, 9, 13, 15, 16 y los numeros α, β, etc. serán 8, 9, 11, 15, 16, 3, 5, 6. Los residuos entre ellos son 8, 9, 15 y 16, así ±h, h', etc. se convierten en ±5, 3, 7, 4. Quienes hayan resuelto a menudo problemas de este tipo encontraran esto extremadamente util si calculan para varios numeros primos p los valores de h, h', etc. correspondientes a valores individuales de k (1, 2, 3, ...p — 1) bajo la doble suposicion (a saber, donde —mn es un residuo y donde es un no residuo de p). Observamos que hay siempre 2(p — 1) numeros h, —h, h', etc. cuando los numeros k y —mn son ambos residuos o ambos no residuos de p; 2 (p — 3) numeros cuando el primero es un residuo y el ultimo un no residuo; 2 (p +1) números cuando el primero es un no residuo y el ultimo un residuo; pero debemos omitir la demostracion de este teorema para no ser demasiado prolijos.

Segundo, podemos explicar un tanto expeditamente los casos cuando E es un número primo que divide a n, o la potencia de un numero primo (impar) que divide o no divide a n. Trataremos todos estos casos juntos y, reteniendo la notacion del artículo 324, pondremos n = n'pv tal que n' no es divisible por p. Los numeros α, b, c, etc. serán los productos del numero p^-1 por todos los números menores que p (excepto 0) o por todos los no residuos de p menores que p, segun μ sea par o

impar. Expresamos esto indefinidamente por upμ—1. Sea k el valor de la expresión mm (mod. ρμ+νel cual no será divisible por p porque A no lo es. Todos los α, β, γ, etc. serán congruentes a k modulo p, y así ρμ no excluirá nada de Ω si kNp. Si realmente kRp y así tambien kRpA+v, sea r un valor de la expresián y/k (mod. pA+v) que no es divisible por p, y sea e el valor de — (mod. p). Entonces tendremos

α = r2 + 2erapv (mod. pA+v) y claramente α es un residuo de p^+v y los valores de la expresion -^/α (mod. pA+v) se convierten en ±(r + eapv), así, todos los h, h0, h", etc. son expresados por r + uep^+v-1. Finalmente concluimos que los námeros h, h0, h00, etc. provienen de la adicián del námero r con los productos del námero p^+v-1 por todos los námeros menores que p (excepto 0) cuando μ es par; o por todos los no residuos de p menores que este límite cuando μ es impar y eRp o, lo que viene a ser la misma cosa, cuando — 2mrn0Rp; o por todos los residuos (excepto 0) cuando μ es impar y —2mrn'Np.

Pero exactamente como encontramos los námeros h, h0, etc. para cada uno de los números excluyentes, será posible ejecutar la misma exclusion por operaciones mecánicas que el experto puede desarrollar fácilmente si esto le parece átil.

Finalmente debemos observar que cualquier ecuacián ax2 + 2bxy + cy2 = M en la que b2 — ac es negativo, digamos —D, puede ser facilmente reducida a la forma que consideramos en el artículo precedente. Porque si hacemos m el maximo comun divisor de los námeros a y b, y ponemos

D

a x+b y=x

a = ma0, b = mb',

0 02

— = a c — mb = n, m

la ecuacion será equivalente a mx02 + ny2 = a0M. Esto puede ser resuelto por las reglas que dimos antes. Solamente van a ser retenidas aquellas soluciones en las cuales x0 — b0y es divisible por a0, i.e. las que dan valores enteros de x.

Otro método de resolver la congruencia x2 = A para el caso en que A es negativo.

327.

La solucián directa de la ecuacion ax2 + 2bxy + cy2 = M contenida en la seccion V asume que conocemos los valores de la expresion Vb2 — ac (mod. M). Recáprocamente, en el caso donde b2 — ac es negativo, la solucián indirecta anterior da un metodo muy rapido de encontrar tales valores y es preferible al metodo del artfculo 322 y siguientes, especialmente para un valor muy grande de M. Pero supondremos que M es un nuámero primo o, al menos, si es compuesto, que sus factores son emperodesconocidos. Pues si fuera claro que el número primo p divide a M y si M = ρμΜ' de tal forma que M0 no involucre el factor p, sería mas conveniente explorar los valores de la expresión Vb2 — ac para los modulos ρμ y M0 separadamente (obteniendo el primero de los valores según el módulo p, art. 101) y luego deducir los valores segun el modulo M de su combinación (art. 105).

Entonces, es necesario buscar todos los valores de la expresión —D (mod. M) donde D y M son positivos, y M esta contenido en una forma de los divisores de x2 + D (art. 147 y siguientes). De otro modo sería a priori evidente que no hay numeros que satisfagan la expresion dada. Los valores buscados serón siempre opuestos dos a dos. Sean ellos ±r, ±r0, ±r00, etc., y D + r2 = Mh, D + r0 = Mh', D + r00 = Mh", etc.; posteriormente designe las clases a las cuales corresponden las formas (M, r, h), (M, —r, h), (M, r0, h0), (M, —r0, h0), (M, r00, h00),

(M, —r00, h00), etc. respectivamente por C, — C, C0, —C0, C00, — C00, etc. y al conjunto de ellas por G. Hablando en general, estas clases son las que serón consideradas como incógnitas. Sin embargo es claro primero, que todas ellas son positivas y propiamente primitivas, segundo, que ellas corresponden al mismo genero cuyo carácter es facilmente reconocible a partir de la naturaleza del nómero M, i.e. de sus relaciones con cada uno de los divisores primos de D (y con 4 u 8 cuando sea necesario) (cf. art. 230). Ya que suponemos que M esta contenido en una forma de los divisores de x2 + D, sabemos a priori que de seguro hay un genero positivo propiamente primitivo de determinante —D para este carócter aón cuando no haya valores de la expresión V—D (mod. M). Ya que, por lo tanto, este genero es conocido, se puede encontrar todas las clases contenidas en el. Desógnense como C, C0, C00, etc. y el conjunto de ellas por G. Es claro entonces que las clases individuales C, — C, etc. deben ser identicas con clases en G; tambien puede suceder que varias clases en G sean identicas unas a otras y con la misma clase en G; y cuando G contiene solamente una clase, de seguro todas las clases en G coincidiran con ella. Por lo tanto si de las clases C, C0, C00, etc. seleccionamos las (mas simples) formas f, f0, f00, etc. (una de cada una), de entre estas aparecerá una forma de cada clase en G. Ahora, si ax2 + 2bxy + cy2 es una de las formas contenidas en C, existirán dos representaciones del numero M correspondiendo al valor r por esta forma, y si una es x = m, y = n, la otra sera x = —m, y = —n. La unica excepcion ocurre cuando D = 1, en cuyo caso existirán cuatro representaciones (ver art. 180).

Se sigue de esto que si se encuentran todas las representaciones del numero M por las formas individuales f, f0, f00, etc. (usando el metodo indirecto de los artículos precedentes) y deducimos de estos los valores de la expresion V—D (mod. M) a la cual cada una pertenece (art. 154 y siguientes), obtendremos todos los valores de esta expresión, y realmente cada uno de ellos dos veces o, si D = 1, cuatro veces. Q. E. F. Si encontramos alguna forma entre las f, f', etc. por la cual M no puede ser representada, esto es una indicación de que ella no pertenece a una clase en G y así puede ser olvidada. Pero si M no puede ser representada por ninguna de esta formas, —D es necesariamente un no residuo cuadrático de M. Tocante a estas operaciones se tienen las siguientes observaciones.

1. Las representaciones del numero M por las formas f, f', etc. que usamos aquí son aquellas en las cuales los valores de las incógnitas son primos relativos; si aparecen otras en las que estos valores tienen un divisor comón μ (esto puede suceder solamente cuando μ2 divide a M, y sucede con seguridad cuando —DRMf), ellas serón completamente desatendidas para nuestros presentes propositos, aun cuando pueden ser uótiles en otros contextos.
2. Siendo otras cosas iguales, es obvio que la labor implicada sera mós facil cuando el nuómero de clases f, f0, f00, etc. sea menor. Por consiguiente, esto es lo mas corto posible cuando D es uno de los 65 numeros tratados en el artículo 303, porque tienen solamente una clase en cada góenero.
3. Dado que existen siempre dos representaciones x = m, y = n y x = —m, y = —n correspondiendo al mismo valor, es obviamente suficiente considerar únicamente aquellas representaciones en las cuales y es positivo. Tales representa­ciones diferentes corresponderán siempre a diferentes valores de la expresión V—D (mod. M), y el nómero de todos los valores diferentes seró igual al nómero de tales representaciones (siempre exceptuando el caso cuando D = 1 donde el primer nuómero seróa la mitad del segundo).
4. Puesto que, tan pronto como conocemos uno de los dos valores opuestos +r, —r, conocemos inmediatamente el otro, las operaciones pueden ser abreviadas un tanto. Si el valor se obtiene de la representación del nómero M por una forma contenida en la clase C, i.e. si C = C, el valor opuesto —r evidentemente proviene de la representación por una forma contenida en la clase que es opuesta a C, y esta clase siempre sera diferente de C a menos que C sea ambigua. Se sigue que cuando no todas las clases en G son ambiguas, solamente la mitad de las restantes necesitan ser consideradas. Se puede omitir una de cada par de opuestos e inmediatamente

escribir ambos valores después de haber calculado solamente uno. Cuando C es ambigua, ambos valores r y —r emergerán al mismo tiempo; es decir, si tomamos la forma ambigua ax2 + 2bxy + cy2 de C y el valor r es producido por la representación x = m, y = n, el valor —r resultará de la representacion x = — m — , y = n.

1. Para el caso donde D = 1, existe unicamente una clase, de la cual podemos seleccionar la forma x2 + y2. Si el valor r resulta de la representacián x = m, y = n, resultará tambien de x = —m, y = —n; x = n, y = —m; x = —n, y = m y el opuesto, —r, resultara de x = m, y = —n; x = —m, y = n; x = n, y = m; x = —n, y = —m. Así de estas ocho representaciones que constituyen ánicamente una descomposicion, una es suficiente en tanto que asociemos el valor opuesto con el que resulta de nuestra investigacioán.
2. El valor de la expresion V—D (mod. M) al cual corresponde la repre­sentacián M = am2 + 2bmn + cn2 es, por artículo 155, μ(mb + nc) — v(ma + nb) o cualquier numero congruente a el segán M, donde los numeros μ y v satisfacen μ^. + vn = 1. Designando este valor por v, tendremos

mv = μ^.(^Α + nc) — v(M — mnb — n2c) ξ ^m + vn)(mb + nc) ξ mb + nc (mod. M)

Así, es claro que si v es un valor de la expresion mbr+nc (mod. M); similarmente se encuentra que es un valor de la expresion — ma+nb (mod. M). Estas formulas son muy a menudo preferidas a aquella de la cual fueron deducidas.

328.

Ejemplos. I. Busquense todos los valores de la expresion V —1365 (mod. 5428681 = M); el numero M es ξ 1, 1, 1, 6, 11 (mod. 4, 3, 5, 7, 13) y así esta contenido en una forma de los divisores de x2 + 1, x2 + 3, x2 — 5 y en una forma de los no divisores de x2 + 7, x2 — 13 y por lo tanto en una forma de los divisores de x2 + 1365; el carácter del genero en el cual se encontraran las clases G, es 1, 4; R3; R5; N7; N13. Existe solamente una clase contenida en este genero y de esta seleccionaremos la forma 6x2 +6xy+229y2. Para encontrar todas las representaciones del numero M por esta forma, ponemos 2x + y = x0 y tenemos 3x/2 + 455y2 = 2M. Esta ecuacion admite cuatro soluciones en las que y es positivo, a saber y = 127,

x' = ±1083, y = 119, x' = ±1213. De estas obtenemos cuatro soluciones de la ecuación 6x2 + 6xy + 229y2 = M en las que y es positivo,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| x | 478 | -605 | 547 | -666 |
| y | 127 | 127 | 119 | 119 |

La primera solución da para v el valor de la expresión 345g7 o (mod. M)

y encontramos que es 2350978; la segunda produce el valor opuesto -2350978; la tercera, el valor 2600262; y la cuarta, su opuesto -2600262.

1. Si queremos los valores de la expresión V-286 (mod. 4272943 = M), el carócter del genero en el que estan contenidas las clases G, seró 1 y 7, 8; R11; R13. Este seró por lo tanto el genero principal en el cual estan contenidas tres clases, representadas por las formas (1, 0, 286), (14, 6, 23) y (14, -6, 23). Se puede omitir la tercera de estas, ya que es opuesta a la segunda. Por la forma x2 + 286y2 encontramos dos representaciones del nuómero M en las que y es positivo, a saber, y = 103 , x = ±1113. De ellas deducimos estos valores para la expresión dada: 1493445 y -1493445. Encontramos que M no es representable por la forma (14, 6, 23) y concluimos que esos son los únicos valores.
2. Dada la expresión ^-70 (mod. 997331), las clases G deben estar contenidas en el genero cuyo carácter es 3 y 5, 8; R5; N7. Hay unicamente una clase y su forma representante es (5, 0,14). Despues de un calculo se encuentra que el numero 997331 no es representable por la forma (5, 0, 14) y así -70 sera necesariamente un no residuo cuadratico de ese numero.

Dos métodos para distinguir números compuestos de números primos  
y para determinar sus factores.

329.

El problema de distinguir numeros primos de numeros compuestos y de resolver estos ultimos en sus factores primos es conocido como uno de los mas importantes y utiles en aritmetica. Ha ocupado la industria y la sabiduría de geometras antiguos y modernos a tal grado que sería superfluo discutir el problema detenidamente. No obstante debemos admitir que todos los metodos que han sido propuestos hasta ahora son o restringidos a casos muy especiales o tan laboriosos y prolijos que aun para numeros que no exceden los límites de tablas construidas por hombres estimables, i.e., para numeros que no requieren metodos ingeniosos, ponen a prueba la paciencia hasta de los calculistas experimentados. Y estos metodos a duras

penas pueden ser usados para números grandes. Aún cuando las tablas, que están disponibles para quien quiera y las cuales esperamos continuaran siendo extendidas, son realmente suficientes para la mayoría de los casos ordinarios, frecuentemente sucede que el calculista entrenado obtendrá la suficiente ganancia de la reducción de numeros grandes a sus factores de modo que esto lo compensara por el tiempo consumido. Luego, la dignidad de la ciencia misma parece requerir que todos los medios posibles para la solucion de un problema tan elegante y tan celebre sean explorados. Por esta razon, no dudamos que los dos metodos siguientes, cuya eficacia y brevedad podemos confirmar a partir de una larga experiencia, resultaran gratificantes a los aficionados a la aritmetica. Esta en la naturaleza del problema que cualquier metodo se hará mas prolijo a medida que los numeros se hacen mayores. No obstante, en los siguientes metodos, las dificultades crecen algo lentamente, y números con siete, ocho o aun mas dígitos han sido manipulados con exito y rapidez mas alla de la esperada, especialmente por el segundo metodo. Las tecnicas que fueron previamente conocidas requerirían un trabajo intolerable aun para el calculista mas infatigable.

Antes de considerar los siguientes metodos, es siempre muy util tratar de dividir el numero dado por algunos de los primos mas pequeños, digamos por 2, 3, 5, 7, etc. hasta 19 o un poco mas alla, a fin de eludir el uso de metodos sutiles y artificiales cuando la sola division puede ser mas sencilla [[217]](#footnote-218)); y tambien, porque cuando la division no es exitosa, la aplicacion del segundo metodo utiliza con gran beneficio los residuos derivados de estas divisiones. Así, e.g., si el numero 314159265 se va a resolver en sus factores, la division por 3 es exitosa dos veces, y despues, las divisiones por 5 y por 7. Así tenemos 314159265 = 9 · 5 · 7 · 997331 y es suficiente examinar por medios mas sutiles el numero 997331, el cual no es divisible por 11,13,17 ni 19. Similarmente, dado el numero 43429448, podemos remover el factor 8 y aplicar los metodos mas sutiles al cociente 5428681.

330.

El fundamento del PRIMER METODO es el teorema que establece que cualquier número positivo o negativo que es un residuo cuadratico de otro número M, es también un residuo de cualquier divisor de M. Cualquiera sabe que si M no es divisible por ningun numero primo abajo de λ/M, M es de seguro primo; pero si todos

los números primos abajo de este límite que dividen a M son p, q, etc., el número M estú compuesto por estos solamente (o por sus potencias), o existe únicamente un factor primo mayor que y/M. Este se encuentra dividiendo M por p, q, etc. tantas veces como se pueda. Por lo tanto, si designamos el conjunto de todos los números primos abajo de y/M (excluyendo a aquellos que ya sabemos que no dividen al numero) por Ω, evidentemente sera suficiente encontrar todos los divisores de M contenidos en Ω. Ahora, si de alguna manera se constata que un numero r (no cuadrado) es un residuo cuadrático de M, de seguro ningun numero primo del cual r es un no residuo puede ser un divisor de M; por consiguiente se pueden remover de Ω todos los numeros primos de este tipo (ellos usualmente conformaran alrededor de la mitad de los numeros de Ω). Y si llega a ser claro que otro numero r' no cuadrado es un residuo de M, podemos excluir de los restantes numeros primos en Ω aquellos para los cuales r' es un no residuo. De nuevo reducimos estos numeros en casi la mitad, siempre y cuando los residuos r y r' sean independientes (i.e. a menos que uno de ellos sea necesariamente un residuo de todos los numeros de los cuales el otro es un residuo; esto sucede cuando rr' es un cuadrado). Si todavía conocemos otros residuos r'', r''', etc. de M, cada uno de ellos independiente de los restantes[[218]](#footnote-219)), podemos instituir exclusiones similares con cada uno de ellos. Así, la cantidad de números en Ω disminuirá rápidamente hasta que todos ellos sean removidos, en cuyo caso M sera ciertamente un numero primo, o quedaran tan pocos (obviamente todos los divisores primos de M apareceran entre ellos, si existe alguno) que la division por ellos puede ser probada sin demasiada dificultad. Para un numero que no excede un millon aproximadamente, usualmente seis o siete exclusiones seran suficientes; para un numero con ocho o nueve dígitos, de seguro serán suficientes nueve o diez exclusiones. Resta ahora hacer dos cosas, primero encontrar residuos apropiados de M y un numero suficiente de ellos, entonces efectuar la exclusion de la manera mas conveniente. Pero invertiremos el orden de las cuestiones porque lo segundo nos mostrara cuales residuos son los mas apropiados para este proposito.

331.

En la sección IV hemos mostrado detenidamente como distinguir numeros

primos para los cuales un r dado es un residuo (podemos suponer que no es divisible por un cuadrado) de aquellos para los cuales es un no residuo; es decir, como distinguir los divisores de la expresión x2 — r de los no divisores. Todos los divisores estan contenidos bajo fórmulas como rz + a, rz + b, etc. o como 4rz + a y 4rz + b, etc. y los otros bajo formulas semejantes. Siempre que r es un numero muy pequeño, con la ayuda de estas fórmulas podemos llevar a cabo las exclusiones satisfactoriamente; e.g. cuando r = —1 todos los nómeros de la forma 4z + 3 serán excluidos; cuando r = 2 se excluyen todos los numeros de las formas 8z + 3 y 8z + 5, etc. Pero puesto que no siempre es posible encontrar residuos como estos para un nómero M dado, y la aplicacion de las formulas no es muy conveniente cuando el valor de r es grande, se ganara mucho y el trabajo de exclusion se reducirá sobremanera si tenemos una tabla para una cantidad suficientemente grande de numeros (r) tanto positivos como negativos que no sean divisibles por cuadrados. La tabla deberá distinguir nómeros primos que tengan a cada uno (r) como residuo de aquellos para los cuales es un no residuo. Tal tabla puede ser arreglada del mismo modo que el ejemplo al final de este libro que ya hemos descrito arriba; pero a fin de que ella sea útil para nuestros propositos presentes, los numeros primos (modulos) en el margen deben ser continuados mucho mas lejos, a 1000 o 10000. Sería aun mas conveniente si los números compuestos y negativos tambien fueran listados hasta el tope, aunque esto no es absolutamente necesario, como es claro de la seccion IV. La maxima utilidad resultaría si las columnas verticales individuales fueran removibles y pudieran ser rearmadas sobre placas o varillas (como las de Napier). Entonces aquellos que son necesarios en cada caso, i.e. los que corresponden a r, r0, r", etc., los residuos de los numeros dados, pueden ser examinados separadamente. Si estos son colocados correctamente junto a la primera columna de la tabla (que contiene al modulo), i.e. de manera que la posicion en cada una de las varillas que corresponden al mismo numero en la primera columna es puesta en la línea horizontal correspondiente, aquellos nómeros primos que permanecen despues de las exclusiones de Ω correspondientes a los residuos r, r0, r00, etc. pueden ser inmediatamente reconocidos por inspeccion. Ellos son los numeros en la primera columna que tienen pequeñas ranuras en todas las varillas adyacentes. Un primo para el que alguna varilla tiene un espacio vacío debe ser desechado. Un ejemplo ilustrara esto suficientemente bien. Si de algun modo sabemos que los numeros —6, +13, —14, +17, +37, —53 son residuos de 997331, entonces acoplaríamos juntas la primera columna (la cual en este caso sería continuada hasta el numero 997, i.e. hasta el mayor numero primo menor que V997331) y las columnas que tengan como tope los numeros —6, +13, etc. He aquí

una sección de este esquema:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | -6 | + 13 | -14 | + 17 | +37 | -53 |
| 3  5  7  11  13  17 | — |  | — |  | — |  |
| 19  23 |  | — | etc. |  |  | — |
| 113  127  131 |  | — | — |  |  | — |
| — | — | — |  |  |  |
|  |  |  | etc. |  |  |  |

Así, por inspección, de aquellos primos contenidos en esta parte del esquema, se sabe que despues de todas las exclusiones con los residuos -6, 13, etc. ónicamente permanece en Ω el nómero 127. El esquema total extendido hasta el nómero 997 mostraría que no hay otro nómero en Ω. Cuando probamos esto, encontramos que 127 efectivamente divide a 997331. De esta manera encontramos que este nómero puede ser resuelto en los factores primos 127 · 7853[[219]](#footnote-220)).

De este ejemplo es suficientemente claro que aquellos residuos especialmente ótiles son los no demasiado grandes, o que al menos pueden ser descompuestos en factores primos que no son demasiado grandes. El uso directo de la tabla auxiliar no se extiende más alla de los nómeros a la cabeza de las columnas, y el uso indirecto sóolo incluye aquellos nuómeros que pueden ser resueltos en factores contenidos en la tabla.

332.

Daremos tres métodos para encontrar residuos de un número M dado, pero antes de explicar esto queremos hacer dos observaciones que nos ayudaran a determinar residuos maús simples cuando los que tenemos no son bastante idúoneos. Primero, si el número ak2 que es divisible por el cuadrado k2 (que es relativamente primo a M) es un residuo de M, a sera tambien un residuo. Por esta razón, residuos que son divisibles por cuadrados grandes son precisamente tan utiles como los residuos pequeños, y suponemos que todos los factores cuadrados se han eliminado de todos los residuos suministrados por los siguientes metodos. Segundo, si dos o mas números son residuos, su producto tambien sera un residuo. Combinando esta observaciún con la precedente, a menudo puede deducirse, de varios residuos que no son todos lo bastante simples, otro que es simple, con tal que los residuos tengan una gran cantidad de factores comunes. Por esta razon es muy útil tener residuos compuestos de muchos factores que no sean demasiado grandes, y todos ellos serían inmediatamente resueltos en sus factores. La fuerza de estas observaciones sera mejor entendida mediante ejemplos y el uso frecuente que mediante reglas.

1. El metodo mús simple y el mús conveniente, para aquellos que han adquirido alguna destreza a traves del ejercicio frecuente, consiste en descomponer M o mús generalmente un múltiplo de M en dos partes, kM = a + b (ambas partes pueden ser positivas o una positiva y la otra negativa). El producto de estas dos tomado con el signo opuesto sera un residuo de M; pues -ab = a2 = b2 (mod. M) y así -abRM. Los números a y b deben ser tomados de modo que su producto sea divisible por un cuadrado grande y su cociente sea pequenño o al menos resoluble en factores que no sean demasiado grandes, algo que siempre puede hacerse sin dificultad. Se recomienda especialmente que a sea un cuadrado o el doble de un cuadrado o el triple de un cuadrado, etc., el cual difiera de M por un nuúmero pequenño o al menos por un número que pueda ser resuelto en factores apropiados. Así, e.g., 997331 = 9992 - 2 · 5 · 67 = 9942 + 5· 11 · 132 = 2 · 7062 + 3· 17 · 32 =3 · 5752 + 11· 31 · 42 = 3· 5772 - 7· 13 ·42 = 3· 5782 - 7· 19·37 = 11 · 2992 + 2· 3· 5· 29·42 = 11 ·3012 + 5· 122 etc. Así tenemos los siguientes residuos: 2 · 5 · 67, -5 · 11, -2 · 3 · 17, -3 · 11 · 31, 3 · 7 · 13, 3 · 7 · 19 · 37, -2 · 3 · 5 · 11 · 29. La última descomposicion produce el residuo -5 · 11 el cual ya tenemos. Para los residuos -3 · 11 · 31, -2 · 3 · 5 · 11 · 29 podemos sustituir 3 · 5 · 31, 2 · 3 · 29 que resulta de su combinación con -5 · 11.
2. El segundo y tercer metodo se derivan del hecho que si dos formas binarias

(A, B, C) y (A', B', C') del mismo determinante M o — M o más generalmente ±kM pertenecen al mismo genero, los námeros AA', AC' y A'C son residuos de kM; esto no es difícil de ver ya que cualquier námero característico, digamos m, de una forma es tambien un numero característico de la otra, y asá mA, mC, mA' y mC' son todos residuos de kM. Si por consiguiente (a, b, a') es una forma reducida del determinante positivo M o del mas general kM, y (a', b', a''), (a00, b'', a'00), etc. son formas en su período, íestas serían equivalentes a ella y ciertamente contenidas en el mismo gíenero. Los námeros aa', aa'', aa'0', etc. serán todos residuos de M. Se puede computar un gran námero de formas en tal período con la ayuda del algoritmo del artículo 187. Ordinariamente los residuos mas simples resultan de poner a = 1 y se omiten aquellos que tengan factores que son demasiado grandes. Aquí esrán los inicios de los períodos de las formas (1, 998, —1327) y (1, 1412, —918) cuyos determinantes son 997331 y 1994662:

( 1, 998, —1327)

( 1,1412, —918)

( —918, 1342, 211)

( 211,1401, —151)

( —151,1317, 1723) ( 1723, 406,—1O62) (—1062, 656, 1473) ( 1473, 817, —901) ( —901, 985, 1137) etc.

(—1327,329, 67θ)

( 670, 341, —1315)

(—1315,974, 37)

( 37,987, —626)

( —626, 891, 325)

( 325, 734, —1411)

(—1411, 677, 382)

( 382,851, —715)

Por consiguiente todos los nímeros —1327, 670, etc. son residuos del nímero 997331; olvidando aquellos que tengan factores demasiado grandes, tenemos estos: 2 · 5 · 67, 37, 13, —17 · 83, —5 · 11 · 13, —2 · 3 · 17, —2 · 59, —17 · 53; hemos encontrado arriba el residuo 2 · 5 · 67 así como —5 · 11 que resulta de una combinación del tercero y el quinto.

1. Sea C cualquier clase, diferente de la clase principal, de formas de un determinante negativo —M o mas generalmente —kM y sea su período 2C, 3C, etc. (art. 307). Las clases 2C, 4C, etc. pertenecerán al genero principal; 3C, 5C, etc. al mismo genero que C. Si por consiguiente (a, b, c) es la (mís simple) forma en C y (a', b', c') una forma en alguna clase del período, digamos nC, o a' o aa' sera

un residuo de M segun que n sea par o impar (en el primer caso c' sera tambien un residuo, en el ultimo caso ac', ca' y cc' lo serín). El calculo del período, i.e. de las formas mas simples en sus clases, es sorprendentemente facil cuando a es muy pequeno, especialmente cuando es = 3, lo que es siempre permisible cuando

kM = 2 (mod. 3). He aquí el inicio del período de la clase que contiene a la forma (3, 1, 332444):

C ( 3, 1,332444) 2C ( 9,-2,110815) 3C ( 27, 7, 36940) 4C ( 81, 34, 12327) 5C (243, 34, 4109)

6C ( 729,-209,1428) 7C ( 476, 209, 2187) 8C (1027, 342, 1085) 9C ( 932, -437,1275) 10C ( 425, 12, 2347)

Despues de eliminar aquellos que no son Utiles, tenemos los residuos 3 · 476, 1027, 1085, 425 o (removiendo los factores cuadrados) 3 · 7 · 17, 13 · 79, 5 · 7 · 31, 17. Si combinamos juiciosamente estos con los ocho residuos encontrados en II se encuentran los doce siguientes, —2 · 3, 13, —2 · 7, 17, 37, -53, —5 · 11, 79, -83, —2 · 59, —2 · 5 · 31 y 2 · 5 · 67. Los seis primeros son los únicos que usamos en el artículo 331. Si queremos, podemos agregar los residuos 19 y —29, que encontramos en I; los otros incluidos allí son dependientes de los que hemos desarrollado aquú.

333.

El SEGUNDO METODO para resolver un número dado M en factores depende de una consideraciún de los valores de la expresión V — D (mod. M), junto con las siguientes observaciones.

1. Cuando M es un número primo o una potencia de un primo (impar y que no divide a D), — D sera un residuo o un no residuo de M de acuerdo con que M este contenido en una forma de los divisores o de los no divisores de x2 + D. En el primer caso la expresión V—D (mod. M) tendrá únicamente dos valores diferentes, que serúan opuestos.
2. Cuando M es compuesto, es decir, = pp/p//, etc., donde los números p, p0, p0/, etc. son primos (distintos, impares y que no dividen a D) o potencias de tales números: —D serú un residuo de M solamente cuando es un residuo de cada uno de los p, p0, p0/, etc., i.e. cuando todos estos numeros esrán contenidos en formas de los divisores de x2 + D. Designando los valores de la expresión V—D según los modulos p, p0, p0/, etc. respectivamente por ±r, ±r0, ±r0/, etc. aparecen todos los valores de la misma expresiún según el múdulo M al determinar los números que son = r o = —r segun p, aquellos que son = r0 o = —r' según p0, etc. Su numero serú = 2μ, donde μ es el numero de factores p, p0, p0/, etc. Ahora, si estos valores son R, —R, R0, — R0, R0/, etc., se ve inmediatamente que R = R según todos los numeros p, p0, p0/, etc.,

pero que según cualquiera de ellos no se tiene R =—R. Así M será el máximo común divisor de M y R — R, y 1 es el máximo común divisor de M y R + R; pero dos valores que no son ni identicos ni opuestos, e.g. R y R', deben ser congruentes según uno o varios de los numeros p, p', p", etc. pero no según todos ellos y segun los otros tendremos R = —R'. Así el producto de los primeros sera el maximo común divisor de los números M y R — R', y el producto de los ultimos serú el maximo común divisor de M y R + R'. Se sigue de esto que si encontramos todos los máximos comunes divisores de M con las diferencias entre los valores individuales de la expresión p—D (mod. M) y algún valor dado, su conjunto contendrá los números 1, p, p', p'', etc. y todos los productos de pares y triples, etc. de estos numeros. De esta forma, por lo tanto, podran determinarse los números p, p', p'', etc. de los valores de esa expresión.

Ahora, ya que el metodo del artículo 327 reduce estos valores a los valores de expresiones de la forma mn (mod. M) con el denominador n primo relativo a M, no es necesario, para nuestros propositos presentes, computarlos. El maximo común divisor del numero M y la diferencia entre R y R', que corresponden a mn y m, sera obviamente tambien el múximo común divisor de los números M y nn' (R — R'), o de M y mn' — m'n, ya que el ultimo es congruente a nn'(R — R') segun el modulo M.

334.

Podemos aplicar las observaciones precedentes a nuestro problema de dos maneras; la primera no solo decide si el número dado M es primo o compuesto, sino que en el segundo caso da sus factores; la segunda es superior en tanto que ella permite cúlculos mús rápidos, pero, a menos que se repita una y otra vez, no produce los factores de los nuúmeros compuestos, sin embargo los distingue de los nuúmeros primos.

I. Se busca primero un número negativo —D que sea un residuo cuadrático de M; para este fin se pueden usar los metodos dados en I y II del artículo 332. En sí, la selección del residuo es arbitraria, ni hay aquí como en el metodo precedente ninguna necesidad de que D sea un número pequeño. Pero el calculo serú mús corto a medida que el número de clases de formas binarias contenidas en cada genero propiamente primitivo del determinante —D sea mús pequeno. Por consiguiente serú conveniente tomar residuos que esten contenidos entre los 65 enumerados en el artículo 303 si alguno de estos se halla allí. Así, para M = 997331 el residuo —102 serú el mús idoneo de todos los residuos negativos dados arriba. Aparecen todos los valores diferentes de la expresión p—D (mod. M). Si hay solamente dos (opuestos),

M será de seguro un número primo o una potencia de un primo; si hay varios, digamos 2μ, M estarú compuesto de μ números primos o potencias de primos y estos factores pueden ser encontrados por el metodo del artículo precedente. Estos factores, ya sean primos o potencias de primos, pueden ser determinados directamente, pero la manera como se encuentran los valores de la expresión p—D indicarú todos los primos cuyas potencias dividen a M. Puesto que si M es divisible por el cuadrado de un numero primo π, el calculo de seguro producirá una o mas representaciones del número M = am2 + 2bmn + cn2, en las que el maximo común divisor de los números m y n es π (porque en este caso —D es tambien un residuo de Mf). Pero cuando no existen representaciones en las cuales m y n tengan un divisor común, esta es una indicacion confiable de que M no es divisible por un cuadrado, y así todos los números p, p', p", etc. son números primos.

Ejemplo. Por el metodo dado antes se encuentra que existen cuatro valores de la expresion p—408 (mod. 997331) que coinciden con los valores de las expresiones ±1664 y ±; los maximos comunes divisores de 997331 con 3 · 1664 — 113 · 2824 y 3 · 1664 + 113 · 2824 o con 314120 y 324104 son 7853 y 127, así 997331 = 127 · 7853 como antes.

II. Tómese un número negativo —D tal que M esta contenido en una forma de los divisores de x2+D; en sí es arbitrario que numero de este tipo se selecciona, pero es ventajoso tener el numero de clases en el genero del determinante —D tan pequeno como sea posible. No existe dificultad en encontrar un tal numero; puesto que entre cualquier cantidad de numeros probados aproximadamente existen tantos para los que M esta contenido en una forma de los divisores como existen para los cuales M esta contenido en una forma de los no divisores. Por consiguiente sera conveniente comenzar con los 65 numeros del artículo 303 (comenzando con los mas grandes) y si sucede que ninguno de estos es idoneo (en general esto sucederá solamente una vez en 16384 casos), podemos pasar a otros en los cuales solamente hay dos clases contenidas en cada genero. Entonces se investigaran los valores de la expresion p —D (mod. M) y si alguno se encuentra, los factores de M pueden ser deducidos de el, del mismo modo que antes; pero si no se obtienen valores, es decir, si —D es un no residuo de M, ciertamente M no sera numero primo ni potencia de un numero primo. Si en este caso se desean los factores mismos, habremos de repetir la misma operacion, usando otro valor para D o ensayando otro metodo.

Así, e.g., se encuentra que 997331 esta contenido en una forma de los no divisores de x2 + 1848, x2 + 1365, x2 + 1320 pero esta contenido en una forma de

los divisores de x- + 840; para los valores de la expresión V-840 (mod. 997331) se encuentran las expresiones ± -=-7- y ± 3--- y de estos deducimos los mismos factores que antes. Para mas ejemplos consulte los del artículo 328, que muestran primero que 5428681 = 307 · 17863; segundo que 4272943 es un numero primo; tercero, que 997331 esta ciertamente compuesto de mas de un numero primo.

Los límites del presente trabajo nos permite insertar aquí unicamente los principios basicos de cada metodo de hallazgo de factores; guardaremos para otra ocasión una discusión mas detallada, junto con tablas auxiliares y otras ayudas.

Sección Sétima

ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

335.

Dentro de los espléndidos desarrollos, contribución de los matemáticos modernos, la teoría de las funciones circulares sin duda ocupa uno de los lugares más importantes. A menudo tenemos ocasión, en una variedad de contextos, de referirnos a este notable tipo de cantidad, y no hay parte de la matemótica general que no dependa de ella en alguna forma. Ya que los mós brillantes matematicos modernos por su industria y sagacidad la han erigido en una extensiva disciplina, se esperaría firmemente que cualquier parte de la teoría, por no hablar de una parte elemental, debería haber sido significativamente desarrollada. Me refiero a la teoría de funciones trigonometricas correspondientes a arcos que son conmesurables con la circunferencia, i.e., la teoría de polígonos regulares. Solamente una pequeña parte de esta teoría ha sido desarrollada hasta ahora, como la siguiente secciín aclarará. Los lectores podrían sorprenderse de encontrar una discusion de este tema en el presente trabajo, el cual trata con una disciplina aparentemente tan diferente; pero el tratamiento mismo hará abundantemente claro que hay una conexion íntima entre este tema y la Aritmíetica Superior.

Los principios de la teoría que vamos a explicar de hecho se extienden mucho mas allí de lo que indicaremos. Por ello, pueden ser aplicados no solamente a funciones circulares sino tambien a otras funciones trascedentales, e.g., a aquellas que dependen de la integral / 4 y tambien a varios tipos de congruencias. Ya que, sin

embargo, estamos preparando un gran trabajo sobre esas funciones trascendentales

y puesto que trataremos congruencias extensamente en la continuación de estas Disquisitiones, hemos decidido considerar aquí solamente funciones circulares. Y aún cuando es posible discutirlas en toda su generalidad, la reduciremos al caso mas simple en el artículo siguiente, tanto por motivos de brevedad como porque los nuevos principios de esta teoría puedan ser mas fúcilmente comprendidos.

La discusión se reduce al caso más simple, donde el número de partes  
en las cuales se corta el círculo es un número primo.

336.

Designando la circunferencia del círculo o cuatro úngulos rectos por P y suponiendo que m y n son enteros y n un producto de los factores relativamente primos a, b, c, etc., el úngulo A = pp puede ser reducido por los metodos del artículo 310 a la forma A = (p + β + γΥ + etc.)P, y las funciones trigonometricas correspondientes a el pueden ser encontradas por metodos conocidos a partir de los de las partes pp, pp, etc. De esta forma, ya que se pueden tomar a, b, c, etc. como números primos o potencias de numeros primos, es suficiente considerar la division del círculo en partes cuyo numero es un primo o una potencia de un primo y se obtendrá inmediatamente un polígono de n lados a partir de los polígonos de a, b, c, etc. lados. Sin embargo, restringiremos nuestra discusion al caso en que el círculo es dividido en un numero primo (impar) de partes, especialmente por la siguiente razon. Es claro que las funciones circulares correspondientes al angulo ^2“ son deducidas de las funciones pertenecientes a ^p mediante la solucion de una ecuacion de grado p. Y de este, por una ecuacion del mismo grado podemos derivar las funciones correspondientes a ^3“ etc. De esta forma, si ya se tiene un polígono de p lados, para determinar un polígono de ρλ lados necesariamente se requerirá la solucion de λ — 1 ecuaciones de grado p. Aun cuando la siguiente teoría puede ser extendida tambien a este caso, no obstante no podremos evitar tantas ecuaciones de grado p, y no existe manera de reducir su grado si p es primo. Así, e.g., se mostrara abajo que un polígono de 17 lados puede ser contruido geometricamente; pero para obtener un polígono de 289 lados no hay manera de eludir el resolver una ecuacion de grado 17.

Ecuaciones para funciones trigonométricas de arcos que son una parte o partes

de la circunferencia completa,

reducción de las funciones trigonométricas a las raéces de la ecuación xn — 1 = 0.

337.

Es bien conocido que las funciones trigonométricas de todos los ángulos ^ donde la k denota en general todos los números 0, 1, 2, ...n — 1, son expresadas por las raíces de ecuaciones de grado n. Los senos son las raíces de la ecuación (I):

n 1 n\_2 1 n(n 3) n\_4

xn nx 2 + ^xn 4

4 16 1-2

1 n(n — 4)(n 64 1-2-3

5)xn 6 + etc. ± rrnx

2n-1

0

los cosenos son las raíces de la ecuacion (II):

1 o 1 n(n — 3) n-4 1 n(n — 4)(n — 5) n-6

xn nxn

4

+

-xn- ---

16 1 · 2 64 1 · 2 · 3

y las tangentes son las raíces de la ecuacion (III):

x

11 + etc. ± nx —

2n

1

2n

1

= 0

n n(n — 1) n 2 n(n — 1)(n — 2)(n — 3) n 4

xn v, , ’ xn-2 + Axn~- etc. ± nx = 0

12

1234

Estas ecuaciones (que son todas verdaderas para cualquier valor impar de n, y la ecuaciún II es cierta tambien para cualquier valor par), poniendo n = 2m + 1, pueden ser fúcilmente reducidas a grado m. Para I y III esto justamente requiere dividir a la izquierda por x y sustituir x2 por y. De todas formas la ecuacion II incluye la raíz x = 1 (= cos 0) y todas las otras son iguales en pares (cos P = cos (n n1)P, cos = cos (n n°)P, etc.); así el lado izquierdo es divisible por x — 1 y el cociente sera un cuadrado. Si extraemos la raíz cuadrada, la ecuaciún II se reduce a la siguiente:

xm + 1 xm-1 — ^(m — 1)xm-2 — ^(m — 2)xm-3 2 4V ; 8v

. 1 (m — 2)(m — 3) xm-4 , 1 (m — 3)(m — 4) xm-5

etc. = 0

+ 16 1-2 +32 1-2

Sus raíces serón los cosenos de los angulos P, —, —, ... . Hasta ahora no se ha

n n n n

hecho ninguna reducciín mas alla de estas ecuaciones para el caso en que n es un nímero primo.

No obstante, ninguna de estas ecuaciones es tan tratable y tan conveniente para nuestros propositos como xn — 1 = 0. Sus raíces están íntimamente relacionadas

con las raíces de las anteriores. Esto es, escribiendo por brevedad i para la cantidad imaginaria y/ — 1, las raíces de la ecuación xn — 1 = 0 serán

*kP . kP*

cos + i sen = r

*n n*

donde para k se debe tomar todos los números 0, 1, 2, ...n — 1. De esta forma, ya

que

1 *kP kP λ ' λ* i w T *' 1 ( 1\*

- = cos i sen—, las raíces de la ecuacion I seran ó-(r ) o i

*r n n ) r'*

*: 1—r*

2

las

raíces de la ecuaciún II, 1 (r + 1) = ; finalmente las raíces de la ecuacion III,

^ ^. Por esta razon construiremos nuestra investigacion sobre una consideracion de la ecuaciún xn — 1 = 0, asumiendo que n es un número primo impar. Con el fin de no interrumpir el orden de la investigaciíon, consideraremos primero el siguiente lema.

338.

PROBLEMA. Dada la ecuación

(W) ...zm + Azm-1 + etc. = 0

encontrar la ecuación (W0) cuyas raíces son las λ-ésimas potencias de las raíces de la ecuación (W), donde λ es un exponente entero positivo dado.

Solución. Si designamos las raíces de la ecuacion W por a, b, c, etc., las raíces de la ecuacion W0 serán αλ, b\ c\ etc. Por un teorema de Newton muy conocido, de los coeficientes de la ecuacion W se puede encontrar la suma de cualquier potencia de las raíces a, b, c, etc. Por consiguiente, se buscan las sumas

αλ + bA + cA + etc., α2λ + b2A + c2A + etc. etc. hasta amA + bmA + cmA + etc.

y por un procedimiento inverso, de acuerdo con el mismo teorema, pueden ser deducidos los coeficientes de la ecuaciín W0, Q. E. F. Al mismo tiempo, es claro que si todos los coeficientes de W son racionales, todos los de W0 tambien lo serán. Por otro metodo se puede probar que si todos los primeros son enteros, los ultimos tambien serín enteros. No gastaremos mís tiempo sobre este teorema aquí, puesto que no es necesario para nuestro propíosito.

339.

La ecuación xn — 1 = 0 (siempre con la suposición que n es un número primo impar) tiene solamente una raíz real, x = 1; las restantes n — 1 raíces que estan dadas por la ecuación

xn-1 + xn-2 + etc. + x +1=0

son todas imaginarias ; denotaremos su conjunto por Ω y la función

xn-1 + xn-2 + etc. + x + 1 por X

Si por consiguiente r es cualquier raíz en Ω, resulta 1 = rn = r2n etc. y en general ren = 1 para cualquier valor entero positivo o negativo de e. Así, si λ y μ son enteros congruentes según n, tendremos r^ = r+ Pero si λ y μ son no congruentes segun n, entonces r^ y r^ serán diferentes, pues en este caso se puede encontrar un entero ν tal que (λ — μ)ν ξ 1 (mod. n), así ^λ-μ)ν = r y ciertamente γ·λ-μ no es = 1. Es claro que cualquier potencia de r es tambien una raíz de la ecuación xn — 1 = 0. Por lo tanto, ya que las cantidades 1(= r0), r, r2, ...rn-1 son todas diferentes, ellas nos darún todas las raíces de la ecuacion xn — 1 = 0 y así los números r, r2, r3, ...rn-1 coincidirán con Ω. Mas generalmente, entonces, Ω coincidirá con re, r2e, r3e, . ..r(n-1)e, si e es cualquier entero positivo o negativo no divisible por n. Tenemos por lo tanto

X = (x — re)(x

r2e)(x — r3e) ...(x — r(n-1)e)

re + r2e + r3e + ... + r(n-1)e = —1

y de esto

y

1 + re + r2e + ... + r(n-1)e = 0

Si tenemos dos raíces como r y 1 (= rn-1) o en general re y r-e, las llamaremos raíces reciprocas. Evidentemente el producto de dos factores simples x — r y x — 1 es real y es = x2 — 2x cos ω + 1, donde el angulo ω es igual al angulo P o a algín multiplo de el.

340.

Por eso, representando una raíz en Ω por r, todas las raíces de la ecuacion xn — 1 = 0 se expresan mediante potencias de r y el producto de varias raíces de esta

ecuación puede ser expresado por Γλ de manera que λ es 0 o positivo y < n. Por lo tanto, si φ(ί, u,v,. . .) designa una función algebraica racional entera de las incógnitas t, u, v, etc., que es una suma de terminos de la forma htaUvY ..., evidentemente si sustituimos t, u, v, etc. por las raíces de la ecuacion χη — 1 = 0, digamos t = a, u = b, v = c, etc., entonces φ(α, b,c,. . .) puede ser reducido a la forma

A + A'r + A00r2 + A'"r3 + ■■■ + Av rn-1

de tal manera que los coeficientes A, A0, etc. (algunos de ellos pueden no aparecer y por lo tanto son = 0) son cantidades determinadas. Y todos estos coeficientes serán enteros si todos los coeficientes en ^>(t,u, v,. . .), i.e., todos los h, son enteros. Si despues de esto sustituimos t, u, v ... , por a2, b2, c2, ... , respectivamente, cada termino htauβvY ... que ha sido reducido a ru se hace ahora r2a y asó:

222

φ(α ,b ,c ,

..) = A + A'r2 + A00r4 + A000r6 + + Av r

2n2

y en general para cualquier valor entero de λ,

φ(αλ^λ,^,...) = A + A0rx + A00r2X + ■■■ + Av r(n-1)A

Esta proposicion es muy importante y es fundamental para la discusion siguiente. Tambien se sigue de ello que

φ (1, 1,1,..·) = φ(αη^η^η,...) = A + A0 + A00 + ■■■ + Av

y

φ(α, b, c,...) + φ(α2^2,^,

. •) +

) + ... + φ(αη^η,^,...) = nA

De aquí, esta suma es entera y divisible por n cuando todos los coeficientes en <^>(t, u, v,. ..) son enteros.

Teoria de las raíces de la ecuación χη — 1 = 0 (donde n es primo).  
Omitiendo la raíz 1, las restantes (Ω) estan en X = χη-1 + χη-2+ etc. +x + 1 = 0.  
La funcion X no se puede descomponer en factores con coeficientes racionales.

341.

TEOREMA. Si la función X es divisible por la función de grado más pequeño P = χλ + AxA-1 + Βχλ-2 + ■■■ + Kx + L

los coeficientes A, B, ...L no pueden ser todos racionales.

Demostración. Sea X = PQ y P el conjunto de las raíces de la ecuación P = 0, Q el conjunto de las raíces de la ecuación Q = 0, así que Ω consiste de P y Q tomados juntos. Ademas, sea R el conjunto de raíces recíprocas de P, & el conjunto de raíces recíprocas de Q y sean las raíces que estan contenidas en R, raíces de la ecuacion R = 0 (esto se convierte en χλ + Lχλ— + etc. + LLx + L = 0) y sean aquellas que estan contenidas en & , raíces de la ecuacion S = 0. Evidentemente si tomamos las raíces R y & juntas obtenemos el conjunto Ω y RS = X. Ahora, distinguimos cuatro casos.

1. Cuando P coincide con R y consecuentemente P = R. En este caso obviamente pares de raíces en P serán siempre recíprocas y así P sera el producto de ^ λ factores dobles de la forma x2 — 2x cos ω + 1. Como este factor = (x — cos ω)2 + sen ω2, es claro que para cualquier valor real de x, P tiene necesariamente un valor real positivo. Sean P' = 0, P" = 0, P'" = 0, . ..Pv = 0 las ecuaciones cuyas raíces son las potencias cuadradas, cubicas, cuartas, ... (n — 1)- esimas de las raíces de P respectivamente, y sean p, p', p'', . ..pv los valores de las funciones P, P', P'', . ..Pv, respectivamente, que se obtienen al hacer x = 1. Entonces, por lo que se dijo antes, p sera una cantidad positiva, y por una razon similar tambien serán positivos p', p'', etc. Ya que, por consiguiente, p es el valor de la funcion (1 — t)(1 — u)(1 — v) etc., que es obtenida sustituyendo t, u, v, etc. por las raíces contenidas en P; p' es el valor de la misma funcion obtenida al sustituir t, u, v, etc., por los cuadrados de esas raíces; y 0 es su valor cuando t = 1, u =1, v = 1, etc.: la suma p + p' + p'' ··· + pv sera un entero divisible por n. Ademas es facil ver que el producto PP'P''... sera = Xλ y as í pp'p''... = ηλ.

Ahora, si todos los coeficientes en P fueran racionales, todos aquellos en P', P'', etc. tambien lo serían, por el artículo 338. Sin embargo, por el artículo 42, todos esos coeficientes tendr ían que ser enteros. Así p, p', p'', etc. tambien deberán ser enteros; como su producto es ηλ y su numero es n — 1 > λ, algunos de ellos (al menos n — 1 — λ) deben ser = 1, y los otros iguales a n o a una potencia de n. Y si g de ellos son = 1, la suma p + p' + etc. sera ξ g (mod. n) y as í, de seguro, no divisible por n. As í, nuestra suposicion es inconsistente.

1. Cuando P y R no coinciden pero contienen algunas raíces comunes, sea T este conjunto y T = 0, la ecuacion de la cual ellos son las raíces. Entonces T sera el maximo comun divisor de las funciones P y R (como es claro de la teoría de las ecuaciones). Sin embargo, pares de raíces en T serán recíprocas y como fue demostrado antes, no todos los coeficientes en T pueden ser racionales. Pero esto de seguro sucedería si todos los de P, y así tambien los de R, fueran racionales, como

resulta de la naturaleza de la operación por medio de la cual encontramos el máximo común divisor. Así, nuestra suposicián es absurda.

1. Cuando Q y & coinciden o tienen raíces comunes, se prueba, exacta­mente de la misma forma, que no todos los coeficientes de Q son racionales; pero ellos serían racionales si todos los de P fueran racionales, y esto es imposible.
2. Si P no tiene raíces en comun con R y Q ninguna en común con &, todas las raíces P deberían encontrarse necesariamente en &, y todas las raíces Q en R. Por lo tanto P = S y Q = R, y así X = PQ serí el producto de P por R; i.e.,

de χλ + Αχλ-1 ■■■ + Kx + L por χλ + —χλ-1 ■ ■■ + —x + —

L L L

Así, haciendo x = 1, resulta

nL = (1 + A... + K + L)2

Ahora, si todos los coeficientes en P fueran racionales, y así por el artículo 42 tambien enteros, L, el cual debe dividir al ultimo coeficiente en X, i.e., la unidad, sera necesariamente = ±1 y así ±n sería un cuadrado. Pero ya que esto es contrario a la hipotesis, la suposicion es inconsistente.

Entonces, por este teorema es claro que no importa como se factorice X, algunos de los coeficientes, al menos, serían irracionales, y así, no se pueden determinar excepto mediante una ecuaciín de grado mayor que la unidad.

*Declaración del propósito de las investigaciones siguientes.*

342.

No serí inutil declarar en pocas palabras el proposito de las investigaciones siguientes. Es resolver gradualmente la X en mas y mas factores, de manera que sus coeficientes sean determinados por ecuaciones de un orden tan pequeño como sea posible, hasta llegar finalmente a factores simples o sea a las raíces Ω. Probaremos que si el nímero n — 1 es resuelto de alguna manera en factores enteros α, β, γ, etc. (se puede asumir cada uno de ellos primo), X se puede resolver en α factores de grado n—- con coeficientes determinados por una ecuacion de grado α; cada uno de estos serí resuelto en otros β de grado n-- con la ayuda de una ecuaciín de grado β etc. Así, si ν designa el nímero de factores α, β, γ, etc., la determinaciín de las raíces Ω se reduce a la solucion de ν ecuaciones de grados α, β, γ, etc. Por ejemplo, para

n = 17, donde n — 1 = 2 · 2 · 2 · 2, habrá que resolver cuatro ecuaciones cuadráticas; para n = 73, tres ecuaciones cuadráticas y dos cábicas.

En lo que sigue a menudo hay que considerar potencias de la raíz r cuyos exponentes son tambien potencias: expresiones de esta clase son muy difíciles

de imprimir. Por lo tanto, para facilitar la tipografía utilizaremos la siguiente abreviación. Para r, r2, r3, etc. escribiremos [1], [2], [3], etc. y en general para r\ donde λ es cualquier entero, escribiremos [λ]. Tales expresiones no estan

completamente determinadas, pero lo estarán tan pronto como tomemos una raíz específica de Ω para r o sea para [1]. En general [λ] y [μ] serán iguales o diferentes de acuerdo con que λ y μ sean congruentes o no congruentes segun el modulo n. Ademas [0] = 1; [λ] · [μ] = [λ + μ]; [λ]ν = [λν]; la suma [0] + [λ] + [2λ] ... + [(n — 1)λ] es 0 o n de acuerdo con que λ sea no divisible o divisible por n.

Todas las raíces de Ω se distribuyen en ciertas clases (períodos).

343.

Si, para el modulo n, g es ese tipo de numero que en la seccion III llamamos una raíz primitiva, los n — 1 numeros 1, g, g2, . ..gn-2 serán congruentes a los numeros 1, 2, 3, ...n — 1 segun el modulo n. El orden sera diferente, pero todo numero en una serie sera congruente a alguno en la otra. De esto se sigue inmediatamente que las raíces [1L [gL [g2L ...[gn 2] coinciden con Ω. Por un argumento similar las raíces

[λ], [Ag], [Ag2], ... [λϊ"-2]

coincidirán con Ω cuando λ es cualquier entero no divisible por n. Además, ya que gn-1 = 1 (mod. n), es facil ver que las dos raíces ^g^] y ^gv] serán identicas o diferentes de acuerdo con que μ y v sean congruentes o no congruentes segán n — 1.

Si por lo tanto G es otra raáz primitiva, las raáces [1], [g], ... [gn-2] tambien coincidiráan con [1], [G], ... [Gn-2], exceptuando el orden. Además, si e es un divisor de n — 1, y se pone n — 1 = ef, ge = h, Ge = H, entonces los f números 1, h, h2, ...hf-1 serán congruentes a 1, H, H2, ...Hf 1 segun n (sin considerar el orden). Supongamos que G = gu (mod. n), que μ es un námero positivo arbitrario < f y que v es el residuo más pequeño de μω (mod. f). Entonces resultará ve = μ^ (mod. n — 1) y asá gve = g^we = G^e (mod. n) o Hμ = hv; i.e., cualquier námero en la segunda serie 1, H, H2, etc. sera congruente a un námero en la serie 1, h, h2, ...

y viceversa. Así, las f raíces [1], [h], [h2], ... [hf [[220]](#footnote-221)] serán idénticas con [1], [H], [H2], ... [Hf-1]. De la misma manera, es facil ver que las series mas generales

[λ], [Ah], [Ah2],... [Ah/-1] y [λ], [AH], [AH2],... [AHf-1]

coinciden. Designaremos la suma de tales f raíces, [A] + [Ah] + etc. + [Ahf-1] por (f, A). Puesto que ella no cambia al tomar una raíz primitiva diferente g, debe ser considerada como independiente de g. Llamaremos al conjunto de las mismas raíces el período (f, A) y olvidaremos el orden de las raíces \*). Para exhibir un tal período sera conveniente reducir cada raíz a su expresiín mís simple, esto es, sustituir los nímeros A, Ah, Ah2, etc. por sus residuos mas pequeños segín el modulo n. Se podrían ordenar los terminos de acuerdo con los tamaños de estos residuos.

Por ejemplo, para n = 19, 2 es una raíz primitiva y su período (6,1) consiste de las raíces [1], [8], [64], [512], [4096] y [32768] o sea [1], [7], [8], [11], [12] y [18]. Similarmente, el período (6,2) consiste de las raíces [2], [3], [5], [14], [16] y [17]. El período (6,3) es identico con el precedente. El período (6,4) contiene las raíces [4], [6], [9], [10], [13] y [15].

*Varios teoremas concernientes a estos períodos.*

344.

Se ofrecen inmediatamente las siguientes observaciones acerca de períodos de este tipo.

1. Ya que Ahf ξ A, Ah/+1 ξ Ah, etc. (mod. n), es claro que (f, A), (f, Ah), (f, Ah2), etc. estan compuestos por las mismas raíces. En general, por consiguiente, si designamos por [A0] cualquier raíz en (f,A), este período serí completamente identico a (f, A0). Si por lo tanto dos períodos que tienen el mismo nímero de raíces (los llamaremos similares) tienen una raíz en común, ellos serín identicos. Por lo tanto no puede ocurrir que dos raíces esten contenidas juntas en un período y solamente una de ellas se encuentre en otro período similar. Ademas, si dos raíces [A] y [A0] pertenecen al mismo período de f terminos, el valor de la expresión ^ (mod. n) es congruente a alguna potencia de h; esto es, podemos asumir que A0 ξ Agve (mod. n).
2. Si f = n — 1, e = 1, el período (f, 1) coincidira con Ω. En los casos restantes Ω estarí compuesto por los períodos (f, 1), (f, g), (f, g2), ... (f,ge-1). Por

lo tanto estos períodos serán completamente diferentes unos de otros y es claro que cualquier otro período similar (f, λ) coincidirá con uno de estos si [λ] pertenece a Ω, i.e., si λ no es divisible por n. El período (f, 0) o (f, kn) esta evidentemente compuesto de f unidades. Tambien es claro que si λ es cualquier numero no divisible por n, el conjunto de e períodos (f, λ), (f, λ$), (f, λ^2), ... (f, λ^6-1) tambien coincidirá con Ω. Así, e.g., para n = 19, f = 6, Ω consistirá de los tres períodos (6,1), (6,2) y (6,4). Cualquiera otro período similar, excepto (6,0), puede ser reducido a uno de estos.

1. Si n — 1 es el producto de tres nímeros positivos a, b y c, es evidente que cualquier período de bc terminos esta compuesto de b períodos de c terminos; por ejemplo (bc, λ) esta compuesto por (c, λ), (c, λ$β), (c, λ$2β) ... (c, λ$βδ-β). Estos ultimos se dicen estar contenidos en los primeros. Así para n = 19 el período (6,1) consiste de los tres períodos (2,1), (2,8) y (2,7). El primero contiene las raíces r y r18; el segundo r8 y r11; el tercero r7 y r12.

345.

TEOREMA. *Sean* (f, λ) *y* (f, μ) *dos periodos similares, idénticos o diferentes,* (f, λ) *consistiendo de las raíces* [λ], [λ0], [λ00], *etc. Entonces el producto de* (f, λ) *por*

(f, μ) *será la suma de* f *períodos similares, a saber*

= (X λ + μ) + (Λ λ' + μ) + (Λ λ00 + μ) + etc. = W

Demostracián. Sea como antes n — 1 = ef; g una raíz primitiva para el modulo n y h = ge. De lo que hemos dicho antes, tenemos (f, λ) = (f, λΛ) = (f, λΛ2) etc. El producto buscado sería

= [μ] · (f, λ) + [μΛ] · (f, λΛ) + [μΛ2] · (f, λΛ2) + etc.

y así

= [λ + μ] +[λΛ + μ] ··· +[λΛ/ 1 + μ]

+ [λΛ + μΛ] +[λΛ2 + μΛ] · · · +[λΛ^ + μΛ]

+ [λΛ2 + μΛ2] +[λΛ3 + μΛ2] · · · +[λΛ/+1 + μΛ2] etc.

una expresiín que contendrá en conjunto f2 raíces. Y si se suman las columnas verticales juntas, resulta

(Λ λ + μ) + (Λ λΛ + μ) + ··· + (Λ λΛ^ 1 + μ)

una expresión que coincide con W, porque por hipótesis los números λ, λ0, λ00, etc. son congruentes a λ, λΚ, λΚ2, . ..λΚ-1 según el modulo n (aquí no estamos interesados en el orden) y así tambien

λ + μ, λ + μ, λ + μ, etc.

serán congruentes a

λ + μ, λΚ + μ, λΚ2 + μ, ... λΚ/ 1 + μ Q. E. D.

Agregamos los siguientes corolarios a este teorema:

1. Si k designa cualquier entero, el producto de (f, &λ) por (f, &μ) sera

= (f, k(λ + μ)) + (/) k(λ0 + μ)) + (/) k(λ00 + μ)) + etc.

1. Ya que los terminos particulares de W coinciden con la suma (f, 0) la cual = f, o con una de las sumas (f, 1), (f, g), (f, g2) ... (f, ge-1), W puede ser reducido a la siguiente forma

W = of + b(f, 1) + í/(f, g) + b00(f, g2) + ··· + be(/. ge-1)

donde los coeficientes a, b, b0, etc. son enteros positivos (o alguno puede aún ser = 0). Es tambien claro que el producto de (f, ^) por (f, kμ) entonces se convertiró en

= af + b(f, k) + b0(f, kg) + ··· + be(f, kge-1)

Así, e.g., para n = 19 el producto de la suma (6, 1) por ella misma, o sea el cuadrado de esta suma, sera = (6, 2) + (6, 8) + (6, 9) + (6,12) + (6,13) + (6,19) = 6 + 2(6,1) + (6, 2) + 2(6,4).

1. Puesto que el producto de los terminos individuales de W por un período similar (f, v) puede ser reducido a una forma analoga, es evidente que el producto de tres períodos (f, λ) · (f, μ) · (f, v) puede ser representado por cf + d(f, 1) ... + de(f, ge-1) y los coeficientes c, d, etc. serán enteros y positivos (o = 0) y para cualquier valor entero de k tenemos

(f, ^) · (f, kμ) · (f, kv) = cf + d(f, k) + d0(f, kg) + etc.

Este teorema puede ser extendido al producto de cualquier número de períodos similares, y no importa si estos períodos son todos diferentes o parcialmente o totalmente idúnticos.

1. Se sigue de esto que si en cualquier funciún algebraica racional entera F = ^>(t, u, v,. ..) sustituimos las incognitas t, u, v, etc. por los períodos similares (f, λ), (f, μ), (f, v), etc. respectivamente, su valor serú reducible a la forma

A + B(f, 1) + B'(f. g) + B"(f, g2)... + B‘(f. ge-1)

y los coeficientes A, B, B', etc. serán enteros si todos los coeficientes en F son enteros. Pero si despues sustituimos t, u, v, etc. por (f, kX), (f, kμ), (f, kv), etc. respectivamente, el valor de F sera reducido a A + B(f, k) + B'(f, kg) + etc.

346.

TEOREMA. Suponiendo que λ es un número no divisible por n, y escribiendo por brevedad p en lugar de *(f,X),* cualquier otro período similar (f, μ), en el cual μ no es divisible por n, puede ser reducido a la forma

α + βρ + γρ2 + ··· + £pe-1

donde los coeficientes α, β, etc. son cantidades racionales determinadas.

Demostración. Desígnense por p', p", p"', etc. los períodos (f, Xg), (f, Xg2), (f, Xg3), etc. hasta (f, Xge-1). Su número serú e — 1 y uno de ellos necesariamente coincidirú con (f^). Inmediatamente resulta la ecuación

0 = 1 + p + p' + p'' + p'00 + etc. (I)

Ahora, si de acuerdo con las reglas del artúculo precedente se desarrollan las potencias de p hasta la e — 1-esima, se extenderún otras e — 2 ecuaciones

0 = p2 + A + ap + a'p' + a''p'' + a'''p'0' + etc. (II)

0 = p3 + B + bp + b'p' + b''p'' + b'''p''' + etc. (///)

0 = p4 + C + cp + c'p' + c''p'' + c'''p''' + etc. (IV)

etc.

Todos los coeficientes A, a, a0, etc.; B, b, b', etc.; etc. serán enteros y, como sigue inmediatamente del articulo precedente, completamente independientes de λ; esto es, se obtienen las mismas ecuaciones no importa cual sea el valor que demos a λ. Esta observación puede ser extendida a la ecuación I en tanto que λ no sea divisible por n. Supongamos que (f, μ) = p'; por ello es facil ver que si (f, μ) coincide con cualquiera de los otros períodos p'', p'00, etc. la siguiente línea de argumento puede ser usada de modo completamente análogo. Ya que el número de ecuaciones I, II, III, etc. es e — 1, las cantidades p'', p''', etc. cuyo numero es = e — 2, pueden ser eliminadas de ellas por metodos conocidos. La ecuacion resultante (Z) estará libre de ellas:

0 = A + Bp + Cp2 + etc. + Mpe-1 + Np'

Esto se puede hacer de manera tal que todos los coeficientes A, B, ... N sean enteros y de seguro no todos = 0. Ahora, si no tenemos N = 0, se sigue que p' puede ser determinado como lo demanda el teorema. Queda por lo tanto probar que no puede hacerse N = 0.

Suponiendo que N = 0, la ecuacion Z se convierte en Mpe-1 + etc. + Bp + A = 0. Ya que ella no puede tener grado mayor que e — 1, no es satisfecha por más que e — 1 valores diferentes de p. Pero ya que las ecuaciones de las cuales se deduce Z son independientes de λ, se sigue que Z no depende de λ y así ella tendrá lugar, no importa que entero no divisible por n tomemos para λ. Por consiguiente esta ecuacion Z será satisfecha por cualquiera de las sumas (f, 1), (f,g), (f,g2), ... (f,ge-1), y se sigue inmediatamente que no todas estas sumas pueden ser diferentes sino que al menos dos de ellas deben ser iguales. Suponga que una de estas dos sumas iguales contiene las raíces [Z], [Z'], [Z''], etc. y la otra las raíces [η], [η'], [η''], etc. Supondremos (esto es legítimo) que todos los numeros Z, Z', Z'', etc., η, η', η'', etc. son positivos y < n. Evidentemente todos serín diferentes y ninguno de ellos = 0. Designaremos por Y la funciín

etc.

etc.

ζ + xz + xz +

xn xn' \_ xn"

tAy tAy tAy

Su termino mayor no puede exceder a xn-1 y Y = 0 si se pone x = [1]. Así Y tendrá un factor x — [1] en común con la funciín denotada por X en lo que precede y es fícil probar que esto sería absurdo. En efecto, si Y y X tienen un factor común, el maximo comín divisor de las funciones X e Y (no puede tener grado n — 1 porque Y es divisible por x) tendría todos sus coeficientes racionales. Esto seguiría de lanaturaleza de las operaciones involucradas en encontrar el máximo común divisor de dos funciones cuyos coeficientes son todos racionales. Pero en el artículo 341 probamos que X no puede tener un factor con coeficientes racionales de grado menor que n — 1. Por lo tanto la suposición N = 0 no puede ser consistente.

Ejemplo. Para n = 19, f = 6 resulta p2 = 6 + 2p + p' + 2p''. Ya que 0 = 1+ p + p' + p'', deducimos que p' = 4 — p2, p'' = —5 — p + p2. Por consiguiente

(6, 2) = 4 — (6,1)2, (6,4) = —5 — (6,1) + (6,1)2

1. = 4 — (6, 2)2, (6,1) = —5 — (6, 2) + (6, 2)2

(6,1) = 4 — (6,4)2, (6,2) = —5 — (6,4) + (6,4)2

347.

TEOREMA. Sea F = p(t,u, v,...) una función algebraica racional entera invariable[[221]](#footnote-222)) en las incognitas t, u, v, etc. Sustituyendo estas por las f raíces contenidas en el período (f,A), por las reglas del artículo 340 el valor de F es reducido a la forma

A + A'[1] + A''[2] + etc. = W.

Entonces las raíces que pertenecen al mismo período de f terminos tendrán coeficientes iguales en esta expresion.

Demostración. Sean [p] y [q] dos raíces pertenecientes al mismo período y suponga que p y q son positivas y menores que n. Hay que mostrar que [p] y [q] tienen el mismo coeficiente en W. Sea q ξ pgve (mod. n); y sean [A], [A'], [A''], etc. las raíces contenidas en (f, A), donde suponemos que A, A', A'', etc. son positivos y menores que n; finalmente sean μ, μ', μ'', etc. los menores residuos positivos de los numeros Agve, A'gve, A''gve, etc. segun el modulo n. Evidentemente estos serán identicos con los numeros A, A', A'', etc., aunque el orden puede estar transpuesto. Del artículo 340 es claro que

p([Agve], [A'gve], [AVe],...) = (/)

es reducido a

A + A'[gve] + A''[2gve] + etc. o a A + A' [θ] + A" [θ'] + etc. = (W')

Aquí, θ, θ', etc. designan los residuos mínimos de los números gve, 2gve, etc. según el modulo n y así vemos que el coeficiente que tiene [q] en (W') es el mismo que tiene [p] en (W). Si desarrollamos la expresiún (I) obtendremos lo mismo que obtenemos de desarrollar la expresión φ([μ], [μ'], [μ''], etc.) porque μ ξ λgve, μ' ξ λ'gve, etc. (mod. n). De hecho, esta ultima expresiún produce el mismo resultado que φ([λ], [λ'], [λ''], etc.), ya que los números μ, μ', μ'', etc. difieren de los números λ, λ', λ'', etc. solamente en el orden y esto no tiene importancia en una función invariable. Asú, W' es completamente identico con W y por eso la raúz [q] tendrú el mismo coeficiente que [p] en W. Q. E. D.

Entonces es claro que W puede ser reducido a la forma

A + i) + a'(f,g) + a''(f,g2) + ··· + ae(f,ge

y los coeficientes A, a, ...αε serán cantidades determinadas y enteras si todos los coeficientes racionales en F son enteros. Asú, e.g., si n = 19, / = 6, λ = 1 y la funcion φ designa la suma de los productos de las incúgnitas tomadas dos a dos, su valor es reducido a 3 + (6, 1) + (6, 4).

Si despues de esto t, u, v, etc. son sustituidas por las raúces de otro período (/, &λ), el valor de F se convertirá en

A + a(/, k) + a'(/, kg) + a''(/, kg2) + etc.

348.

En cualquier ecuaciúon

xf — -1 + -2 — -3 ··· =0

los coeficientes α, β, γ, etc. son funciones invariables de las raúces; esto es, α es la suma de todas ellas, β es la suma de sus productos tomados dos a la vez, γ es la suma de sus productos tomados tres a la vez, etc. Por lo tanto en la ecuaciún cuyas

raíces son aquéllas contenidas en el período (f, λ), el primer coeficiente será = (f, λ) y cada uno de los otros puede ser reducido a la forma

A + 1) + a(f,g) + ··· + a£(f,ge 3)

con todos los A, a, a0, etc. enteros. Es luego evidente que la ecuación cuyas raíces son las raíces contenidas en cualquiera otro período (f, kλ) puede ser derivada de la anterior sustituyendo (f, 1) por (f, k) en cada uno de los coeficientes, (f, g) por (f, kg), y en general (f,p) por (f,kp). De esta forma por lo tanto, se pueden especificar e ecuaciones z = 0, z0 = 0, z" = 0, etc., cuyas raíces serán las raíces contenidas en (f, 1), (f, g), (f, g2), etc., tan pronto como encontremos las e sumas (f, 1), (f,g), (f, g2), etc. o mejor dicho tan pronto como encontremos una cualquiera de ellas. Esto es cierto porque, por el artículo 346, todas las restantes pueden ser deducidas racionalmente de una de ellas. Hecho esto, la función X sera resuelta en e factores de grado f, pues evidentemente el producto de las funciones z, z', z00, etc. sera = X.

Ejemplo. Para n = 19 la suma de todas las raíces en el período (6, 1) es (6, 1) = α; la suma de sus productos tomados dos a la vez = 3 + (6, 1) + (6,4) = β; similarmente, la suma de los productos tomados tres a la vez = 2 + 2(6, 1) + (6, 2) = γ; la suma de los productos tomados cuatro a la vez = 3 + (6, 1) + (6, 4) = δ; la suma de los productos tomados cinco a la vez = (6, 1) = ε; el producto de todos ellos = 1. Así la ecuacion

z = χ6 — αχ5 + βχ4 — γχ3 + δχ2 — εχ + 1 = 0

contendrá todas las raíces incluidas en (6, 1). Y si sustituimos (6, 1), (6, 2) y (6,4) por (6, 2), (6, 4) y (6, 1) respectivamente en los coeficientes α, β, γ, etc., resultara la ecuaciín z' = 0, la cual contendrá las raíces de (6, 2). Si la misma permutaciín se aplica de nuevo, tendremos la ecuaciín z00 = 0 conteniendo las raíces de (6, 4), y el producto zz0z00 = X.

349.

A menudo es mas conveniente, en especial cuando f es un nímero grande, deducir los coeficientes β, γ, etc. de las sumas de las potencias de las raíces, por el teorema de Newton. Así la suma de los cuadrados de las raíces contenidas en (^λ) es = (f, 2λ), la suma de los cubos es = (f, 3λ), etc. Si escribimos q, q0, q00, etc. por (f, λ), (f, 2λ), (f, 3λ), etc. tendremos

a = q, 2β = aq — q , 3γ = ^q — aq0 + q00, etc.

donde, por el artículo 345, el producto de dos períodos ha de ser convertido inmediatamente en una suma de períodos. Así, en nuestro ejemplo, escribiendo p, p0 y P00 por (6,1), (6, 2) y (6, 4) respectivamente, tendremos q, q0, q00, q000, q0000 y q00000 respectivamente = p, p0, p0, p00, p0 y p00. Luego

a = p, 2β = p2 — pp0 = 6 + 2p + 2p003γ = (3 + p + p00)p — pp0 + p0 = 6 + 6p + 3p04δ = (2 + 2p + p0)p — (3 + p + p00)p0 + pp0 — p00 = 12 + 4p + 4p00, etc.

Sin embargo, es suficiente computar la mitad de los coeficientes de esta manera, porque no es difícil probar que los últimos son iguales a los primeros en orden inverso; esto es, el último = 1, el penúltimo = a, el antepenúltimo = β, etc.; o, de otra manera, el último puede ser derivado del primero sustituyendo (f, 1), (f, g), etc. por los períodos (f, —1), (f, —g), etc. o sea (f, n — 1), (f, n — g), etc. Los primeros casos se tienen cuando f es impar. El último coeficiente, sin embargo, siempre será = 1. La base para esto es establecida por el teorema del artículo 79, pero por razones de brevedad no nos dilataremos en el argumento.

350.

TEOREMA. Sea n — 1 el producto de los tres enteros positivos a, β y γ y considere el período (βγ, λ) de βγ términos compuesto de los β períodos menores de γ terminos, (γ, λ), (γ, λ0), (γ, λ00), etc. Supongamos luego que en una función de β incógnitas tal como en el artículo 347, esto es en F = ^>(t, u, v,...), se sustituyen las incógnitas t, u, v, etc. por las sumas (γ, λ), (γ,λ0), (γ, λ00), etc. respectivamente y de acuerdo con las reglas del artóculo 345.IV su valor es reducido a

A + α(γ, 1) + α0(γ, g) ··· + αζ(γ, gQ/9-Q) ··· + αθ(γ, gQ/9-1) = W

Entonces digo que si F es una función invariable, los períodos en W que están contenidos en el mismo período de βγ terminos (i.e. en general los períodos (γ^μ) y (γ^αν+μ) donde ν es cualquier entero), tendrón los mismos coeficientes.

Demostración. Ya que el período (βγ,λga) es idéntico a (βγ, λ), los períodos menores (γ^ga), (γ, λ/gα), (γ,λ//gα), etc. los cuales comprenden al primero, necesariamente coinciden con aquellos que comprenden al ultimo, aunque en un orden diferente. Si se supone que F sera transformado en W/ sustituyendo t, u, v, etc. por las primeras cantidades, respectivamente, W' coincidiró con W. Pero por el artículo 347 resulta

W0

A + a(Y,ga) + a/(Y,gQ+1 A + a(Y,ga) + a/(Y,ga+1

) ■■■ + az (γ ,gaP) ■■■ + αθ (γ^αβ+α-1) ) ■■■ + αΖ (γ 1) ■■■ + αθ (γ,gα-1)

así esta expresión debe coincidir con W y el primero, segundo, tercero, etc. coeficientes en W (comenzando con a) deben coincidir con el α + 1-esimo, el α + 2-esimo, el α + 3-esimo, etc. Concluimos en general que los coeficientes de los períodos (γ, g^), (γ^+μ), (γ^2^), ... (γ,gva+^, los cuales son el μ — 1-esimo, el α + μ +1-^simo, el 2α + μ +1-^simo, ...να + μ + 1-^simo ... deben coincidir con alguno otro. Q. E. D.

Así, es claro que W puede ser reducido a la forma

A + a(^1) + a/(^ g) ■■■ + a£(^ ga-1)

con todos los coeficientes A, a, etc. enteros, si todos los coeficientes en F son enteros. Suponga despues de esto que sustituimos las incognitas en F por los β períodos de γ terminos que constituyen otro período de βγ terminos, por ejemplo, aquellos contenidos en (βγ, λ^ que son (γ, λ^, (γ, λ^), (γ, λ0^), etc. Entonces el valor resultante sera A + α(βγ, k) + a0(βγ, gk) ■■■ + ae(βγ, ga 1k).

Es obvio que el teorema puede ser extendido al caso donde α = 1 o βγ = n — 1. En este caso todos los coeficientes en W serón iguales, y W sera reducido a la forma A + a^, 1).

351.

Ahora, reteniendo la terminología del artículo precedente, es claro que los coeficientes individuales de la ecuacion cuyas raíces son las β sumas (γ, λ), (γ, λ0), (γ, λ0/), etc. pueden ser reducidos a una forma como

A + a(^1) + a/(^ g) ■■■ + ae(^ ga-1)

y los numeros A, a etc. serón todos enteros. Se deriva de esto la ecuacion cuyas raíces son los β períodos de γ terminos contenidos en otro período (βγ, ^) si en todos loscoeficientes sustituimos todos los períodos (βγ,μ) por (βγ,k^). Si por consiguiente α = 1, todos los β períodos de γ terminos estarán determinados por una ecuación de grado β, y cada uno de los coeficientes será de la forma A + α(βγ, 1). Como resultado, todos ellos serán cantidades conocidas porque (βγ, 1) = (n — 1,1) = — 1. Si α > 1, los coeficientes de la ecuación cuyas raíces son todos los períodos de γ terminos contenidos en un período dado de βγ terminos, serán cantidades conocidas en tanto que todos los valores numericos de todos los α períodos de βγ terminos sean conocidos. El calculo de los coeficientes de estas ecuaciones sera a menudo mas fácil, especialmente cuando β no es muy pequeño, si primero se calculan las sumas de las potencias de las raíces y se deducen de estas los coeficientes por el teorema de Newton, como arriba en el artículo 349.

Ejemplo. I. Para n = 19 se busca la ecuacion cuyas raíces son las sumas (6, 1), (6, 2) y (6, 4). Designando estas raíces por p, p0, p", etc. respectivamente y la ecuacion buscada por

x3 — Ax2 + Bx — C = 0

tenemos

A = p + p + p, B = pp + pp + pp, C = ppp

Entonces

A = (18,1) = —1

y

pp0 = p + 2p0 + 3p00, pp" = 2p + 3p0 + p00, p0p00 = 3p + p0 + 2p00

así

B = 6(p + p0 + p00) = 6(18,1) = —6

y finalmente

C = (p + 2p0 + 3p00)p00 = 3(6, 0) + 11(p + p0 + p00) = 18 — 11 = 7

por lo tanto la ecuacion buscada es

x3 + x2 — 6x — 7 = 0

Usando el otro metodo, tenemos

p + p0 + p00 = — 1

p2 = 6 + 2p + p0 + 2p00, p02 = 6 + 2p0 + p00 + 2p, p002 = 6 + 2p00 + p + 2p0

de donde

p2 + p'2 + p"2 = 18 + 5 (p + p' + p") = 13

y similarmente

p3 + p'3 + p''3 = 36 + 34(p + p' + p'') = 2

De esto y del teorema de Newton derivamos la misma ecuación que antes.

II. Para n = 19 se busca la ecuación cuyas raíces son las sumas (2, 1), (2, 7) y (2, 8). Si las designamos por q, q' y q" encontramos

q + q' + q'' = (6, ^ qq' + qq'' + q'q'' = (6, 1) + (6, 4), qq'q'' = 2 + (6, 2)

y así, reteniendo la misma notacion que en lo precedente, la ecuación buscada sera

x3 — px2 + (p + p'')x — 2 — p' = 0

La ecuación cuyas raíces son las sumas (2, 2), (2, 3) y (2, 5) contenidas en (6, 2) puede ser deducida de lo anterior sustituyendo p, p' y p'' por p', p'' y p, respectivamente, y si hacemos la misma sustitución nuevamente, se obtiene la ecuacion cuyas raíces son las sumas (2,4), (2, 6) y (2,9) contenidas en (6,4).

*La solución de la ecuación* X = 0 *según se desarrolla de la investigación precedente.*

352.

El teorema anterior junto con sus corolarios contiene los principios bósicos de la teoría completa, y el metodo de hallazgo de los valores de las raíces Ω puede ser tratado ahora en unas pocas palabras.

Primero hay que tomar un número g que sea una raíz primitiva para el modulo n y encontrar el residuo mínimo de las potencias de g hasta gn-2 segín el modulo n. Resuelva n — 1 en factores, y de hecho en factores primos si es conveniente reducir el problema a ecuaciones del menor grado posible. Estos se llaman (el orden es arbitrario) α, β, γ, . ..C y defina

n — 1

α

βγ ...C = a

n — 1

αβ

γ...ζ =b

etc.

Distribuya todas la raíces Ω en α períodos de a terminos, y de nuevo cada uno de estos en β períodos de b terminos, y nuevamente cada uno de estos en γ períodos, etc.

Determine como en el artículo precedente la ecuación (A) de grado a, cuyas raíces son las a sumas de a terminos; sus valores pueden ser determinados resolviendo esta ecuacion.

Pero aquí surge una dificultad porque parece incierto que sumas deben hacerse iguales a que raíces de la ecuación (A); esto es, cual raíz debe ser denotada por (a, 1), cuól por (a, g), etc. Podemos resolver esta dificultad de la siguiente forma. Designamos con (a, 1) una raíz cualquiera de la ecuacion (A); en efecto, como cualquier raíz de esta ecuacion es la suma de a raíces de Ω, y es completamente arbitrario cual raíz de Ω se denota por [1], es posible asumir que [1] expresa una de las raíces que constituyen una raíz dada de la ecuacion (A), y de aquí esta raíz de la ecuacion (A) sera (a, 1). Aín así la raíz [1] no estará completamente determinada; todavía permanece completamente arbitrario o indefinido cuíl de las raíces que componen (a, 1) escogemos para adoptar como [1]. Tan pronto como (a, 1) sea determinada, todas las sumas restantes de a terminos pueden ser racionalmente deducidas de ella (art. 346). Así, es claro que es necesario resolver para una sola raíz de la ecuacion. Tambien se puede usar el siguiente metodo, menos directo, para el mismo propísito. Tome para [1] una raíz definida; i.e. sea [1] = cos + i sen ppp con el entero k tomado arbitrariamente pero de tal manera que no sea divisible por

n. Cuando se hace esto, tambien [2], [3], etc. determinaran raíces definidas, y las sumas (a, 1), (a, g), etc. designarán cantidades definidas. Ahora, si estas cantidades son calculadas de una tabla de senos con precision tal que se pueda decidir cuales son las mís grandes y cuales las mas pequeñas, esta sera dejada como la manera de distinguir sin duda las raíces individuales de la ecuacion (A).

Cuando de esta forma se han encontrado todas las a sumas de a terminos, determínese por los metodos del artículo precedente la ecuaciín (B) de grado β, cuyas raíces son las β sumas de b terminos contenidas en (a, 1); todos los coeficientes de esta ecuaciín serán cantidades conocidas. Ya que en esta etapa es arbitrario cual de los a = βb raíces contenidas en (a, 1) es denotada por [1], cualquier raíz dada de la ecuacion (B) puede ser expresada por (b, 1) porque es lícito suponer que una de las b raíces de las cuales esta compuesta es denotada por [1]. Determínese por lo tanto una raíz cualquiera de la ecuacion (B) por una solucion de esta. Sea ella = (b, 1) y derive de esta por el artículo 346 todas las restantes sumas de b terminos. De esta manera tenemos al mismo tiempo un metodo de corroboracion de los calculos, puesto que el total de todas las sumas de b terminos que pertenecen a un período cualquiera de a terminos es conocido. En algunos casos es igualmente facil formar otras a — 1 ecuaciones de grado β, cuyas raíces sean respectivamente las β sumas individuales

de b términos contenidas en los restantes períodos de a términos (a, g), (a, g2), etc. y determinar todas las raíces mediante la solución tanto de estas ecuaciones como de la ecuación B. Entonces, de la misma manera que antes, con la ayuda de una tabla de senos, podemos decidir cuales son los períodos de b terminos para los cuales las raíces individuales encontradas de esta manera son iguales. Pero para ayudar en esta decision pueden ser usados varios otros mecanismos que no se pueden explicar plenamente aquí. Uno de ellos, sin embargo, el caso donde β = 2, es especialmente ótil y puede ser explicado mas brevemente por ilustracion que por reglas. Lo utilizaremos en los siguientes ejemplos.

Despues de encontrar los valores de todos las αβ sumas de b terminos de esta forma, se puede utilizar un metodo similar para determinar por ecuaciones de grado γ todas las αβγ sumas de c terminos. Esto es, se puede o encontrar una ecuacion de grado γ de acuerdo con el artículo 350, cuyas raíces son las γ sumas de c terminos contenidos en (b, 1), y resolviendo esta encontrar una raíz que se llama (c, 1) y finalmente de esto por los metodos del artículo 346 deducir todas las sumas restantes; o de manera similar encontrar las αβ ecuaciones de grado γ cuyas raíces son respectivamente las γ sumas de c terminos contenidas en los períodos individuales de b terminos. Se puede resolver todas estas ecuaciones para todas sus raíces y determinar el orden de las raíces con la ayuda de una tabla de senos como hicimos antes. Sin embargo, para γ = 2 se puede usar el mecanismo que mostraremos mas abajo.

Continuando de esta manera finalmente habrá todas las n-1 sumas de Z terminos; y si se encuentra por los metodos del artículo 348 la ecuacion de grado Z cuyas raíces son las Z raíces de Ω contenidas en (Z, 1), todos sus coeficientes serán cantidades conocidas. Y si resolvemos para una raíz cualquiera, se puede hacerla = [1], y sus potencias darán todas las otras raíces Ω. Si nos gusta mas, podemos resolver para todas las raíces de esa ecuacion. Entonces mediante la solucion de las otras n?1 — 1 ecuaciones de grado Z, las cuales contienen respectivamente todas las Z raíces en cada uno de los restantes per iodos de Z terminos, se puede encontrar todas las restantes raíces Ω.

Es claro, sin embargo, que en tanto que la primera ecuacion (A) sea resuelta, o en tanto que se tengan los valores de todas las α sumas de a terminos, tendremos tambien la resolucion de X en α factores de grado a, por el artículo 348. Luego, despues de resolver la ecuacion (B) o despues de encontrar los valores de todas las αβ sumas de b terminos, cada uno de esos factores sera resuelto asimismo en β factores, y as I X sera resuelto en αβ factores de grado b, etc.

Ejemplo para n = 19 donde la operación se reduce a resolver dos ecuaciones cúbicas y una cuadrática.

353.

Primer ejemplo para n = 19. Ya que aquí n — 1 = 3 · 3 · 2, la búsqueda de las raíces Ω se reduce a la soluciún de dos ecuaciones cúbicas y una cuadrática. Este ejemplo es entendido mas facilmente porque para la mayor parte las operaciones necesarias ya han sido discutidas antes. Tomando el número 2 como la raíz primitiva g, los residuos mínimos de sus potencias producirán lo siguiente (los exponentes de las potencias esrán escritos en la primera línea y los residuos en la segunda):

1. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17
2. 2. 4. 8. 16. 13. 7. 14. 9. 18. 17. 15. 11. 3. 6. 12. 5. 10

De esto, por los artículos 344 y 345, se deduce facilmente la siguiente distribución de todas las raíces Ω en tres períodos de seis terminos y de cada uno de ellos en tres períodos de dos terminos:

Ω

(18,1)

|  |  |  |
| --- | --- | --- |
| í | (2, 1) .· | ·. [1], [18] |
| (6,1) { | (2, 8) .. | ·. [8], [11] |
| 1 | (2, 7) .. | ·. [7], [12] |
| í | (2, 2) . | ·. [2], [17] |
| (6, 2) \ | (2,16) .. | ·. [3], [16] |
| 1 | (2,14) .. | ·. [5], [14] |
| í | (2, 4) .. | ·. [4], [15] |
| (6,4) { | (2,13) .. | ·. [6], [13] |
|  | (2, 9) .. | ·. [9], [10] |

La ecuacion (A), cuyas raíces son las sumas (6, 1), (6, 2) y (6, 4), resulta ser

o 9

x3 + x — 6x — 7 = 0 y una de las raíces es —1,2218761623. Expresando en terminos de (6, 1), tenemos

(6, 2) = 4 — (6,1)2 = 2,5070186441

1. = —5 — (6,1) + (6,1)2 = —2,2851424818

Así X se resuelve en tres factores de grado 6, si estos valores son sustituidos en las formulas del artículo 348.

La ecuación (B), cuyas raíces son las sumas (2, 1), (2, 7) y (2, 8), resulta ser

x3 - (6,1)x2 + [(6,1) + (6,4)]x - 2 - (6, 2) = 0

o

x3 + 1,2218761623x2 - 3,5070186441x - 4,5070186441 = 0

Una raíz es -1,3545631433 que llamaremos (2,1). Por el metodo del artículo 346 se encuentran las siguientes ecuaciones donde, por brevedad, se escribe q en vez de

1. :

(2, 2) = q2 - 2

(2, 3) = q3 - 3q

1. = q4 - 4q2 + 2

(2, 5) = q5 - 5q3 + 5q

(2, 6) = q6 - 6q4 + 9q2 - 2

(2, 7) = q7 - 7q5 + 14q3 - 7q

(2, 8) = q8 - 8q6 + 20q4 - 16q2 + 2

(2, 9) = q9 - 9q7 + 27q5 - 30q3 + 9q

En el presente caso estas ecuaciones pueden ser encontradas mas facilmente del modo siguiente que por los metodos del artículo 346. Suponiendo

Γ11 kP . kP

I1I = cos + i sen

L J 19 19

tenemos

[18]

cos

18kP

*~19~*

+ i sen

18kP

19

kP kP

= cos i sen

19 19

y así

(2, 1) = 2 cos

kP

Ί9

y en general

[λ]

cos

λkP

*l9~*

λkP

+ i sen ,

19 ’

y así (2,λ)

[λ] + [18λ]

[λ] + [-λ] = 2 cos

λkP

Por lo tanto si ^q = cos ω, resultaró (2, 2) = 2cos2w, (2, 3) = 2cos3w, etc., y las mismas formulas de antes serón derivadas del conocimiento de ecuaciones para los

Los valores de (2, 7) y (2, 8) pueden encontrarse de la ecuaciún (B) donde son las dos raíces restantes. La duda sobre cual de estas raíces es (2, 7) y cual es (2, 8) puede eliminarse por un cúlculo aproximado de acuerdo con las formulas dadas antes o por medio de tablas de senos. Una rapida consulta nos muestra que (2, 1) = 2cos ω haciendo ω = P y así tenemos

cosenos de ángulos múltiples. Ahora, valores numericos:

(2, 2) = -0,1651586909

1. = 1,5782810188
2. = -1,9727226068

(2, 5) = 1,0938963162

de estas formulas se derivan los siguientes

(2, 6) = 0,4909709743

(2, 7) = -1,7589475024 (2, 8) = 1,8916344834

(2, 9) = -0,8033908493

49 8 56 1

(2, 7) = 2 cos — P = 2 cos — P, y (2,8) = 2 cos — P = 2 cos — P

V ’ ; 19 19 ’ \* V ’ ; 19 19

Similarmente podemos encontrar las sumas (2,2), (2,3) y (2,5) tambien por la

ecuación

x3 - (6, 2)x2 + [(6,1) + (6, 2)]x - 2 - (6,4) = 0

cuyas raíces son ellas, y la incertidumbre sobre que raíces corresponden a que sumas se puede eliminar exactamente de la misma manera que antes. Finalmente, las sumas (2, 4), (2, 6) y (2, 9) se pueden encontrar por la ecuacion

x3 - (6,4)x2 + [(6, 2) + (6,4)]x - 2 - (6,1) = 0

[1] y [18] son las raíces de la ecuaciún x2 - (2, 1)x + 1 = 0. Una de ellas sera

= i(2.1) - ^1 - i(2, l)2 = 1(2.1) + ^- 1(2,2)

y la otra

=1<2,1} - VFIm

y los valores numericos serán = -0,6772815716 ± 0,7357239107i. Las dieciseis raíces restantes pueden ser encontradas de las potencias de una u otra de estas raíces o resolviendo las otras ocho ecuaciones similares. Para decidir, en el segundo metodo

cual raíz tiene el signo positivo para su parte imaginaria y cual el negativo, podemos usar tablas de senos o el artificio que explicamos en el siguiente ejemplo. De esta manera encontraremos los siguientes valores, con el signo superior correspondiendo a la primera raíz y el signo inferior a la segunda raíz:

1. y [18] = -0,6772815716 ± 0,7357239107i
2. y [17] = -0,0825793455 τ 0,9965844930i
3. y [16] = 0,7891405094 ± 0,6142127127i
4. y [15] = -0,9863613034 ± 0,1645945903 i
5. y [14] = 0,5469481581 τ 0,8371664783 i
6. y [13] = 0,2454854871 ± 0,9694002659i
7. y [12] = -0,8794737512 τ 0,4759473930i
8. y [11] = 0,9458172417 τ 0,3246994692 i
9. y [10] = -0,4016954247 ± 0,9157733267i

*Ejemplo para* n = 17 *donde la operación se reduce  
a resolver cuatro ecuaciones cuadráticas.*

354.

Segundo ejemplo para n = 17. Aquí n - 1 = 2 · 2 · 2 · 2, así el calculo se reducirá a cuatro ecuaciones cuadráticas. Para la raíz primitiva tomaremos el número 3, cuyas potencias tienen residuos mínimos según el múdulo 17 que son

1. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15
2. 3. 9. 10. 13. 5. 15. 11. 16. 14. 8. 7. 4. 12. 2. 6

De esto derivamos la siguiente distribución del conjunto Ω en

dos períodos de ocho

terminos, cuatro de cuatro terminos, ocho de dos terminos:

Ω

(16,1)

(8,1)

(8, 3)

(4, 1) (4, 9) (4, 3) (4,10)

(2, 1) (2,13) (2, 9) (2,15) (2, 3) (2, 5) (2,10) (2,11)

[1], [16]

1. , [13] [8], [9]
2. , [15]
3. , [14]
4. , [12] [7], [10]
5. , [11]

Se encuentra por las reglas del artículo 351 que la ecuación (A), cuyas raíces son las sumas (8, 1) y (8, 3), es x2 + x — 4 = 0. Sus raíces son — 1 + 1λ/Ϊ7 = 1,5615528128 y —1 — 1 -\/l7 = —2,5615528128. Haremos la primera = (8,1) y así necesariamente la óltima = (8, 3).

La ecuación (B), cuyas raíces son las sumas (4, 1) y (4, 9), es x2 —(8, 1)x—1 = 0. Sus raíces son 1 (8,1) ± 2\J4 + (8,1)2 = 1 (8,1) ± }^\] 12 + 3(8,1) + 4(8, 3). Haremos (4, 1) igual a la cantidad que tenga el signo radical positivo y cuyo valor numerico es 2,0494811777. Así la cantidad con el signo del radical negativo y cuyo valor numerico es —0,4879283649 serí expresada por (4, 9). Las sumas restantes de cuatro terminos, a saber (4, 3) y (4, 10), pueden ser calculadas de dos maneras. Primera, por el metodo del artículo 346, que da las siguientes formulas cuando abreviamos (4, 1) con la letra

p:

31

(4, 3) = — - + 3p — -p3 = 0,3441507314 22

31

1. = - + 2p — p2 — - p3 = —2,9057035442 22

El mismo metodo da la fórmula (4, 9) = —1 — 6p+p2 + p3 y de esta obtenemos el mismo valor que antes. El segundo metodo permite determinar las sumas (4, 3) y (4, 10) resolviendo la ecuación x2 — (8, 3)x — 1 = 0 de la que ellas son las raíces. Estas raíces son 1 (8, 3) ± 4 + (8, 3)2, o sea

11 11

2(8,3) + -^12 + 4(8,1)+3(8,3) y 2(8,3) — ^12 + 4(8,1)+3(8,3)

Se puede remover la duda de cual raíz debe ser expresada por (4,3) y cual por (4, 10) mediante el siguiente artificio que mencionamos en el artículo 352. Calcule el producto de (4,1) — (4,9) por (4, 3) — (4,10) que es = 2(8,1) — 2(8, 3) [[222]](#footnote-223)). Ahora el valor de esta expresiín es positivo = +2VT7 y, ya que el primer factor del producto,

1. — (4, 9) = +^12 + 3(8,1) + 4(8, 3), es positivo, el otro factor (4, 3) — (4,10), deberá ser tambien positivo. Por lo tanto (4, 3) es igual a la primera raíz que tiene el signo positivo enfrente del radical, y (4, 10) es igual a la segunda raíz. De esto resultarán los mismos valores numericos que antes.

Habiendo encontrado todas las sumas de cuatro terminos, procedemos a las sumas de dos terminos. La ecuaciín (C), cuyas raíces son (2, 1) y (2, 13) y estí

contenida en (4, 1), será x2 — (4,1)x + (4, 3) = 0. Sus raíces son

11 11

2(4,1) ± 2J—4(4,3) + (4,1)2 osea -(4,1) ± -^4+(4,9) — 2(4,3)

Cuando tomamos la cantidad radical positiva, obtenemos el valor 1,8649444588, la que hacemos = (2, 1) y así (2, 13) será igual a la otra cuyo valor es = 0,1845367189. Si las sumas restantes de dos terminos han de ser encontradas por el metodo del artículo 346, se pueden usar las mismas formulas para (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7) y (2, 8) como lo hicimos en el ejemplo precedente para cantidades similares, es decir, (2, 2) (o (2, 15)) = (2, 1)2 — 2 etc. Pero si parece preferible encontrarlas en pares resolviendo una ecuación cuadrática, para (2, 9) y (2, 15) obtenemos la ecuacián x2 — (4,9)x +(4,10) = 0 cuyas raíces son ^(4, 9) ± 4 + (4,1) — 2(4,10). Se puede

determinar que signo usar del mismo modo que antes. Calculando el producto de

1. — (2,13) por (2, 9) — (2,15) resulta —(4,1) + (4,9) — (4, 3) + (4,10). Ya que este es negativo y el factor (2, 1) — (2, 13) es positivo, (2, 9) — (2, 15) deberá ser negativo y es necesario usar el signo superior positivo para (2, 15) y el signo inferior negativo para (2, 9). De esto se computa que (2, 9) = —1,9659461994 y (2,15) = 1,4780178344. Entonces, ya que calculando el producto de (2, 1) — (2, 13) por (2, 3) — (2, 5) resulta la cantidad positiva (4, 9) — (4,10), el factor (2, 3) — (2, 5) debe ser positivo. Y por un calculo parecido al anterior se encuentra

(2, 3) = 1(4,3) + 2^4+(4,10) — 2(4,9) = 0,8914767116 22

(2, 5) = 2(4,3) — 2^4+(4,10) — 2(4,9) = —0,5473259801

Finalmente, mediante operaciones completamente analogas se descubre

1. = 2(4,10) — 2^4+(4, 3) — 2(4,1) = —1,7004342715

22

1. = 2(4,10) + 2^4+(4, 3) — 2(4,1) = —1,2052692728

22

Resta ahora descender a las raíces Ω mismas. La ecuacián (D) cuyas raíces son [1] y [16] nos da x2 — (2, 1)x +1 =0. Las raíces de ella son ^ (2, 1) ± (2, 1)2 — 4

o mejor dicho

1(2.1) ± 2 A4 — (2.1)2 osea i(2,1) ± 2 ij 2 — (2,15)

Tomaremos los signos superiores para [1], los inferiores para [16]. Se deducen las catorce raíces restantes de las potencias de [1] o por la solución de siete ecuaciones cuadráticas, cada una de las cuales nos dará dos raíces, y la incertidumbre acerca de los signos de las cantidades radicales puede ser removida mediante el mismo mecanismo usado antes. Así [4] y [13] son las raíces de la ecuacián x2 — (2, 13)x+1 = 0 y así igual a 2(2, 13) ± 2i\¡2 — (2, 9). Calculando el producto de [1] — [16] por [4] — [13] sin embargo obtenemos (2, 5) — (2, 3), una cantidad real negativa. Por lo tanto, puesto que [1] — [16] es +i\j2 — (2, 15), i.e. el producto imaginario i por una cantidad real positiva, [4] — [13] debe tambien ser el producto de i por una cantidad real positiva, porque i2 = —1. Como conclusion tomaremos el signo superior para [4] y el signo inferior para [13]. Similarmente para las raíces [8] y [9] encontramos 2(2, 9) ± 2i\¡2 — (2, 1) así, ya que el producto de [1] — [16] por [8] — [9] es (2, 9) — (2, 10) y negativo, debemos tomar el signo superior para [8] y el signo inferior para [9]. Si computamos entonces las restantes raíces obtendremos los siguientes valores numericos, donde el signo superior ha de ser tomado para la primera raíz y el signo inferior para la segunda:

± 0,3612416662 i ± 0,6736956436 i ± 0,8951632914i ± 0,9957341763 i ± 0,9618256432 i ± 0,7980172273 i ± 0,5264321629 i ±0,1837495178 i

[1], [16]

1. , [15]
2. , [14]
3. , [13]
4. , [12]
5. , [11]
6. , [10]
7. , [9]

0,9324722294

0,7390089172

0,4457383558

0,0922683595

0,2736629901

0,6026346364

0,8502171357

0,9829730997

Lo que precede puede bastar para resolver la ecuacion xn — 1 = 0 y así tambien para encontrar las funciones trigonometricas correspondientes a los arcos que son conmesurables con la circunferencia. Pero esta materia es tan importante que no podemos concluir sin indicar algunas de las observaciones que arrojan luz sobre el tema, lo mismo que ejemplos relacionados con el o que dependen de el. Entre estos seleccionaremos específicamente aquellos que pueden ser resueltos sin una gran cantidad de aparato que depende de otras investigaciones y los consideramos solamente como ejemplos de esta inmensa teoría que deberá ser considerada detalladamente en una ocasion posterior.

*Investigaciones adicionales sobre los períodos de raíces.  
Sumas con un número par de términos son cantidades reales.*

355.

Ya que siempre n se supone impar, 2 estará entre los factores de n — 1, y el conjunto Ω estará compuesto de 2(n — 1) períodos de dos terminos. Un tal período (2,λ) consistirá de las raíces [λ] y [λg2(n-1)], denotando, como antes, g como cualquier raíz primitiva para el modulo n. Pero g2 (n-U = — 1 (mod. n) y así λg2(n-1) = —λ (ver art. 62) y ^g2(n-1)] = [—λ]. Por lo tanto, suponiendo que [λ] = cos ^p + i sen ^p y [—λ] = cos ^p — i sen ^p, resulta la suma (2,λ) = 2 cos ^p. Hasta este punto ánicamente deducimos la conclusián de que el valor de cualquier suma de dos terminos es una cantidad real. Puesto que cualquier período que tenga un námero par de terminos = 2α se puede descomponer en a períodos de dos terminos, en general es claro que el valor de cualquier suma que tenga un numero par de terminos es siempre una cantidad real. Por lo tanto, si en el artículo 352 entre los factores α, β, γ, etc., se reservan dos hasta el final, todas las operaciones serán hechas sobre cantidades reales hasta que lleguemos a una suma de dos terminos, y los imaginarios serán introducidos cuando pasamos de estas sumas a las raíces mismas.

*De la ecuación que define la distribución de las raíces Ω en dos períodos.*

356.

Merecen atención especial las ecuaciones auxiliares mediante las cuales se determinan para cualquier valor de n las sumas que forman el conjunto Ω. Ellas estan conectadas de una manera sorprendente con las propiedades mas reconditas del nímero n. Aquí nos restringiremos al estudio de los dos casos siguientes. Primero, la ecuacion cuadrática cuyas raíces son sumas de 2(n — 1) terminos, segundo, en caso de que n — 1 tenga el factor 3, consideraremos la ecuacion cubica cuyas raíces son sumas de 3(n — 1) terminos.

Escribiendo por brevedad m en lugar de 2 (n — 1) y designando por g alguna raíz primitiva para el modulo n, el conjunto Ω consistira de dos períodos (m, 1) y (m, g). El primero contendrá las raíces [1], [g2], [g4], ... [gn-3], el ultimo las raíces [g], [g3], [g5], ... [gn-2]. Suponiendo que los residuos m ínimos positivos de los numeros g2, g4,...gn-3 segun el modulo n son, en orden arbitrario, R, R0, R00, etc. y los residuos de g, g3, g5, ...gn-2 son N, N0, N00, etc., entonces las raíces de las que consiste (m, 1), coinciden con [1], [R], [R0], [R00], etc. y las raíces del período (m, g) con [N], [N0], [N00], etc. Es claro que todos los numeros 1, R, R0, R00, etc. son residuos

cuadráticas del número n. Puesto que todos ellos son diferentes y menores que n, y ya que su numero es = 2 (n — 1) y así igual al número de todos los residuos positivos de n que son menores que n, estos residuos coincidirún completamente con aquellos números. Igualmente, todos los numeros N, N', N'', etc. son diferentes uno del otro y de los numeros 1, R, R', etc. y junto con estos agotan todos los números 1, 2, 3, ...n — 1. Se sigue que los numeros N, N', N'', etc. deben coincidir con todos los na residuas cuadráticas positivos de n que son menores que n. Ahora, si se supone que la ecuación cuyas raíces son las sumas (m, 1) y (m, g) es

x2 — Ax + B = 0

resulta

A = (m, 1) + (m, g) = —1, B = (m, 1) · (m, g)

El producto de (m, 1) por (m,g) es, por el artículo 345,

= (m, N + 1) + (m, N' + 1) + (m, N'' + 1) + etc. = W

y de ese modo se reducirá a una forma a(m, 0) + e(m, 1) + γ(m, g). Para determinar los coeficientes α, β y γ observamos primera que α + β + γ = m (porque el número de sumas en W = m); segunda, que β = γ (esto sigue del artúculo 350 pues el producto (m, 1) · (m,g) es una función invariable de las sumas (m, 1) y (m, g) de las que se compone la suma mús grande (n — 1, 1)); tercera, puesto que todos los numeros N + 1, N' + 1, N'' + 1, etc. esrán contenidos entre las cotas 2 y n +1, es claro que a ninguna suma en W puede ser reducida a (m, 0) y asú α = 0 cuando el número n — 1 no se halla entre los numeros N, N', N'', etc. a que una suma, digamos (m,n) puede ser reducida a (m, 0) y asú α = 1 cuando n — 1 no se halla entre los números N, N', N'', etc. En el primer caso por lo tanto se infiere α = 0, β = γ = 2m, en el ultimo α = 1, β = γ = 2(m — 1). Ya que los números β y γ deben ser enteros, se sigue que se tendrá el primer caso, esto es, n — 1 (o lo que es lo mismo, —1) no se encontrará entre los no residuos de n cuando m es par o n es de la forma 4k +1. El último caso se tendrá, esto es, n — 1o sea —1 serú un no residuo de n, siempre que m sea impar o n sea de la forma 4k + 3 [[223]](#footnote-224)). Ahora, ya que (m, 0) = m, (m, 1) + (m,g) = —1, el

producto buscado será = — 2m en el primer caso y será = ^ (m +1) en el último. Así la ecuacián en el primer caso será x2 + x — | (n — 1) =0 con raíces — 1 ± \yjñ, en el último x2 + x + 1 (n +1) con raíces — ^ ± 2iyfñ.

Sea R el conjunto de todos los residuos cuadráticos positivos de n que son menores que n y sea N el conjunto de todos los no residuos correspondientes. Entonces, no importa cuál raíz de Ω sea escogida por [1], la diferencia entre las sumas X][R] y Σ[Ν] será = ±yfñ para n ξ 1 e = ±iyfñ para n ξ 3 (mod. 4). Se sigue que si k es cualquier entero no divisible por n

\_ kRP \_ kNP , ^ \_ kRP \_ kNP o

> cos > cos = ±vn y > sen > sen = 0

n n n n

para n ξ 1 (mod. 4). Por otra parte para n ξ 3 (mod. 4) la primera diferencia sera = 0 y la segunda = ±\fñ. Estos teoremas son tan elegantes que merecen una distinción especial. Observamos que los signos superiores siempre se mantienen cuando en vez de k se toma la unidad o un residuo cuadratico de n y los inferiores cuando k es un no residuo. Estos teoremas mantienen la misma o aán mayor elegancia cuando son extendidos a valores compuestos de n. Pero estas materias están en un nivel superior de investigacion y reservaremos sus consideraciones para otra ocasion.

Demostración de un teorema mencionado en Sección IV.

357.

Sea

z = xm — axm— + bxm-2 — etc. = 0

la ecuacián de grado m cuyas rames son las m rames contenidas en el período (m, 1). Aquá a = (m, 1) y cada uno de los coeficientes restantes b, etc. serán de la forma A + B(m, 1) + C(m, g) con A, B y C, enteros (art.348). Denotando por z0 la funcián en la que se transforma z cuando se sustituyen (m, 1) por (m, g) en todas partes y (m, g) por (m, g2), o lo que es la misma cosa (m, 1), entonces las rames de la ecuacion z0 = 0 serán las rames contenidas en (m, g) y el producto

xn - 1

/

zz

x1

Por lo tanto z puede ser reducida a la forma R + S(m, 1) + T(m, g) donde R, S y T serán funciones enteras de x con todos sus coeficientes enteros. Hecho esto, resulta

z0 = R + S (m,g) + T (m, 1)

Y si por brevedad escribimos p y q por (m, 1) y (m,g) respectivamente

2z = 2R + (S + T)(p + q) - (T - S)(p - q)=2R - S - T - (T - S)(p - q) y similarmente

2z = 2R - S - T + (T - S)(p - q)

así, poniendo

2R - S - T = Y, T - S = Z (p - q)2Z2 y ya que (p - q)2 = ±n

resulta 4X = Y2

4X = Y2 ^ nZ2

El signo superior vale cuando n es de la forma 4k +1, el inferior cuando n es de la forma 4k + 3. Este es el teorema que prometimos probar (art. 124). Es facil ver que los dos terminos de mayor grado en la función Y siempre serán 2xm + xm-1 y el mayor en la funcion Z, xm-1. Todos los coeficientes restantes serán enteros, variarán de acuerdo con la naturaleza del námero n y no se puede dar una fármula analítica general.

Ejemplo. Para n = 17, por las reglas del artículo 348, la ecuacián cuyas raíces son las ocho raíces contenidas en (8,1) sera

x8 - px7 + (4 + p + 2q)x6 - (4p + 3q)x5 + (6 + 3p + 5q)x4

- (4p + 3q)x3 + (4 + p + 2q)x2 - px + 1 = 0

por lo tanto

R = x8 + 4x6 + 6x4 + 4x2 + 1 S = -x7 + x6 - 4x5 + 3x4 - 4x3 + x2 - x T = 2x6 - 3x5 + 5x4 - 3x3 + 2x2

y

Y = 2x8 + x7 + 5x6 + 7x5 + 4x4 + 7x3 + 5x2 + x + 2 Z = x7 + x6 + x5 + 2x4 + x3 + x2 + x

He aquí algunos otros ejemplos

|  |  |  |
| --- | --- | --- |
| n | Y | Z |
| 3 | 2x + 1 | 1 |
| 5 | 2x2 + x + 2 | x |
| 7 | 2x3 + x2 — x — 2 | 2  x2 + x |
| 11 | 2x5 + x4 — 2x3 + 2x2 — x — 2 | 4 1  x4 + x |
| 13 | 2x6 + x5 + 4x4 — x3 + 4x2 + x + 2 | 53 x5 + x3 + x |
| 19 | 2x9 + x8 — 4x7 + 3x6 + 5x5 — 5x4 —3x3 + 4x2 — x — 2 | x8 x6 I x5 I x4 x3 I x  1 \*Aj 1 \*Aj \*Aj 1 \*Aj |
| 23 | 2xn + x10 — 5x9 — 8x8 — 7x7 — 4x6 | x10 + x9 \_ x7 \_ 2x6 \_ 2x5  \*Aj 1 \*Aj \*Aj \*Aj \*Aj |
|  | +4x5 + 7x4 + 8x3 + 5x2 — x — 2 | 42  —x4 + x2 + x |

De la ecuación que distribuye las raíces Ω en tres períodos.

358.

Procedemos ahora a la consideración de las ecuaciones cúbicas que determinan las tres sumas de ^(n — 1) terminos que componen el conjunto Ω, para el caso en que n es de la forma 3k + 1. Sea g cualquier raíz primitiva para el módulo n y 3 (n — 1) = m que seró un entero par. Entonces las tres sumas que componen Ω serón (m, 1), (m,g) y (m, g2), por las cuales escribimos p, p0 y p" respectivamente. Es claro que la primera contiene las raíces [1], [g3], [g6], ... [gn-4], la segunda las raíces [g], [g4], ... [gn-3], y la tercera las raíces [g2], [g5], ... [gn-2]. Suponiendo que la ecuación buscada es

x3 — Ax2 + Bx — C = 0

resulta

A = p + p + p, B = pp + pp + pp, C = ppp

y directamente A = —1. Sean A, B, C, etc., los residuos positivos mónimos de los nómeros g3, g6, ...gn-4 segón el modulo n, en orden arbitrario, y sea K el conjunto de ellos y el numero 1. Similarmente sean A0, B0, C0, etc. los residuos mónimos de los nómeros g, g4, g7, ...gn-3 y K0 su conjunto; finalmente sean A00, B00, C00,

etc. los residuos mónimos de g2, g5, g8, ...gn-2 y K00 su conjunto. Asó todos los nómeros en K, K , K serán diferentes y coincidirán con 1, 2, 3, ...n — 1. Primero que todo, debemos observar aquó que el nómero n — 1 debe estar en K, pues es facil

. 3 m . y y

ver que es un residuo de g 2 . Tambien sigue de esto que los dos numeros h, n — h se encontrarán siempre en uno mismo de los tres conjuntos K, K0 y K00, porque si

uno de ellos es un residuo de la potencia g\ el otro será un residuo de la potencia gAi 2 o de g 2 si λ > —. Denotaremos por (KK) el numero de enteros en la serie 1, 2, 3, . ..n — 1 que pertenencen a K por si mismos y cuando son aumentados en una unidad; similarmente (KK0) será el numero de enteros en la misma serie, que están ellos mismos contenidos en K pero están en K0 cuando son aumentados en una unidad. Sera inmediatamente obvio cual es el significado de las notaciones (KK00), (K0K), (K0K0), (K0K00), (K00K), (K00K0) y (K00K00). Hecho esto, digo primero que (KK0) = (K0K). En efecto, suponiendo que h, h0, h00, etc. son todos los námeros de la serie 1,2,3, ...n — 1 que estan ellos mismos en K pero con los práximos námeros mayores h + 1, h0 + 1, h00 + 1, etc. en K0, de modo que por definicián el numero de ellos es (KK0), entonces es claro que todos los números n — h — 1, n — h0 — 1, n — h00 — 1, etc. estan contenidos en K0 y los proximos námeros mayores n — h, n — h0, etc. en K; y ya que existen (K0K) de tales námeros en total, de seguro no podemos tener (K0K) < (KK0). Se demuestra similarmente que no es posible tener (KK0) < (K0K), asái estos nuámeros son necesariamente iguales. Exactamente de la misma manera se prueba que (KK00) = (K00K) y (K0K00) = (K00K0). Segundo, ya que cualquier numero en K, con excepción del mas grande, n — 1, debe ser seguido por el siguiente mayor en K o en K0 o en K00, la suma (KK) + (KK0) + (KK00) debe ser igual al numero de todos los numeros en K disminuido en una unidad, esto es = m — 1. Por una razán similar

(K0K) + (K0K0) + (K0K00) = (K00K) + (K00K0) + (K00K00) = m

Con estos preliminares, por las reglas del artículo 345 desarrollaremos el producto pp' en (m, A0 + 1) + (m, B0 + 1) + (m, C0 + 1) + etc. Esta expresion se reduce facilmente a (K0K)p + (K'K')p' + (K0K00)p00. Por el artículo 345 se obtiene de esto el producto p0p00 sustituyendo (m, 1), (m, g) y (m, g2) por las cantidades (m, g), (m,g2) y (m, g3) respectivamente, i.e., p, p0 y p00 por p0, p00 y p respectivamente . Así tenemos p0p00 = (K0K)p0 + (K0K0)p00+(K0K00)p y similarmente p00p = (K0K)p00+(K0K0)p+(K0K00)p0. De esto obtenemos primero

B = m(p + p0 + p00) = —m

y segundo de una manera similar a aquella por la cual fue desarrollado pp0, se reduce tambien pp00 a (K00K)p + (K00K0)p0 + (K00K00)p00. Y ya que esta expresion debe ser identica a la precedente, es necesario que (K00K) = (K0K0) y (K00K00) = (K0K). Ahora, poniendo

(K0K00) = (K00K0) = a

(K00K00) = (K0K) = (KK0) = b (K0K0) = (K00K) = (KK00) = c

resulta m — 1 = (KK) + (KK0) + (KK00) = (KK) + b + c. Y ya que a + b + c = m, (KK) = a — 1. Así las nueve cantidades desconocidas se reducen a tres a, b y c o mejor, ya que a + b + c = m, a dos. Finalmente, es claro que el cuadrado p2 se convierte en (m, 1 + 1) + (m, A + 1) + (m, B + 1) + (m, C + 1) + etc. Entre los terminos de esta expresión tenemos (m, n) que se reduce a (m, 0) o sea a m, y los restantes terminos se reducen a (KK)p + (KK0)p0 + (KK00)p00, así p2 = m + (a — 1)p + bp0 + cp00.

Como un resultado de las investigaciones anteriores tenemos las siguientes reducciones:

p2 = m + (a — 1)p+bp0 +cp00 pp0 = bp+cp0+ap00

pp00 = cp+ap0 +bp00

p0p00 = ap +bp0 +cp00

donde las tres incognitas satisfacen la ecuación condicional

a + b + c = m (I)

y por otra parte es cierto que estos numeros son enteros. Como una consecuencia tenemos

C = p · p0p00 = ap2 + bpp0 + cpp00

= am + (a2 + b2 + c2 — a)p + (ab + bc + ac)p0 + (ab + bc + ac)p00

Pero ya que pp0p00 es una funcion invariable de p, p0 y p00, los coeficientes por los que ellos son multiplicados en la expresion precedente son necesariamente iguales (art. 350) y hay una nueva ecuacion

a2 + b2 + c2 — a = ab + bc + ac (II)

y de esta C = am + (ab + bc + ac)(p + p0 + p00) o (causa de (I) y por el hecho que p + p0 + p00 = —1)

C = a2 — bc (///)

Ahora, aun cuando C depende de tres incognitas y existen solamente dos ecuaciones, no obstante con la ayuda de la condicion de que a, b y c son enteros, ellos seran

suficientes para determinar C completamente. Para demostrar esto, expresamos la ecuación (II) como

12a + 12b + 12c + 4 = 36a2 + 36b2 + 36c2 — 36ab — 36ac — 36bc — 24a + 12b +12c + 4

Por (I), el lado izquierdo se convierte en = 12m + 4 = 4n. El lado derecho se reduce a

(6a — 3b — 3c — 2)2 + 27(b — c)2

o, escribiendo k en vez de 2a — b — c, a (3k — 2)2 + 27(b — c)2 . Así el número 4n (i.e. el cuadruple de cualquier número primo de la forma 3m + 1) puede ser representado por la forma x2 + 27y2. Esto puede, por supuesto, deducirse sin ninguna dificultad de la teoría general de formas binarias, pero es notable que tal descomposiciún esta ligada a los valores de a, b y c. Ahora, el numero 4n siempre puede ser descompuesto de una única manera en la suma de un cuadrado y 27 veces otro cuadrado. Demostraremos esto como sigue [[224]](#footnote-225)). Si se supone que

4n = t2 + 27u2 = t'2 + 27u/2

tenemos primero

(tt' — 27uu')2 + 27(tu' + t'u)2 = 16n2

segundo

(tt' + 27uu')2 + 27(tu' — t'u)2 = 16n2

tercero

(tu' + t'u)(tu' — t'u) = 4n(u'2 — u2)

De esta tercera ecuacion se sigue que n, por ser un numero primo, divide uno de los numeros tu' + t'u, tu' — t'u. De la primera y segunda, sin embargo, es claro que cada uno de estos números es menor que n, así al que n divide es necesariamente = 0. Por lo tanto u' — u2 = 0 y u' = u2 y t' = t2; i.e. las dos descomposiciones no son diferentes. Supongamos ahora que se conoce la descomposicioún de 4n en un cuadrado mas 27 veces un cuadrado (esto se puede hacer por el metodo directo de la sección V o por el metodo indirecto de los art. 323 y 324). Si 4n = M2 + 27N2, los cuadrados (3k — 2)2 y (b — c)2 estarán determinados y tendremos dos ecuaciones

en lugar de la ecuación (II). Pero claramente no solo estará determinado el cuadrado (3k — 2)2 sino tambien su raíz 3k — 2. Porque debe ser = +M o = —M, la ambigüedad es facilmente eliminada, pues ya que k debe ser un entero, resulta 3k — 2 = +M o = — M de acuerdo con que M sea de la forma 3z + 1 o 3z + 2\*). Ahora, puesto que k = 2a — b — c = 3a — m, resulta a = 3 (m + k), b + c = m — a = 3 (2m — k) y así

C = a[[225]](#footnote-226) — bc = a2 = 1(m + k)2 -

-1(b +c)2 + 4(b — c)2

36(2m—k)2+1 n2=k2+3km+4 n2

y entonces se han encontrado todos los coeficientes de la ecuación. Q. E. F. Esta fórmula seró mucho mós simple si sustituimos N2 por sus valores de la ecuación (3k — 2)2 + 27N2 = 4n = 12m + 4. Despues del calculo obtenemos

C

1

9

(m + k + 3km)

1

9

( m + kn)

El mismo valor puede ser reducido a (3k — 2)N2 + k[[226]](#footnote-227) — 2k2 + k — km + m. Aunque esta expresión es menos útil, muestra inmediatamente que C resulta ser un entero, como debería.

Ejemplo. Para n = 19 tenemos 4n = 49 + 27, asó 3k — 2 = +7, k = 3,

C = 1 (6 + 57) = 7 y la ecuacion buscada es x3 + x2 — 6x — 7 = 0, como antes

(art. 351). Similarmente, para n = 7, 13, 31, 37, 43, 61 y 67 el valor de k es

respectivamente 1, —1, 2, —3, —2, 1, —1 y C = 1, —1, 8, —11, —8, 9, —5.

Aunque el problema que hemos resuelto en este artóculo es bastante intrincado, no hemos querido omitirlo a causa de la elegancia de la solucion y porque da ocasion para usar varios artificios que son frucríferos tambien en otras discusiones j).

Reducción a ecuaciones puras de las ecuaciones que dan las raíces Ω.

359.

Las investigaciones precedentes trataban del descubrimiento de ecuaciones auxiliares. Ahora explicaremos una propiedad muy notable concerniente a sus soluciones. Consta que todos los trabajos de los geometras eminentes han fracasado en la búsqueda de una solución general de ecuaciones de grado mayor que cuatro, o (para definir lo que se desea mas exactamente) de la REDUCCION DE ECUACIONES MIXTAS A ECUACIONES PURAS. Existe la pequeña duda de si este problema no solamente estú mas alla de las facultades del anúlisis contemporaneo sino que propone lo imposible (cf. lo que dijimos de este asunto en Demonstr. nova etc., art. 9). No obstante es cierto que existen innumerables ecuaciones mixtas de todos los grados que admiten una reduccion a ecuaciones puras, y esperamos que los geometras encontraraún esto gratificante si demostramos que nuestras ecuaciones son siempre de esta clase. Pero a causa de la longitud de esta discusion, presentaremos aquí solamente los principios mas importantes para demostrar que la reducciún es posible; reservamos para otra ocasiún una consideracion mús completa, la que el tema merece. Presentaremos primero algunas observaciones generales acerca de las raíces de la ecuaciún xe — 1 = 0, la que tambien abarca el caso en que e es un número compuesto.

1. Estas raíces estan dadas (como se sabe de los libros elementales) por cos pp +i sen pp, donde para k tomamos los e números 0, 1, 2, 3, ...e—1 o cualesquiera otros que sean congruentes a estos segun el modulo e. Una raúz, para k = 0 o para cualquier k divisible por e serú = 1. Para cualquier otro valor de k serú una raúz que es diferente de 1.
2. Puesto que (cos pp + i sen pp )λ = cos AE + i sen Ap, es claro que si R es una tal raúz correspondiente a un valor de k que es primo relativo a e, entonces en la progresiún R, R2, R3, etc., el e-esimo termino serú = 1 y todos los valores antecedentes son diferentes de 1. Se sigue inmediatamente que todas las e cantidades 1, R, R2, R3, . ..Re-1 son diferentes y, ya que todas ellas satisfacen la ecuacion xe — 1=0, ellas darán todas las raíces de esta ecuacion.
3. Finalmente, bajo la misma suposicion, la suma

1 + RA + R2A ··· + RA(e-1) = 0

1 ολβ

para cualquier valor del entero λ no divisible por e. Por esto es = 1-ÑÜ y el numerador de esta fraccion es = 0, pero el denominador no es = 0. Cuando λ es divisible por e, la suma obviamente = e.

360.

Sea n, como siempre, un número primo, g una raíz primitiva para el módulo n, y n — 1 el producto de tres enteros positivos α, β y γ. Por brevedad incluiremos en este los casos en que α o γ = 1. Cuando γ = 1, reemplazamos las sumas (γ, 1), (γ, g), etc. por las raíces [1], [g], etc. Supongamos por lo tanto que todas las α sumas de βγ terminos (βγ, 1), (βγ, g), (βγ^2) y (βγ^α-1) son conocidas y que queremos encontrar las sumas de γ terminos. Hemos reducido la operación anterior a una ecuacion mixta de grado β. Ahora mostraremos como resolverla mediante una ecuacion pura del mismo grado. Por brevedad en vez de las sumas

(γ, 1), (7.g“), (γ,92“), ... (7,s“e-“)

los cuales estan contenidas en (β,γ, 1), escribiremos a, b, c, . ..m respectivamente. En vez de las sumas

(γ,g), (7,g“+1), ...(γ,9“β-“+Ι)

contenidas en (βγ^) escribiremos a0, b0, . ..m0. Y en vez de

(7,g2), (γ,ϊ"+2),...(7,«“β-“+2)

escribiremos a00, b00, ...m00, etc. hasta que se llegue a aquellas que estan contenidas en (βγ, ga-1).

I. Sea R una raíz arbitraria de la ecuacion xe — 1 = 0 y supongamos que la potencia de grado β de la funcion

t = a + Rb + R2c + ··· + Re-1m

es, de acuerdo con las reglas del artículo 345,

N + Aa + Bb + Cc ··· + Mm + A0a0 + B0b0 + C0c0 ··· + M0m0 + A00a00 + B00b00 + C00c00 ··· + M00m00 + etc. = T

donde todos los coeficientes N, A, B, A0, etc. son funciones racionales enteras de R. Suponganse tambien que las β-esimas potencias de las otras dos funciones

u = Re a + Rb + R2c ··· + Re-1m y u0 = b + Rc + R2d ··· + Re-2m + Re-1a

se hacen respectivamente U y U'. Es fácil ver del artículo 350 que, puesto que u' resulta de reemplazar las sumas a, b, c, ...m con b, c, d, ...a, tenemos

U' = N + Ab + Bc + Cd ■■■ + Ma + Ab' + B'c' + Cd ·· · + M'a'

+ *A'b''* + *B* 'V + *C''d' ■■■* + *M" a"*

+ etc.

Tambien es claro que u = Rur y luego U = Re U'. Ya que Re = 1, los coeficientes correspondientes en U y U' serán iguales. Finalmente, ya que t y u difieren solamente en cuanto a que a se multiplica por la unidad en t y por Re en u, todos los coeficientes correspondientes (i.e., aquellos que multiplican las mismas sumas) en T y en U, serán iguales, y así tambien los coeficientes correspondientes en T y en U'. Por lo tanto A = B = C etc. = M; A = B' = C etc.; A' = B" = C' etc.; en T se reduce a una forma como

*N* + *A(βΊ,* 1) + *A^, g)* + *A'(βY, g2)* + erá.

donde los coeficientes individuales N, A, A, etc. son de la forma

*pRe-1* + *p'Re-2* + *p''Re*-3 + etc.

de tal forma que p, p', p'', etc. son enteros dados.

II. Si se toma por R una raíz determinada de la ecuación xe — 1 = 0 (suponemos que ya tenemos sus soluciones) de tal manera que ninguna potencia menor que la βrásima potencia es igual a la unidad, T tambien sera una cantidad determinada, y de esto es posible derivar t mediante la ecuacion pura te—T = 0. Pero, puesto que esta ecuacián tiene β raíces que son t, Rt, R2t, ...Re-1t, puede existir una duda sobre cual de las raíces debe ser escogida. Sin embargo, esto es arbitrario como se mostrara. Recuerdese que, despues de que todas las sumas de βγ terminos están determinadas, la raíz [1] se define como cualquiera de las βγ raíces contenidas en (βγ, 1), que luego debe ser denotada por este símbolo. Así es completamente arbitrario cual de las β sumas que conforman (βγ, 1) queremos designar por a. Si despues de que una de estas sumas se expresa por a, se supone que t = T, es facil ver que la suma que se designaba por b puede ser cambiada a a y lo que anteriormente fue c, d, ...a, b ahora se convierte en b, c, ...m, a, y el valor de t es ahora = R = TRe-1.

Similarmente, si conviene hacer a igual a la suma que en un principio fue c, el valor de t se convierte en TR'3-2 y así sucesivamente. Así, t puede considerarse igual a cualquiera de las cantidades T, TR'3-1, TR'3-2, etc., i.e., a cualquier raíz de la ecuación χβ — T = 0, de acuerdo con que una u otra de las sumas en (βγ, 1) sea expresada por (γ, 1). Q. E. D.

1. Despues de que la cantidad t ha sido determinada de esta forma, hay que determinar las otras β — 1 que resultan de t sustituyendo R sucesivamente por R2, R3, R4, ...R@, esto es

t0 = a + R2b + R4c ■■■ + R2/9-2m, t" = a + R3b + R6c ■■■ + R3/9-3m, etc.

La ultima de estas ya se conoce, porque ella evidentemente = a + b + c■■■ + m = (βγ, 1); las otras pueden encontrarse de la siguiente forma. Por los preceptos del artículo 345 se puede encontrar el producto t^-2t0 tal como t en I. Entonces usamos un míetodo tal como el precedente para mostrar que de esto, se puede reducir a una forma

N + Α(βγ, 1) + Α0(βγ, g) + Α00(βγ, g2) etc. = T0

donde N, A, A0, etc. son funciones racionales enteras de R y así T0 es una cantidad conocida y t0 = ——r-. Exactamente de la misma manera se encuentra T00 por el cólculo del producto t^-3t00. Esta expresión tendró una forma similar y puesto que su valor

■ ■ q 100 3 999

es conocido se deriva la ecuación t = ——^. Entonces t puede ser encontrado de la

ecuación

*... — 000...*

t = — donde T es asimismo una cantidad conocida, etc.

Este metodo no sería aplicable si fuera t = 0, porque entonces T = T0 = T00 etc. = 0. Pero se puede mostrar que esto es imposible, aunque la demostración es tan larga que es necesario omitirla aquó. Tambien existen algunos artificios especiales para convertir las fracciones —, ——-, etc. en funciones racionales enteras de R y algunos metodos mós cortos, en el caso donde α = 1, para encontrar los valores de t0, t00, etc., pero no los consideramos aquó.

1. Finalmente, una vez encontrados t, t0, t00, etc., observando III del artóculo precedente, resulta inmediatamente que t + t0 + t00 + etc. = βα. Esto da el valor de a y de esto, por el artóculo 346, se pueden derivar los valores de todas las restantes sumas de γ terminos. Los valores de b, c, d, etc. tambien pueden ser encontrados, como lo mostrara una pequeña investigation, de las ecuaciones siguientes:

βb = R^-1t + R^-2t0 + R^-3t00 + etc. βc = R2/3-2t + R2/3-4t0 + R2/3-6t00 + etc. βd = R3d-3t + R3d-6t0 + R3d-9t00 + etc., etc.

Entre el gran número de observaciones que podemos hacer concernientes a la discusión precedente enfatizamos solamente una. Con respecto a la soluciún de la ecuaciúon pura xe — T = 0, es claro que en muchos casos T tiene el valor imaginario P + iQ, así la solución depende en parte de la division de un angulo (cuya tangente = Q), en parte de la división de una razón (uno a y/P2 + Q2) en β partes. Es

notable (no proseguiremos con este tema aquí) que el valor de ^P2 + Q2 siempre puede ser expresado racionalmente mediante cantidades ya conocidas. Así, excepto por la extracción de una raíz cuadrada, la única cosa que se requiere para una solucion es la division del óngulo, e.g., para β = 3 solamente la triseccion de un angulo.

Finalmente, puesto que nada nos impide hacer α = 1, γ = 1 y de este modo β = n — 1, es evidente que la solución de la ecuacion xn — 1=0 puede ser reducida inmediatamente a la solución de una ecuación pura xn-1 — T = 0 de grado n — 1. Aquó T se determinara por las rames de la ecuación xn-1 — 1 = 0. Como un resultado, la division del circulo completo en n partes requiere, 1o, la division del circulo completo en n — 1 partes; 2o, la división de otro arco en n— 1 partes, el cual puede ser construido tan pronto como la primera división este hecha; 3o, la extraccion de una raóz cuadrada y se puede mostrar que siempre es -^/ñ.

Aplicación de lo anterior a funciones trigonomútricas.

Método para encontrar los angulos de raúces particulares en Ω.

361.

Falta examinar mas de cerca la conexión entre las rames Ω y las funciones

trigonometricas de los óngulos —, —, —, ... -—n^-. El metodo usado para encontrar

las rames de Ω (a menos que consultemos tablas de senos, pero esto sería menos

directo) deja incierto cuales rames corresponden a los óngulos individuales; i.e., cuól p p 2p 2p

raóz = cos + i sen —, cual = cos + i sen —, etc. Pero esta incertidumbre se

n n n n

puede eliminar fócilmente reflexionando que los cosenos de los angulos —, , 0—— ,

... (n 2n)— estan decreciendo continuamente (tomando en cuenta los signos) y que los senos son positivos. Por otro lado los angulos (n n1)—, (n n2)—, (n n3)—, ... (u+2—)— tienen los mismos cosenos que los de antes, pero los senos son negativos, aunque tienen los mismos valores absolutos. Por lo tanto, de las raíces Ω, las dos que tienen la mayor parte real (son iguales una a la otra) corresponden a los angulos —, (n n1)—. La primera tiene positivo el coeficiente de i, la segunda lo tiene negativo. De las n — 3 raíces restantes, aquellas que tienen la mayor parte real corresponden a los angulos

, y así sucesivamente. En tanto que se conozca la raíz correspondiente al ángulo P, las correspondientes a los restantes angulos se pueden determinar a partir de ella porque, si suponemos que es = [λ], las raíces [2λ], [3λ], [4λ], etc. corresponderán a los ángulos ^, etc. Así en el ejemplo del artículo 353 vemos que la raíz correspondiente al angulo Jg P debe ser [11] y [8] la del angulo P. Similarmente las raíces [3L [16L [14L [5], etc. corresponderan a los íngulos jj P, 17 P, J9P, J6P, etc. En el ejemplo del artículo 354 la raíz [1] corresponderá al angulo J7P, [2] al angulo J7P, etc. De esta forma los cosenos y senos de los íngulos P, 2E., etc. serán completamente determinados.

*Se derivan tangentes, cotangentes, secantes y cosecantes  
a partir de senos y cosenos sin división.*

362.

Con respecto a los restantes funciones trigonometricas de estos angulos, pudieron, por supuesto, derivarse de los cosenos y senos correspondientes mediante míetodos ordinarios bien conocidos. Así secantes y tangentes se pueden encontrar dividiendo respectivamente la unidad y el seno por el coseno; cosecantes y cotangentes dividiendo la unidad y el coseno por el seno. Pero a menudo sera mucho mís ítil obtener las mismas cantidades con la ayuda de las siguientes formulas, usando sílo adiciín y ninguna division. Sea ω uno cualquiera de los íngulos P, ... n1)P y

sea cos ω + i sen ω = R, de modo que R sera una de las raíces Ω, entonces

cos ω =

2(r+R)

1 + R22R

sen ω =

— (R

2iv

R)

i(1 - R2)

2R

y de esto

sec ω =

2R

1 + R2 ’

tan ω =

i(1 - R2)

1 + R2 ’

csc ω =

2Ri

R2 - 1 ’

cot ω =

i(R2 + 1)  
R2- 1

Ahora mostraremos como transformar los numeradores de estas cuatro fracciones de modo que sean divisibles por los denominadores.

I. Ya que R = Rn+1 = R2n+1 tenemos 2R = R + R2n+1. Esta expresión es divisible por 1 + R2 pues n es un nímero impar. Así tenemos

sec ω = R - R3 + R5 - R7 ··· + R2n-1

y así (puesto que senω = — sen(2n — 1)ω, sen3w = — sen(2n — 3)ω etc. tenemos sen ω — sen 3ω + sen 5ω ··· + sen(2n — 1)ω = 0)

sec ω = cos ω — cos 3ω + cos 5ω ··· + cos(2n — 1)ω  
o finalmente (ya que cos ω = cos(2n — 1)ω, cos 3ω = cos(2n — 3)ω, etc.)

= 2(cos ω — cos 3ω + cos 5ω ··· ^ cos(n — 2)ω) ± cos ηω

los signos superiores o inferiores se tomarán de acuerdo con que n sea de la forma 4k + 1 o 4k + 3. Obviamente esta formula tambien se puede expresar como

secω = ± 1 — 2cos 2ω + 2 cos 4ω ··· ± 2cos(n — 1)ω)

II. Similarmente, sustituyendo 1 — R2 por 1 — R2n+2 resulta

tan ω = i(1 — R2 + R4 — R6 ··· — R2n)

(ya que 1 — R2n = 0, R2 — R2n-2 = 2i sen 2ω, R4 — R2n-4 = 2i sen4ω, etc.) tan ω = 2^ sen 2ω — sen 4ω + sen 6ω ··· ^ sen(n — 1)ω^

III. Puesto que 1 + R2 + R4 — · + R2n-2 = 0, tenemos

η = n — 1 — R2 — R4 ··· — R2n-2 = (1 — 1) + (1 — R2) + (1 — R4) ··· + (1 — R2n-2)

y cada uno de sus terminos es divisible por 1 — R2. Así

=1 + (1 + R2) + (1 + R2 + R4) ··· + (1 + R2 + R4 ··· + R2n-4) = (n — 1) + (n — 2)R2 + (n — 3)R4 ··· + R2n-4

Multiplicando por 2 y restando la cantidad

0 = (n — 1)(1 + R2 + R4 ··· + R2n-2)

y asimismo multiplicando por R tenemos 2 nR

= (n — 1)R + (n — 3)R3 + (n — 5)R5 ··· — (n — 3)R2n-3 — (n — 1)R2n-1

1 R2

y de esto inmediatamente obtenemos

csc ω = — ((— — 1) sen ω + (— — 3) sen 3ω ■■■ — (— — 1) sen(2— — 1)ω) 2

= -((— — 1) sen ω + (— — 3) sen 3ω + etc. + 2 sen(— — 2)ω)

Esta fórmula puede ser expresada tambien como 2

^2sen 2ω + 4 sen 4ω + 6 sen 6ω ■■■ + (— — 1) sen(— — 1)ω)

csc ω = — -

—

1. Multiplicando el valor de jzRz, dado antes, por 1 + R2 y restando la cantidad

0 = (— — 1)(1 + R2 + R4 ■■■ + R2n-2)

tenemos

—(1 + R2)  
1- R2

= (— — 2)R2 + (— — 4)R4 + (— — 6)R6 ■■■ — (— — 2)R

2*n—2*

cot ω = — ((— — 2) sen 2ω + (— — 4) sen4ω + (— — 6) sen 6ω ■■■ — (— — 2) sen(— — 2)ω) 2

y de esto sigue inmediatamente que 1

= — ((— — 2) sen 2ω + (— — 4) sen 4ω ■■■ +3 sen(— — 3)ω + sen(— — 1)ω)

y esta formula tambien se puede expresar como

2

cot ω = ( sen ω + 3 sen 3ω ■■■ + (— — 2) sen(— — 2)ω)

*Método de reducir sucesivamente las ecuaciones para funciones trigonométricas.*

363.

Suponiendo otra vez que — — 1 = ef, la función X puede ser resuelta en e factores de grado f en tanto que se sepan los valores de todas las e sumas de f terminos (art. 338). De la misma manera, suponiendo que Z = 0 es una ecuación de grado — — 1 cuyas raíces son los senos o cualquiera otra funcion trigonometrica de los

ángulos F... n1)F, la función Z se puede resolver en e factores de grado f de

la siguiente forma.

Sea Ω el conjunto de los e períodos de f terminos (f, 1) = P, P', P", etc. Sea P el período de las raíces [1], [a], [b], [c], etc.; P' el de las raíces [a0], [b0], [c0], etc.; P00 el de las raíces [a00], [b00], [c00], etc., etc. Sea el angulo ω correspondiente a la raíz [1], y así los ángulos αω, bω, etc. a las raíces [a], [b], etc.; los angulos α0ω, b/ω, etc. a las raíces [a0], [b0], etc.; los ángulos α00ω, ^0ω, etc. a las raíces [a00], [b00], etc. Es fícil ver que todos estos angulos tomados juntos coinciden, con respecto a sus funciones trigonometricas[[227]](#footnote-228)), con los íngulos F, 2T, , ... n1)F. Ahora si se

denota la funcion que se trata por el carácter φ prefijado al íngulo, y si Y es el producto de los e factores

x — φω, x — φ^ω, x — φδω etc.

y el producto de los factores x — φ^0ω, x — φ^0ω, etc. = Y0, el producto de x — φ^00ω, x—φ^00ω, etc. = Y00 etc.: entonces necesariamente el producto YY0Y00 ··· = Z. Resta ahora mostrar que todos los coeficientes en las funciones Y, Y0, Y00, etc. pueden ser reducidos a la forma

A + B(f, 1) + C(f, g) + D(f,g2) ··· + L(f, ge-1)

Hecho esto, evidentemente todos ellos serín conocidos en tanto se conozcan los valores de todas las sumas de f terminos: mostramos esto de la siguiente forma.

Tal como cos ω = [1] + ^ [1]n-1, sen ω = — 2i[1] + 2i[1]n-1 así por el artículo precedente todas las restantes funciones trigonomíetricas del íangulo ω se pueden reducir a la forma A + B[1] + C[1]2 + D[1]3 + etc. y no es difícil ver que la funciín del íngulo kω se hace = A + B[k] + C[k]2 + D[k]3 + etc. donde k es cualquier entero. Ahora, puesto que los coeficientes individuales en Y son funciones racionales enteras invariables de φω, φ^ω, φ^ω, etc., si se sustituyen sus valores por estas cantidades, sus coeficientes individuales se convertirán en funciones racionales enteras invariables de [1], [a], [b], etc. Por lo tanto, por el artículo 347, ellas se reducirán a la forma A + B(f, 1) + C(f, g) + etc. Los coeficientes en Y0, Y00, etc. tambien pueden ser reducidos a formas similares. Q. E. D.

364.

Agregamos unas pocas observaciones acerca del problema del artículo prece­dente.

1. Los coeficientes individuales en Y' son funciones de raíces contenidas en el período P' = (f,a') tal como las funciones de las raíces en P dan los coeficientes correspondientes en Y. Es claro del artículo 347, por lo tanto, que se puede derivar Y' de Y, sustituyendo en todo lugar en Y las cantidades (f, 1), (f, g), (f, g2), etc. por (f, a'), (f, a'g), (f, a'g2), etc. respectivamente. Igualmente Y'' puede ser derivado de Y, sustituyendo en todo lugar en Y las cantidades (f, 1), (f, g), (f,g2), etc. por (f, a''), (f, a''g), (f, a''g2), etc. respectivamente, etc. Por consiguiente, en tanto que se tenga la función Y, las restantes Y', Y'', etc. siguen facilmente.
2. Suponiendo

Y = xf — axf 1 + 2 — etc.

los coeficientes α, β, etc. son respectivamente la suma de las raíces de la ecuacion Y = 0, i.e., de las cantidades φω, φαω, φ&ω, etc., la suma de sus productos tomados dos a dos, etc. Pero a menudo estos coeficientes se encontraran mucho mas comodamente por un metodo similar al del artículo 349, esto es, calculando la suma de las raíces φω, ^αω, φ&ω, etc., la suma de sus cuadrados, cubos, etc. y deduciendo de esto por el teorema de Newton esos coeficientes. Siempre que φ designe la tangente, secante, cotangente o cosecante se dan aún otros metodos de abreviacion del proceso, pero no podemos considerarlos aquí.

1. El caso donde f es un nímero par merece consideration especial porque entonces cada uno de los períodos P, P', P'', etc. estará compuesto de ^f períodos de dos terminos. Si P consiste de los períodos (2, 1), (2, a), (2, b), (2, c), etc., entonces los nímeros 1, a, b, c, etc. y n — 1, n — a, n — b, n — c, etc. tomados en conjunto coincidirán con los numeros 1, a, b, c, etc. o al menos (esto viene a ser la misma cosa) serán congruentes a ellos segun el modulo n. Pero ^>(n — 1)ω = ±φω, ^>(n — α)ω = ±φαω etc., donde los signos superiores son tomados cuando φ designa el coseno o la secante, los inferiores cuando φ designa el seno, la tangente, la cotangente o la cosecante. Se sigue de esto que en los dos primeros casos, los factores que componen Y seran iguales dos a dos, y así Y es un cuadrado y sera = y2 si y se pone igual al producto de

x — φω, x — φαω, x — φbω etc.

En los mismos casos, las funciones restantes Y', Y'', etc. serán cuadrados, y suponiendo que P' esta compuesto de (2, a'), (2, b'), (2, c'), etc.; P'' de (2, a''), (2, b''), (2, c''), etc., etc., el producto de x — φα'ω, x — φάω, x — φΡω, etc. = y', el producto de x — φα''ω, x — φά''ω, etc. = y'', etc., entonces Y' = y' , Y'' = y'' , etc.; y la función Z tambien sera un cuadrado (cf. antes, art. 337) y sus raíces serán iguales al producto de y, y', y'', etc. Pero claramente y', y'', etc. pueden ser derivadas de y tal como dijimos en I que Y',Y'' son derivadas de Y. Luego, los coeficientes individuales en y tambien pueden ser reducidos a la forma

A + 1) + C (/ g) + etc.

porque las sumas de las potencias individuales de las raíces de la ecuacion y = 0 son iguales a la mitad de las sumas de las potencias de las raíces de la ecuacion y = 0 y así son reducibles a una forma tal. En los cuatro casos posteriores sin embargo, Y seraí el producto de los factores

x2 — (φω)2, x2 — (φαω)2, x2 — (φάω)2 etc.

xf — Axf 2 + ^xf 4 — etc.

y así de la forma

Es claro que los coeficientes A, μ, etc. pueden ser deducidos de las sumas de cuadrados, bicuadrados, etc. de las raíces φω, φαω, φάω, etc. La misma cosa es cierta para las funciones Y', Y'', etc.

Ejemplo. I. Sea n =

Z = (x8 +— x7 — 7 x6 v 2 4

17, f = 8 y φ el coseno. Entonces resulta

3 5 , 15 ■4 , 5 „,3 5 J2 1

1

x5 + x4 + x3 x2 x + )

4

2

16

16

32

32 256

y así VZ serí resuelta en dos factores y, y' de grado cuatro. El período P = (8,1) consiste de (2, 1), (2, 9), (2, 13) y (2, 15); así y sera un producto de los factores

x — φω, x — φ9ω

Sustituyendo φΡω por ^ [k] + 2 [n — k]

, x — φ13ω se encuentra

, x — φ15ω que

φω + φ9ω + φ13ω + φ15ω (φω)2 + (φ9ω)2 + (φ13ω)2 + (φ15ω)2

1)

1

2+4(8,1)

Asimismo la suma de los cubos es = 3 (8,1) + 8 (8, 3) y la suma de los bicuadrados es = 12 + 16(8,1). Así por el teorema de Newton los coeficientes en y serán

y = x4 - 1(8,1)x3 + 1 ((8,1) + 2(8, 3))x2 - 8 ((8,1) + 3(8,3))x + ^ ((8,1) + (8, 3))

(MvU)\*2+(4+b/ü)

(3 — 1 ^)x2 + — 8 A7)

e y0 es derivado de y intercambiando (8,1) y (8, 3). Por lo tanto sustituyendo (8,1) y (8, 3) por los valores — 2 + 2λ/Ϊ7 y — 2 — 2λ/Ϊ7, obtenemos

y = x4 + (j— 1 dux3 y0 =x4 + (j + 4 cüe3

x

x

1

16

1

16

Similarmente λ/Z se puede resolver en cuatro factores de grado dos. El primero será (x — φω)^ — φ13ω), el segundo (x — ^>9^)(x — φ15ω), el tercero (x — φ3ω)^ — φ5ω), el cuarto (x — <£>10^)(x — φ11ω), y todos los coeficientes en estos factores pueden ser expresados en terminos de las cuatro sumas (4, 1), (4,9), (4,3) y (4,10). Evidentemente el producto del primer factor por el segundo factor sera y, el producto del tercero por el cuarto sera y0.

Ejemplo. II. Si, con todo lo demas igual, se supone que φ representa el seno, de modo que

Z = x26 — II x14 + 119 x12 —

4 16

221 xio + 235 x8 561 t6 ,^57 ,

32 + 256 512 + 2048

51 2 17

x2 +

4096 65536

ha de ser resuelto en dos factores y e y0 de grado 8, entonces y será un producto de cuatro factores cuadrados

x2 — (φω)2, x2 — (φ9ω)2, x2 — (φ13ω), x2 — (φ15ω)2

Ahora, ya que φΑω = — 2i[k] + 2i[n — k], resulta

(φΑω)2 = — 4[2k] + 2[n] — 4[2n — 2k] = 2 — 4[2k] — l[2n — 2k]

Así, la suma de los cuadrados de las raíces φω, φ9ω, φ13ω, φ15ω sera 2 — 2 (8, 1), la suma de sus cuartas potencias = 3 — 26(8, 1), la suma de sus sextas potencias

= 5 — 64(8, 1) — 64(8, 3), la suma de sus octavas potencias 35 — 256(8, 1) — 32(8, 3). Por lo tanto

y = X8 — (2 — 4(8, 1)2χ6 + (3

2 16

5 (8,1) + 8(8, 3))x4

9 5 ) „ 15 3

(8,1) + 64(8,3))x +^ — 256(8,1) + 256(8,3)

64

e y0 es determinado a partir de y intercambiando (8, 1) y (8, 3), así, sustituyendo los valores de estas sumas obtenemos

8

y = x

/

y

8

= X

(f — 8 A7)x6

,17 1

— -vT7)~4

32 32 7

51 7

X

(U — U^17)x2 +

v32 64

(— + ^/17)x6 + (— + —λ/Ϊ7)

88

32 32

X

17 7

(— + —λ/Ϊ7)χ2 +

32 64

17 \_

256 — 17

256 +

1

64

1

64

λ/17

^17

Así Z puede ser resuelto en cuatro factores cuyos coeficientes se pueden expresar por sumas de cuatro terminos. El producto de dos de ellos sera y, el producto de los otros dos sería y0.

*Secciones del circulo que pueden realizarse por ecuaciones cuadráticas  
o sea por construcciones geométricas.*

365.

Así, si n es un número primo, por la discusión precedente hemos reducido la division del círculo en n partes a la solucion de tantas ecuaciones como factores haya en el número n— 1. El grado de la ecuacion se determina por el tamaño de los factores. Por lo tanto, siempre que n — 1 es una potencia del número 2, lo que ocurre cuando el valor de n es 3, 5, 17, 257, 65537, etc., la divisiún del círculo se reduce a ecuaciones cuadrúticas únicamente, y las funciones trigonometricas de los angulos P, 2E, etc. pueden ser expresadas por raúces cuadradas que son mas o menos complicadas (de acuerdo con el tamano de n). Asú, en estos casos la division del cúrculo en n partes o la inscripcion de un polígono regular de n lados puede ser efectuada por construcciones geometricas. Asú, e.g., para n = 17, por los artículos 354 y 361 se deriva la siguiente expresión para el coseno del angulo 47 P:

1

16

+

4W34 — 2^17 + 8\/17 + 3νΪ7 —^34 16

1

8

2vT7 — 2\J 34 + 2vT7

El coseno de múltiplos de este ángulo tendrá una forma similar, pero el seno tendrá un signo radical más. Ciertamente es asombroso que aunque la divisibilidad geometrica del circulo en tres y cinco partes fue conocida ya en los tiempos de Euclides, nada fue agregado a este descubrimiento durante 2000 años. Todos los geometras han asegurado que, excepto por aquellas secciones y las que se derivan directamente de ellas, esto es, division en 15, 3 · 2μ, 5 · 2μ, y 2μ partes, no existen otras que puedan ser efectuadas por construcciones geometricas. Es fácil mostrar que si el námero primo n es = 2m + 1, el exponente m no puede tener otros factores primos excepto 2, y así es igual a 1 o 2 o una potencia mayor del numero 2. Pues si m fuera divisible por algán námero impar ζ (mayor que la unidad) de modo que m = ζη, entonces 2m + 1 sería divisible por 2n + 1 y asá necesariamente compuesto. Todos los valores de n, que pueden ser reducidos a ecuaciones cuadráticas esrán, por consiguiente, contenidos en la forma 22 +1. Asá, los cinco numeros 3, 5, 17, 257, 65537 resultan de hacer ν = 0, 1, 2, 3, 4 o m =1, 2, 4, 8, 16. Pero la division geometrica del cárculo no puede ser efectuada para todos los námeros contenidos en la formula sino solamente para aquellos que son primos. Fermat fue engañado por su induccián y afirmá que todos los nuámeros contenidos en esa forma son necesariamente primos, pero el distinguido Euler notá primero que esta regla es erránea para ν = 5 o sea m = 32, puesto que el námero 232 + 1 = 4294967297 contiene el factor 641.

Siempre que n — 1 contenga otros factores primos distintos de 2, somos llevados a ecuaciones de mayor grado, a saber, a una o mas ecuaciones cubicas cuando 3 aparece una o varias veces entre los factores primos de n — 1, a ecuaciones de quinto grado cuando n — 1 es divisible por 5, etc., PODEMOS PROBAR CON TODO RIGOR QUE ESTAS ECUACIONES DE MAYOR GRADO NO PUEDEN SER ELUDIDAS DE NINGUNA FORMA NI PUEDEN SER REDUCIDAS A ECUACIONES DE MENOR GRADO. Los Emites del presente trabajo excluyen aquá esta demostracián, pero emitimos esta advertencia no sea que alguien intente llevar a cabo otras construcciones geometricas que no son las sugeridas por nuestra teoría (e.g., secciones en 7, 11, 13, 19, etc. partes) y asá gaste su tiempo inuátilmente.

366.

Si un circulo ha de ser cortado en aa partes, donde a es un número primo, evidentemente esto puede ser hecho geometricamente cuando a = 2 pero no para cualquier otro valor de a si α > 1, pues entonces además de las ecuaciones requeridas para la division en a partes, será necesario resolver otras α — 1 de grado a, y estas

no pueden ser evitadas ni reducidas de ninguna manera. Por lo tanto, en general, el grado de las ecuaciones necesarias se puede encontrar de los factores primos del número (a — 1)aa-1 (incluyendo tambien el caso en que α = 1).

Finalmente si el círculo ha de ser cortado en N = aabC ... partes, donde a, b, c, etc. son números primos diferentes, es suficiente hacer divisiones en aa, lP, c7, etc. partes (art. 336). Así, a fin de conocer el grado de las ecuaciones necesarias para este propúosito, es necesario considerar los factores primos de los nuúmeros

(a — 1)aa-1, (b — 1)b^-1, (c — 1)c7-1, etc.

o, lo que viene a ser la misma cosa, los factores de su producto. Se observa que este producto indica el número de enteros primos relativos a N y menores que el (art. 38). Geometricamente, por lo tanto, esta division puede ser realizada solamente cuando este numero es una potencia de 2. Pero cuando los factores incluyen numeros primos diferentes de 2, digamos p, p, etc., entonces las ecuaciones de grados p, p, etc. no pueden ser evitadas. En general, por lo tanto, a fin de poder dividir geometricamente el círculo en N partes, N debe ser 2 o una potencia mas alta de 2, o un numero primo de la forma 2m + 1, o el producto de varios numeros primos de esta forma, o el producto de uno o varios de tales numeros primos por 2 o por una potencia mas alta de 2. En resumen, se requiere que N no incluya factores primos impares que no sean de la forma 2m + 1 ni algun factor primo de la forma 2m + 1 mas que una vez. Los siguientes son los 38 valores de N abajo de 300:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

APENDICE.

Al art. 28. La solución de la ecuación indeterminada ax = by ± 1 no fue encontrada primero por el ilustre Euler (como se consignó en esta Sección) sino por un geometra del siglo diecisiete, Bachet de Meziriac, el celebre editor y comentador de Diofanto. Fue el ilustre Lagrange quien le restituyo este honor (Add. a l’Algebre d’Euler, p. 525, donde a la vez indica el fondo del metodo). Bachet publico su descubrimiento en la segunda edicion del libro Probiemes plaisans et délectables qui se font par les nombres, 1624. En la primera edicion (Lyon, 1612), que fue la ónica que vi, este no fue incluido, aunque fue mencionado.

A los art. 151, 296, 297. El ilustre Legendre presento su demostracion nuevamente en su excelente trabajo, Essai d’une théorie des nombres, p. 214 y siguientes, pero no cambio nada esencial. Así, este metodo todavía esta sujeto a las objecciones contenidas en el artículo 297. Es cierto que el teorema (sobre el cual se basa una suposicion) que establece que cualquier progresion aritmetica l, l + k, l+2k, etc. contiene numeros primos si k y l no tienen un divisor común, se expone mas detalladamente en esta obra (p. 12 y siguientes), pero todavía no parece satisfacer el rigor geometrico. Pero aun si este teorema fuera enteramente demostrado, la segunda suposicion permanece (que existen numeros primos de la forma 4n + 3 para los cuales un numero positivo primo dado de la forma 4n + 1 es un no residuo cuadratico) y yo no se si esto puede ser probado rigurosamente a menos que el teorema fundamental sea asumido. Pero debe observarse que Legendre no asumio tacitamente esta ultima suposicion, ni intento disimularla (p. 221).

A los art. 288-293. El mismo asunto presentado aquí como una aplicación de la teoría de formas ternarias, y que parece ser tan categórico con respecto al rigor y generalidad que nada mas podría desearse, es tratado mucho mas completamente por el ilustre Legendre en la tercera parte de su trabajo, pp. 321-400[[228]](#footnote-229)). El usa principios y míetodos muy diferentes de los nuestros, pero de esta forma encuentra muchas dificultades que le impiden proporcionar una demostración rigurosa a estos notables teoremas. El indica francamente estas dificultades, pero, a menos que yo este equivocado, estas pueden ser mas facilmente dispensadas con la suposición otra vez aquí del teorema cabalmente mencionado en la nota al pie de p. 371 (aquel que comienza “En cualquier progresion aritmetica,” etc.).

Al art. 306 VIII. En el tercer millar de determinantes negativos existen 37 que son irregulares; 18 de ellos tienen 2 como índice de irregularidad, los otros 19 índice 3.

Al art. 306 X. Recientemente hemos tenido exito en resolver completamente las cuestiones propuestas aquí. Publicaremos muy pronto esta discusión en nuestra continuacion del presente trabajo. Ella ilustra brillantemente muchas partes de la Aritmetica y el Analisis superiores. La misma soluciín prueba que el coeficiente m en el artículo 304 es = γπ = 2, 3458847616, donde γ es la misma cantidad que en el artículo 302 y π es la longitud de la mitad de la circunferencia de un círculo de radio 1.

TABLAS

2 . 3 . 5 . 7 . 11 13 . 17 . 19 . 23 . 29 31 . 37 . 41 . 43 . 47 53 . 59 . 61 . 67 . 71 73 . 79 . 83 . 89

3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 1 | 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. | \*. | 5. | 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. | 8. | 4. | 7 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. | 8. | 9. | 7. | 11 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| \* | 3. | 1. | 2. | 1 | 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 . | 11. | 7. | 9. | 13 | 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17 . | 5. | 2. | 12. | 6 | 13 . | 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8. | 20. | 15. | 21. | 3 | 12 . | 17 . | 5 |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. | 7. | \*. | 5. | 16 | 19 . | 13 . | 18 . | 11 |  |  |  |  |  |  |  |  |  |  |  |
| 1. | \*. | 5. | 16. | 13 | 8. | 15 . | 12 . | 11 |  |  |  |  |  |  |  |  |  |  |  |
| 11 . | 27. | 18. | 20. | 23 | 2. | 7. | 15 . | 24 |  |  |  |  |  |  |  |  |  |  |  |
| 12 . | 13. | 20. | 4. | 29 | 23 . | 1. | 22 . | 21 . | 27 |  |  |  |  |  |  |  |  |  |  |
| \* | 3. | 1. | 2. | 5 | 7 . | 4. | 7. | 6. | 3 | 0 |  |  |  |  |  |  |  |  |  |
| 11. | 34. | 1. | 28. | 6 | 13 . | 5. | 25 . | 21 . | 15 | 27 |  |  |  |  |  |  |  |  |  |
| 26. | 15. | 22. | 39. | 3 | 31 . | 33 . | 9. | 36 . | 7 | 28 . | 32 |  |  |  |  |  |  |  |  |
| 39. | 17. | 5. | 7. | 6 | 40 . | 16 . | 29 . | 20 . | 25 | 32 . | 35 . | 18 |  |  |  |  |  |  |  |
| 30. | 18. | 17. | 38. | 27 | 3. | 42 . | 29 . | 39 . | 43 | 5. | 24 . | 25 . | 37 |  |  |  |  |  |  |
| 2. | 13. | 41. | \*. | 16 | 9. | 31 . | 35 . | 32 . | 24 | 7. | 38 . | 27 . | 36 . | 23 |  |  |  |  |  |
| 25. | 9. | 31. | 38. | 46 | 28 . | 42 . | 41 . | 39 . | 6 | 45 . | 22 . | 33 . | 30 . | 8 |  |  |  |  |  |
| 25. | 32. | 34. | 44. | 45 | 23 . | 14 . | 22 . | 27 . | 4 | 7 . | 41 . | 2. | 13 . | 53 | 28 |  |  |  |  |
| 47. | 42. | 14. | 23. | 45 | 20 . | 49 . | 22 . | 39 . | 25 | 13 . | 33 . | 18 . | 41 . | 40 | 51 | 17 |  |  |  |
| \*. | 3. | 1. | 10. | 5 | 15 . | 12 . | 7. | 14 . | 11 | 8. | 9. | 14 . | 13 . | 12 | 5 | 1 | 3 |  |  |
| 29. | 9. | 39. | 7. | 61 | 23 . | 8. | 26 . | 20 . | 22 | 43 . | 44 . | 19 . | 63 . | 64 | 3 | 54 | 5 |  |  |
| 58. | 18. | 14. | 33. | 43 | 27 . | 7. | 38 . | 5. | 4 | 13 . | 30 . | 55 . | 44 . | 17 | 59 | 29 | 37 | 11 |  |
| 8. | 6. | 1. | 33. | 55 | 59 . | 21 . | 62 . | 46 . | 35 | 11 . | 64 . | 4. | 51 . | 31 | 53 | 5 | 58 | 50 . 44 |  |
| 50. | 71. | 34. | 19. | 70 | 74 . | 9. | 10 . | 52 . | 1 | 76 . | 23 . | 21 . | 47 . | 55 | 7 | 17 | 75 | 54 . 33 | 4 |
| 25. | \*. | 35. | 22. | 1 | 38 . | 15 . | 12 . | 5. | 7 | 14 . | 24 . | 29 . | 10 . | 13 | 45 | 53 | 4 | 20 . 33 | 48 . 52 |
| 3. | 52. | 81. | 24. | 72 | 67 . | 4. | 59 . | 16 . | 36 | 32 . | 60 . | 38 . | 49 . | 69 | 13 | 20 | 34 | 53 . 17 | co  -j |
| 72. | 87. | 18. | 7. | 4 | 65 . | 82 . | 53 . | 31 . | 29 | 57 . | 77 . | 67 . | 59 . | 34 | 10 | 45 | 19 | 32 . 26 | 68 . 46 . 27 |
| 86. | 2. | 11. | 53. | 82 | 83 . | 19 . | 27 . | 79 . | 47 | 26 . | 41 . | 71 . | 44 . | 60 | 14 | 65 | 32 | 51 . 25 | 20 . 42 . 91 . 18 |

3

5

7

9

11

13

ι6

17

19

23

25

27

29

31

32

37

41

43

47

49

53

59

61

64

67

71

73

79

8i

83

89

97

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | —1 | +2 | +3 | +5 | +7 | +11 | +13 | +17 | +19 | +23 | +29 | +31 | +37 | +41 | +43 | +47 | +53 | +59 | +61 | +67 | +71 | +73 | +79 | +83 | +89 | +97 |
| 3  5  7  11  13  17  19  23  29  31  37  41  43  47  53  59  6i  67  71  73  79  83  89  97 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | — |

3

7

9

11

13

17

19

23

27

29

31

37

41

43

47

49

53

59

6i

67

71

73

79

8i

83

89

97

(o)... 3; (1)...6

(o)... 142857

(o)...1; (1)...2; (2)...4; (3)...8; (4)...7; (5)...5 (o)... o9; (1)...18; (2)...36; (3)... 72; (4)... 45

(o)... o76923; (1)... 461538

(o)... o588235294 117647 (o)... o526315789 47368421

(o)... o4347826o8 6956521739 13

(o)... o37; (1)...o74; (2)...148; (3)... 296; (4)...592; (5)...185

(o)... o344827586 2o68965517 24137931

(o)... o32258o645 16129; (1)... 548387o967 74193

(o)... o27; (1)... 135; (2)...675; (3)... 378; (4)...891; (5)... 459

(6)... 297; (7)...486; (8)...432; (9)... 162; (lo)...8l0; (11)...o54

(o)... o2439; (1)... 14634; (2)... 878o4; (3)... 26829; (4)... 6o975; (5)... 65853; (6)... 95121; (o)... o232558139 53488372o9 3; (1)... 65116279o6 976744l86o 4

(7).. . 7o731

.28395o617

(o)... o212765957 4468o85lo6 3829787234 ^553^4 893617

(o)... o2o4o81632 653o612244 8979591836 7346938775 51

(o)... o188679245 283; (1)... 49o566o377 358; (2)... 75471¾811 32°; (3)... 6226415o94 339 (o)... o169491525 4237288135 59322o3389 83o5o84745 7627118644 o6779661

(o)...o163934426 2295o81967 213114754o 9836o65573 77o4918o32 7868852459

(o)... o149253731 343283582o 89552238^ 597; (1)... 1791o44776 1194o2985o 7462686567 164

(o)... o14o845o7o 4225352112 ^^33^ 28169; (1)... 8732394366 197183o985 9154929577 46478

(o)... o1369863; (1)... o6849315; (2)... 34246575; (3)... 71232876; (4)... 56164383

(5)... 8o821917; (6)... o41o9589; (7).. . 2o547945; (8)... o2739726

(o)... o126582278 481; (1)... 367o886o75 949; (2)... 645569feo2 531

(3)... 7215189873 417; (4)... 924o5o6329 113; (5)... 7974683544 3o3

(o)... o12345679; (1)... 1358o2469; (2)... 493827l6o; (3)... 432o98765; (4)... 753o86419; (5)..

1. ...o12o481927 71o8433734 939759o361 4457831325 3
2. ...6o24o96385 5421686746 9879518o72 2891566265 o
3. ... o11235955o 5617977528 o8988764o4 494382o224 7191
4. ... 337o786516 8539325842 6966292134 83146o6741 573o

(o)... o1o3o92783 5o51546391 7525773195 8762886597 9381443298 969o721649 484536o824 742268o412 371134o2o6 185567

CONTENIDOS.

Dedicación p. 1

[Prefacio p. 3](#bookmark8)

Sección Primera. De la congruencia de los números en general p. 7

Números congruentes, modulos, residuos y no residuos, art. 1 Residuos mínimos, art. 4

Proposiciones elementales sobre congruencias, art. 5 Algunas aplicaciones, art. 12

Sección Segunda. Sobre las congruencias del primer grado p. 13

Teoremas preparatorios sobre los números primos, factores, etc., art. 13 La resolución de las congruencias del primer grado, art. 26 Acerca de la busqueda de un número congruente a un numero dado segun un moúdulo dado, art. 32

Congruencias lineales con varias incognitas, art. 37 Varios teoremas, art. 38

Sección Tercera. Sobre residuos de las potencias p. 38

Los residuos de los terminos de una progresiún geometrica que comienza desde la unidad constituyen una serie perioúdica, art. 45 Se consideran primero los módulos que son números primos.

El numero de terminos en el período es un divisor de p — 1 si el múdulo = p, art. 49

El teorema de Fermat, art. 50

Cuantos números corresponden a un período, en el cual el número de terminos

es un divisor dado del número p — 1, art. 52

Raíces primitivas, bases e índices, art. 57

Algoritmos de los índices, art. 58

Sobre las raíces de la congruencia xn = A, art. 60

La conexiún entre los indices en sistemas diferentes, art. 69

Bases adaptadas para usos especiales, art. 72

Metodo para la determinaciún de las raíces primitivas, art. 73

Varios teoremas sobre los períodos y las raíces primitivas, art. 75

(El teorema de Wilson, art. 76)

Sobre los modulos que son potencias de nímeros primos, art. 82 Modulos que son potencias de 2, art. 90 Modulos compuestos de varios primos, art. 92

SECCION Cuarta. Sobre las congruencias de segundo grado p. 73

Residuos y no residuos cuadraticos, art. 94

Cuando el modulo es un numero primo, el nímero de residuos menores que el mídulo es igual al nímero de no residuos menores, art. 96 La cuestiín de si un nímero compuesto es un residuo o un no residuo de un nímero primo dado depende de la naturaleza de los factores, art. 98 Sobre los modulos que son nímeros compuestos, art. 100

Criterio general sobre si un nímero dado es un residuo o un no residuo de un nímero primo dado, art. 106

Investigaciones sobre los nímeros primos cuyos residuos o no residuos sean

nímeros dados, art. 107

Residuo —1, art. 108

Residuos +2 y —2, art. 112

Residuos +3 y —3, art. 117

Residuos +5 y —5, art. 121

Sobre ±7, art. 124

Preparaciín para la investigación general, art. 125

Por inducción se apoya un teorema general (fundamental), y se deducen algunas conclusiones de el, art. 130

Demostración rigurosa del teorema fundamental, art. 135

Metodo analogo para la demostración del teorema del art. 114, art. 145

La resolution del problema general, art. 146

Sobre las formas lineales que contienen todos los nómeros primos de los cuales un nómero dado cualquiera es un residuo o no residuo, art. 147 Sobre los trabajos de otros acerca de estas investigaciones, art. 151 Sobre las congruencias no puras del segundo grado, art. 152

SECCION Quinta. Sobre las formas y las ecuaciones indeterminadas de

segundo grado p. 121

Propósito de la investigación: definition y notación de las formas, art. 153 Representación de los números; el determinante, art. 154

Los valores de la expresión Vb2 — ac (mod. M) a los cuales pertenece la representation del nómero M por la forma (a, b,c), art. 155 Una forma que implica otra o contenida en ella; la transformation propia e impropia, art. 157

La equivalencia propia e impropia, art. 158 Formas opuestas, art. 159 Formas contiguas, art. 160

Divisores comunes de los coeficientes de las formas, art. 161

El nexo de todas las transformaciones semejantes de una forma dada en otra

forma, art. 162

Formas ambiguas, art. 163

Teorema sobre el caso en que una forma esta contenida en otra al mismo tiempo propia e impropiamente, art. 164

Generalidades sobre las representaciones de los numeros por las formas y su

nexo con las transformaciones, art. 166

Sobre las formas de un determinante negativo, art. 171

Aplicaciones especiales a la descomposicion de los nómeros en dos cuadrados, en un simple y un doble cuadrado, en un simple y un triple cuadrado, art. 182 Sobre las formas de un determinante positivo no cuadrado, art. 183

Formas de determinante cuadrado, art. 206

Formas contenidas en otras a las cuales no son equivalentes, art. 213 Formas con determinante 0, art. 215

Solución general de toda ecuación indeterminada de segundo grado con dos incognitas, art. 216 Anotaciones historicas, art. 222

*Investigaciones ulteriores sobre las formas*

Distribution de formas de un determinante dado en clases, art. 223

Distribution de clases en órdenes, art. 226

La partición de órdenes en generos, art. 228

Sobre la composición de formas, art. 234

Composition de ordenes, art. 245

Composition de generos, art. 246

Composición de clases, art. 249

Para un determinante dado existe el mismo número de clases en cada genero del mismo orden, art. 252

Se comparan el nuómero de clases contenidas en góeneros individuales de óordenes distintos, art. 253

Sobre el nómero de clases ambiguas, art. 257

La mitad de todos los caracteres asignables para un determinante dado no puede pertenecer a un genero propiamente primitivo (positivo para un determinante negativo), art. 261

Una segunda demostración del teorema fundamental y de los demas teoremas acerca de los residuos -1, +2, -2, art. 262

Se determina mas exactamente la mitad de los caracteres que no pueden corresponder a ninguón góenero, art. 263

Un metodo especial para descomponer primos en dos cuadrados, art. 265 *Una digresión conteniendo un estudio de formas ternarias,* art. 266 *Algunas aplicaciones a la teoría de las formas binarias.*

Para encontrar una forma cuya duplicacioón produce una forma binaria dada del góenero principal, art. 286

Todos los caracteres, salvo aquéllos mostrados como imposibles en art. 263 y 264, petenecen a algún genero, art. 287

La teoría de la descomposición de números y formas binarias en tres cuadrados, art. 288

Demostracion de los teoremas de Fermat: todo entero puede descomponerse en tres números triangulares o cuatro cuadrados, art. 293 Solucion de la ecuacion ax2 + by2 + cz2 = 0, art. 294

Sobre el metodo con el cual Legendre tratú de demostrar su teorema fundamental, art. 296

Representaciones de cero por formas ternarias cualesquiera, art. 299

Solucioún general de ecuaciones indeterminadas de segundo grado en dos

variables por racionales, art. 300

Del número promedio de generos, art. 301

Del nuúmero promedio de clases, art. 302

Algoritmo singular para clases propiamente primitivas; determinantes regu­lares e irregulares, etc., art. 305

SECCION Sexta. Aplicaciones varias de las investigaciones precedentes. . p. 387

De la descomposicioún de fracciones en otras múas simples, art. 309 La conversiúon de fracciones comunes en decimales, art. 312 Solución de la congruencia x2 ξ A por el metodo de exclusión, art. 319 Solución de la ecuaciún indeterminada mx2+ny2 = A por exclusiones, art. 323 Otro metodo de resolver la congruencia x2 ξ A para el caso en que A es negativo, art. 327

Dos múetodos para distinguir nuúmeros compuestos de nuúmeros primos y para determinar sus factores, art. 329

SECCION SETIMA. Ecuaciones que definen secciones de un círculo. . . . p. 419

La discusiúon se reduce al caso múas simple, donde el nuúmero de partes en las cuales se corta el cúrculo es un nuúmero primo, art. 336

Ecuaciones para funciones trigonomúetricas de arcos que son una parte o partes de la circunferencia completa, reduccioún de las funciones trigonomúetricas a las raíces de la ecuacion xn — 1 = 0, art. 337

*Teoría de las raíces de la ecuación xn —* 1 = 0 *(donde n es primo).*

Omitiendo la raíz 1, las restantes (Ω) están en la ecuación

X = xn-1 + xn-2+etc.+x + 1 = 0. La función X no se puede descomponer

en factores con coeficientes racionales, art. 341

Declaracion del proposito de las investigaciones siguientes, art. 342

Todas las raíces de Ω se distribuyen en ciertas clases (períodos), art. 343

Varios teoremas concernientes a estos períodos, art. 344

La solucion de la ecuacion X = 0 segun se desarrolla de la investigacion precedente, art. 352

Ejemplo para n = 19 donde la operacion se reduce a resolver dos ecuaciones cúbicas y una cuadrática, art. 353

Ejemplo para n = 17 donde la operacion se reduce a resolver cuatro ecuaciones cuadrúticas, art. 354

*Investigaciones adicionales sobre los períodos de raíces.*

Sumas con un numero par de terminos son cantidades reales, art. 355 De la ecuacion que define la distribucion de las raíces Ω en dos períodos, art. 356

Demostracion de un teorema mencionado en Seccion IV, art. 357 De la ecuaciún que distribuye las raíces Ω en tres períodos, art. 358 Reducciún a ecuaciones puras de las ecuaciones que dan las raíces Ω, art. 359 Aplicacion de lo anterior a funciones trigonométricas.

Metodo para encontrar los angulos de raíces particulares en Ω, art. 361 Se derivan tangentes, cotangentes, secantes y cosecantes a partir de senos y cosenos sin division, art. 362

Metodo de reducir sucesivamente las ecuaciones para funciones trigonometricas, art. 363

Secciones del círculo que pueden realizarse por ecuaciones cuadráticas o sea por construcciones geometricas, art. 365

APENDICE p. 473

Tablas

p. 475

APENDICE.

NOTAS MANUSCRITAS DE GAUSS.

Al art. 40. *Si hay un tercer número C, sea* X' *el máximo común divisor de los números X y C, y determínense números k y γ, tales que kX* + γC = X', *entonces kaA* + *kβB* + γC = X'. *Es evidente que tambiún* X' *es un divisor común de los números A, B y C, y, de hecho, el múximo, puesto que si hubiera otro mayor* = *θ, resultaría*

*ka ■*

*A*

1 +Αβ'

B

1

+ γ ·

*C*

*~θ*

X'

*— entero, θ*

*Q.E.A.*

Así se obtiene lo que íbamos a mostrar al poner ka = a, kβ = b, γ = c y X' = μ.

Al art. 114. Una demostración mas elegante se hace como sigue:

(a3n - an)2 = 2 + (a4n + 1)(a2n - 2) (a3n + an)2 = -2 + (a4n + 1)(a2n + 2)

y así y/2 = ±(a3n — an) y \f—2 ξ ±(a3n + an) (mod. 8n +1).

Al art. 256 VI. Indicamos 16 determinantes positivos de la forma 8n + 5 para los cuales el número de clases propiamente primitivas es tres veces mayor que el número de clases impropiamente primitivas, a saber 37,..., 573. A estos se agregan 677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997, resultando 31 de los 125.

Al art. 301. De esta manera la suma del número de géneros para los determinantes -1a -100 resulta ser = 234, 4, mientras que su valor real es 233. De -1 a -3000, la tabla da 11166, la formula 11167,9.

Al art. 366. Si todos los números 22 +1 fueran primos, entonces una

aproximación suficientemente precisa para el número (N) de enteros de este tipo menores que un numero M dado sería 1 ()2.

Al art. 42. El teorema concerniente a los divisores de una función algebraica racional entera con coeficientes enteros. 22 de julio de 1797.

Al art. 130. Despues de haber demostrado rigurosamente que cada número primo de la forma 4n + 1, tomado positivo o negativamente, es un no residuo de algún

número primo menor que el mismo. Descubrimos esta prueba el 8 de abril de

1796.

Al art. 131. Descubrimos el teorema fundamental por inducción en marzo de

1795.

Encontramos nuestra primera prueba, aquólla contenida en esta seccion, en abril de 1796.

Al art. 133. Iniciamos ahora una investigacion mas general. Consideraremos dos numeros impares cualesquiera P y Q, primos entre sí, provistos de signos cualesquiera. 29 de abril de 1796.

Al art. 145. Ademas, los teoremas pertenecientes a los residuos +2 y —2 entonces deberían suponerse; pero como nuestra demostracion esta completa sin usar

estos teoremas, obtenemos de esto un metodo nuevo para demostrarlos. 4 de

febrero de 1797.

Al encabezamiento de la Seccion V: Sobre las formas y las ecuaciones indeterminadas de segundo grado. De aquó adelante, 22 de junio de 1796.

Al art. 234. ... pasaremos a otro tema muy importante, la composicion de formas. Estas disquisiciones fueron iniciadas en el otoño de 1798.

Al art. 262. A partir de este principio, podemos desarrollar un nuevo metodo, no solamente para el teorema fundamental, sino tambien para demostrar los otros teoremas de la seccion previa que tengan que ver con los residuos —1, +2, —2. — — Los principios de este mótodo fueron primero descubiertos el 27 de julio de 1796, pero fue refinado y reducido a su forma presente en la primavera de 1800.

Al art. 266. ... pero hay muchas verdades bellas concernientes a estas formas cuya fuente real se indaga en la teoría de formas ternarias de segundo grado. Haremos, por tanto, una breve digresión dentro de esta teoría. 14 de febrero de 1799.

Al art. 272. Primero mostraremos como cada forma ternaria puede ser reducida a una forma mas simple y luego mostraremos que el nómero de las formas mas simples (que resulta de tales reducciones) es finito para un determinante dado. 13 de febrero de 1800.

Al art. 287 III. De manera similar se prueba que aquellos caracteres en un orden impropiamente primitivo, que segón los metodos de los artículos 264 II, III resultan ser los unicos posibles, son realmente del todo posibles, independientemente

de si pertenecen a P o a Q. Creemos que estos teoremas, etc. Se probaron por

*primera vez en el mes de abril de 1798.*

Al art. 302. El nómero promedio de clases, sin embargo, (no hace falta una

definición) aumenta de manera muy regular. Una primera idea en el comienzo

*de 1799.*

Al art. 306 X. Finalmente hacemos notar que, puesto que todas las propiedades consideradas en este artículo y el anterior dependen especialmente del nómero n, el cual juega un papel similar al de p — 1 en la Seccion III, este nómero merece atencion cuidadosa. Es muy deseable por lo tanto determinar la relación

general entre este nómero y el determinante al cual pertenece. Todo lo que

*queríamos resulto tan bueno que no dejó nada que desear. 30 de noviembre- 3 de diciembre de 1800.*

Al art. 365. *Descubrimos que un córenlo es geométricamente divisible en 17 partes el 30 de marzo de 1796.*

INDICE DE TERMINOS

carácter

completo, 238. de una forma, 237. clase

ambigua, 230. compuesta, 277. de formas, 228.

derivada de una clase primitiva, 232. duplicacián de una, 278. impropiamente primitiva, 232. negativa, 231. opuesta, 230. positiva, 231. primitiva, 232. principal, 239. propiamente primitiva, 232. congruencia, 18. algebraica, 18. resoluble, 18. resuelta, 18. trascendental, 18. determinante

de una forma, 123, 306. irregular, 380. regular, 380.

exponente de irregularidad, 381. forma

adjunta, 306. ambigua, 137. asociada, 173. binaria, ternaria, etc., 304. compuesta de dos formas, 247. tomada directamente, 250. tomada inversamente, 250.

forma (cont.)

compuesta directamente, 250. compuesta inversamente, 250. compuesta por tres formas, 265. compuesta por varias formas, 265. contenida en otra, 125. impropiamente, 126. propiamente, 126. contigua, 129.

a la primera parte, 129. a la ultima parte, 129. de los divisores, 113. de los no divisores, 113. de segundo grado, 121. de segundo, tercero, cuarto grado, etc., 304. definida, 310. derivada, 231. equivalente, 126.

impropiamente, 127. propiamente, 127. impropiamente primitiva (impropia), 232. indefinida, 310. negativa, 231, 310. opuesta, 129. positiva, 231, 310. primitiva, 231. principal, 239.

propiamente primitiva (propia), 232 que implica otra, 125. que se puede descomponer en formas, 270.

forma (cont.)

reducida, 150, 167, 205. representante de una clase, 228. transformable en ff', 247. genero, 238.

compuesto, 276. principal, 240. índice, 47.

magnitud del período de una fracción, 391.

mantisa de una fracción, 389. módulo, 7. no residuo, 7. nómero

asociado, 61.

característico de una forma, 243. congruente a otro seguón un módulo, 7. excluyente, 396, 399. incongruente a otro segón un modulo, 7.

perteneciente a un exponente, 43. período, 171. asociado, 174. de una clase, 379. de una fraccion, 391.

(f, λ), 428. similar, 428.

permutación semejante, 33.

raíz

primitiva, 46, 69. recíproca, 423. representacion adjunta, 325. del mismo orden, 233. de una forma perteneciente a un divisor cuadrado, 336. de un numero por una forma, 122. impropia, 326.

perteneciente a un valor, 331. propia, 326. residuo, 7.

absolutamente mínimo, 8. asociado, 83. cuadratico, 74, 241. mínimo, 8. transformacion

desemejante, 126. impropia, 126. propia, 126. semejante, 126. triplicacion de una clase, 278. valor

de la expresion

\Jax2 + 2bxy + cy2, 241. diferente, 243. equivalente, 243. opuesto, 331.

\*) Esta relación puede considerarse con más generalidad, como lo haremos en otra ocasión. Aquí solamente añadiremos dos proposiciones que serán Utiles para nuestras investigaciones, a saber:

1°. [α , β, Ί,... λ , μ] · \β, Ί,... λ] — [a , β, γ , ..., λ] · \β, γ , ..., Λ , μ] = ±1

\*) Esto no se permitiría si U = 0: pero entonces la verdad de las ecuaciones (19), (20), (21) se obtendría inmediatamente de la primera, la tercera, y la sexta de las anteriores.

\*) Será, en la notación del art. 27

βη = ±[-h”,h’”, -h””,...± hn]

donde los signos ambiguos puestos deben ser ; —+; +—; +—+ conforme a que n sea de la forma

2) Si “2 = 4, o sea D = m2, la ecuacion t2 + Du2 = m2 admitirá cuatro soluciones: t, u = m, 0; —m, 0; 0, 1; 0, —1. De esto, si F y f son equivalentes de una sola manera y si tenemos alguna transformacion

x = ax' + Py', y = γx' + óy'

resultaran cuatro ecuaciones:

189.

Lo siguiente debe ser notado con relación a este algoritmo.

1. Todos los námeros a, a', a'', etc., 'a, ''a, etc., tendrán el mismo signo; todos los námeros b, b', b", etc., 'b, "b, etc. serán positivos; en la serie ...''h, 'h, h, h', h'', ... alternarán los signos, esto es, si todos los a, a', etc., son positivos, hm o mh sera positivo cuando m sea par, negativo cuando m sea impar; pero si a, a', etc., son negativos hm o mh sera negativo para m par, positivo para m impar.
2. Si a es positivo y entonces h' es negativo, h'' es positivo etc., vamos a tener a'' = —1 negativo, a''' = h''a'' negativo y > a'' (o = a'' si h'' = 1); a'''' = h'''a''' — a''

es positivo y > a''' (porque h'''a''' positivo, a'' negativo); a''''' = h''''a'''' — a''' positivo y > a'''' (porque h''''a'''' es positivo) etc. Es entonces fácil de concluir que la serie a', a'', a''', etc., crecerá sin cota y que siempre habrá dos signos positivos y dos negativos tal que am tiene el signo +, +, —, — segán sea m ξ 0, 1, 2, 3 (mod. 4). Si a es

\*) Para abreviar omitiremos un tratamiento del caso en el cual el determinante sea cero, puesto que requiere un metodo un poco distinto.

1. Gauss escribió en latín las obras que consideró más trascendentales; el latín de las Disquisitiones Arithmeticae fue revisado por el filólogo Meyerhoff; vóase Merzbach, U. C. “An Early Version of Gauss’s Disquisitiones Arithmeticae”, en Mathematical Perspectives, Academic Press, 1981. [↑](#footnote-ref-2)
2. Muchos afirman que con este libro se inicia realmente la Teoría de Nómeros; vease Struik, D. J. A Concise History of Mathematics, New York: Dover Publications, 1967; p. 141. (La primera edición es de 1948). Otros estiman que fue Fermat quien creó la Teoría de Nómeros como una ciencia sistematica, pero Gauss inicio una nueva fase; cfr. Ore, Oystein: Number Theory and its History; New York: Dover Publications, 1948; p. 209. [↑](#footnote-ref-3)
3. Cfr. Buhler, W. K. Gauss: A Biographical Study, New York: Springer-Verlag, 1981; p. 36. [↑](#footnote-ref-4)
4. Las Disquisitiones Arithmeticae de Gauss han sido traducidas a varios idiomas: la traduccion francesa se tituló Recherches Arithmétiques y fue traducida por A. C. M. Poullet-Delisle en 1807; la version alemana Untersuchungen uber hohere Arithmetik traducida por H. Maser en 1889; la rusa es de 1959 editada por I. M. Vinogradov, Trudy po Teorii Cisel; y la inglesa traducida por A. A. Clarke apareció en 1966, y tiene una versión de 1986 revisada por W. C. Waterhouse. [↑](#footnote-ref-5)
5. Aunque en el caso de su madre, al parecer no podía escribir. [↑](#footnote-ref-6)
6. Cfr. Bell, E. T. : Men of Mathematics, New York: Simon and Schuster, 1965 (la primera version es de 1937); p. 219. [↑](#footnote-ref-7)
7. *Idem.* [↑](#footnote-ref-8)
8. Cfr. Bell. Op. cit. p. 221. [↑](#footnote-ref-9)
9. El criterio de Bell difiere del de Bühler, quien tiende a valorar mas el estímulo de Büttner para Gauss. [↑](#footnote-ref-10)
10. Ibtd, p. 223. [↑](#footnote-ref-11)
11. Puede consultarse el libro de Edna Kramer: The Nature and Growth of Modern

    Mathematics, Princeton: Princeton University Press, 1981; p. 474. (La primera edición es de Hawthorn Books, 1970). [↑](#footnote-ref-12)
12. Cfr. Bühler, Op. cit. p. 8. [↑](#footnote-ref-13)
13. Cfr. Bell, Op. cit. pp. 227-228. [↑](#footnote-ref-14)
14. El mismo Bell señala: “Para los grandes matemáticos la madurez temprana y una

    productividad sostenida no son excepción sino la regla. Puede que sea cierto que las ideas más originales se tienen en la juventud; pero cuesta tiempo elaborarlas. Gauss empleó cincuenta años en desarrollar las inspiraciones que tuvo (esta es sustancialmente su propia descripción) antes de que cumpliera veintión años; e incluso con medio siglo de continuo laborar solo consiguió madurar una pequena parte de sus ideas”. Vease Bell: Historia de las Matemáticas, Mexico: Fondo de Cultura Economica, 1985; p. 254. (La primera edicion es de 1940 con el título The Development of Mathematics, New York, McGraw Hill Book Co.). [↑](#footnote-ref-15)
15. Cfr. Gauss, C. F., Werke, ed. Konigliche Gesellschaft fur Wissenschften, Gottingen, 12 vols., Leipzig y Berlín, 1863-1950.; III, pp. 3-56. [↑](#footnote-ref-16)
16. La primera referencia se encuentra en el trabajo de Albert Girard, editor de los trabajos de Stevin (Invention nouvelle en algebre, 1629). Consúltese el libro de Dirk Struik: A Concise History of Mathematics, New York: Dover Publications, 1967; p. 141. (La primera ediciún es de 1948). [↑](#footnote-ref-17)
17. Puede consultarse el excelente libro de Carl Boyer: A History of Mathematics, Princeton: Princeton University Press, 1985; p. 548. (La primera edición es de John Wiley & Sons, Inc., en 1968). [↑](#footnote-ref-18)
18. Pueden consultarse las líneas fundamentales de este trabajo de Gauss en el libro de Dirk Struik: A Source Book of Mathematics 1200-1800, Princeton: Princeton University Press, 1986; pp. 115-123. (La primera edicion es de 1969 por Harvard University Press). [↑](#footnote-ref-19)
19. Cfr. Boyer, Op. cit. p. 549. [↑](#footnote-ref-20)
20. Sobre la teoría de números en los siglos XVII y XVIII se puede ver el trabajo del finlandés Raimo Lehti “Gauss’s Disquisitiones Arithmeticae”, Arkhimedes 29 (1977), no. 2, pp. 49-66. [↑](#footnote-ref-21)
21. Cfr. Boyer, Op. cit. p. 499. [↑](#footnote-ref-22)
22. Ibid. p. 500. [↑](#footnote-ref-23)
23. Por ejemplo, el resultado de Fermat que todo primo de la forma 4n + 1 es la suma de dos cuadrados de manera única, en las Disquisitiones Arithmeticae se desprende de la teoría de las formas binarias cuadráticas que Gauss desarrolla. Cfr. Boyer, Op. cit. p. 236. [↑](#footnote-ref-24)
24. Existen dos manuscritos de una versiún preliminar de las Disquisitiones Arithmeticae, descubiertos por U. Merzbach; vease “An early version of Gauss’s Disquisitiones Arithmeticae”, Mathematical Perspectives, pp. 167-177, Academic Press, New York, 1981. Se describe las diferencias entre las versiones preliminares y las finales. [↑](#footnote-ref-25)
25. Vease Bühler, Op. cit. p. 18. [↑](#footnote-ref-26)
26. Ibid. p. 32. [↑](#footnote-ref-27)
27. Vease el formidable libro de Morris Kline: Mathematical Thought. From Ancient to Modern Times, New York: Oxford University Press, 1990; p. 813. (La primera edición es de 1972). [↑](#footnote-ref-28)
28. Cfr. Bell, Op. cit. p. 229. [↑](#footnote-ref-29)
29. Por lo menos de los resultados disponibles en esas condiciones. [↑](#footnote-ref-30)
30. Este ha sido uno de los grandes temas de la teoría de números despues de Gauss. Sobre residuos de potencias y reciprocidad, el libro Reviews in Number Theory, editado por William LeVeque (Providence, R.I.: AMS, 1974) menciona 81 referencias entre 1940 y 1972, y la continuación del mismo libro, editada por Richard Guy (Providence, R. I.: AMS, 1984), contiene 94 del período 1973-1983. [↑](#footnote-ref-31)
31. De hecho, Gauss realizó 8 diferentes pruebas de este teorema en su vida. [↑](#footnote-ref-32)
32. Vease Bühler, Op. cit. p. 25. [↑](#footnote-ref-33)
33. Vease el extraordinario libro del matemótico norteamericano Leonard E. Dickson: History of the Theory of Numbers, Chelsea, 1951; Tomo III, p. 2. (La primera edicion es del Carnegie Institution, 1919-1923, Washington D.C.). Sobre las formas cuadráticas binarias, las cuadráticas ternarias, y las cuóbicas, vóease las póaginas 92-258 de esta obra de Dickson. [↑](#footnote-ref-34)
34. Para un estudio histórico detallado de las ecuaciones de segundo grado hasta 1920, véase el libro de Dickson, Op. cit. pp. 401-428. [↑](#footnote-ref-35)
35. Vease Bell, Op. cit. p. 236. [↑](#footnote-ref-36)
36. Estos calculos de Gauss anticiparon los metodos generales de Galois treinta años despues. [↑](#footnote-ref-37)
37. El tema de los polinomios ciclotomicos partira de este estudio; puede verse un relativamente reciente trabajo sobre esto realizado por el famoso matemático Tom Apostol: “The resultant of the cyclotomic polynomials Fm(ax) and Fn(bx)”, Math. Comp. 29 (1975), pp. 1-6. [↑](#footnote-ref-38)
38. Vease Bell, Op. cit. p. 236. [↑](#footnote-ref-39)
39. Un reciente artículo, poco conocido, sobre la construction del 17-gono regular se puede ver en: Ritseme, N., “Gauss and the cyclotomic equation”, Nieuw Tijdschr. Wisk. 64 (1976-1977), no. 4, pp. 188-196. [↑](#footnote-ref-40)
40. Cfr. Boyer, Op. cit. p. 552. [↑](#footnote-ref-41)
41. Se puede consultar una introduccián sencilla a la construccián de polígonos regulares en el libro de Ore: Number Theory and its History; pp. 346-358. [↑](#footnote-ref-42)
42. Vease Bell, Op. cit. p. 234. [↑](#footnote-ref-43)
43. *Idem.* [↑](#footnote-ref-44)
44. Se afirma tambien que durante el período de 1798 y 1800 Gauss introdujo mas material en el libro debido a los atrasos en el trabajo editorial, lo que extendiá mucho el libro, en particular la Seccioán quinta. [↑](#footnote-ref-45)
45. Consúltese Bühler, Op. cit. p. 29. [↑](#footnote-ref-46)
46. Ibid. p. 31. [↑](#footnote-ref-47)
47. Véase Kline, Op. cit. p. 815. [↑](#footnote-ref-48)
48. Para una versión simple de la primera prueba de Gauss de esta ley puede consultarse el artículo de L. Carlitz “A note on Gauss’ first proof of the quadratic reciprocity theorem”, en Proc. Amer. Math. Soc. 11 (1960), pp. 563-565. [↑](#footnote-ref-49)
49. Una prueba muy elegante y corta fue hecha por el matemótico D. H. Lehmer en el artículo “A low energy proof of the reciprocity law”, Amer. Math. Monthly 64, (1957), pp. 103-106. Una prueba algebraica se puede ver en S. Chowla en su articulo “The law of quadratic reciprocity”, Norske Vid. Selsk. Forh.(Trondheim) 39 (1966), p. 59. Una prueba geometrica en Kaplan, Pierre: “Une demostration geometrique de la loi de reciprocite quadratique”, Proc. Japan Acad. 45 (1969), pp. 779-780. Vease la de Claes Allander en “Gauss’s Law of reciprocity—a transparent proof” en Nordisk Mat. Tidskr. 22 (1974), pp. 23-25, 40. Hasta el famoso logico Th. Skolem no cedió a la tentacióon de dar una prueba de esta ley, vóease “A proof of the quadratic law of reciprocity with proofs of two so-called ‘Erganzunssatze’”, en el Norske Vid. Selsk. Forh (Trondheim) 34 (1961), pp. 18-24. [↑](#footnote-ref-50)
50. Vease Kline, Op. cit. p. 815. [↑](#footnote-ref-51)
51. Sobre algunos aspectos de la reciprocidad bicuadratica, vease: Brown, Ezra, “Biquadratic reciprocity laws”, Proc. Amer. Math. Soc. 37 (1973), pp. 374-376. [↑](#footnote-ref-52)
52. Vease Kline Op. cit. p. 816. [↑](#footnote-ref-53)
53. Cfr. Bell, Op. cit. pp. 252-253. [↑](#footnote-ref-54)
54. Vease Kline, Op. cit. p. 817. [↑](#footnote-ref-55)
55. *Idem.* [↑](#footnote-ref-56)
56. Gauss no publico este resultado; y más bien fue Jacobi, en una serie de conferencias en Konigsberg en 1836-1837, quien la estableció; aunque Eisenstein publico cinco pruebas de la ley desde 1844. [↑](#footnote-ref-57)
57. En el tratado de Gauss sobre residuos bicuadraticos, en 1831, Gauss “despejo el misterio que todavía rodeaba a los numeros complejos a traves de su representacián por puntos en el plano”: Struik. A Concise ..., p. 142. Consáltese tambien el artículo de E. T. Bell “Gauss and the Early Development of Algebraic Numbers”, Nat Math. Mag., 18 (1944), pp. 188, 219. Pero debe subrayarse—aun mas—que fue Gauss mismo quien dio un tratamiento algebraico y no geometrico a los námeros complejos, adelantándose seis años a Hamilton (este hecho se descubre en la correspondencia de Gauss con Bolyai en 1837). Vease Bell: Historia de las matemáticas, Mexico: Fondo de Cultura Economica, 1985; p. 189. (La primera edicion es de 1940 con el título The Development of Mathematics, New York, McGraw Hill Book Co.). [↑](#footnote-ref-58)
58. Ibid., p. 818. [↑](#footnote-ref-59)
59. Cfr. Bell, Op. cit. p. 238. [↑](#footnote-ref-60)
60. Véase Kline, Op. cit. p. 820. [↑](#footnote-ref-61)
61. *Idem.* [↑](#footnote-ref-62)
62. Ibid. p. 824. [↑](#footnote-ref-63)
63. Hilbert en 1897 condensó todos estos resultados y los solidificó en su “Die Theorie der algebraischen Zahlkorper”. [↑](#footnote-ref-64)
64. Un interesante estudio histórico sobre la génesis de la teoría de las formas cuadráticas, así como una breve reseña sobre los desarrollos posteriores iniciados por Gauss en las Disquisitiones Arithmeticae, es el de Víctor Albis: “Fermat and his problems III”, Bol Mat. 10 (1976), no. 1-6, pp. 86-95; esta es la tercera parte de tres artículos sobre la historia de la teoría de números. [↑](#footnote-ref-65)
65. Vease esta reseña en Kline, Op. cit. pp. 826-829. [↑](#footnote-ref-66)
66. Por ejemplo, es lo que se manifiesta cuando Gauss prueba que todo número de la forma 4n + 1 puede ser representado como la suma de cuadrados en una única manera. Consúltese Kline, Op. cit. p. 828. [↑](#footnote-ref-67)
67. Cfr. Kline, Op. cit. p. 829. [↑](#footnote-ref-68)
68. Vease Boyer, Op. cit. p. 564. [↑](#footnote-ref-69)
69. Ibid., p. 567. [↑](#footnote-ref-70)
70. Su aproximación es aquí diferente de la de Monge, pues conecta consideraciones prácticas con analisis teórico más sutil; vease Struik, A concise..., p. 142. [↑](#footnote-ref-71)
71. Struik afirma que Gauss estaba en posesión de la geometría no-euclidiana desde 1816; véase A concise..., p. 143. [↑](#footnote-ref-72)
72. Un resumen formidable de la producción matemótica de Gauss se puede ver en la conferencia del famoso matemótico frances del grupo Bourbaki, Jean Dieudonne, que se publico como “L’oeuvre mathematique de C. F. Gauss”, París: Universite de París, 1962. [↑](#footnote-ref-73)
73. Cfr. Kramer, Op. cit. p. 475. [↑](#footnote-ref-74)
74. Vease Bell, Op. cit. p. 242. [↑](#footnote-ref-75)
75. Ibid., pp. 250-251. [↑](#footnote-ref-76)
76. Ibid., p. 252. [↑](#footnote-ref-77)
77. Este es el significado de su obra Allgemeine Lehrsatze, acerca de la teoría de fuerzas que actúan inversamente proporcionales al cuadrado de la distancia; desarrollada en 1839 y 1840. Cfr. Struik, A concise..., p. 143. [↑](#footnote-ref-78)
78. Vease Kramer, Op. cit. p. 473. [↑](#footnote-ref-79)
79. Consúltese Bell, Op. cit. p. 256. [↑](#footnote-ref-80)
80. El teorema de los números primos fue demostrado en 1896 por el matematico frances Jacques Hadamard (1865-1963) y el belga Charles J. de la Vallée Poussin (1866-1962). Algunas modificaciones y simplificaciones de la prueba del famoso teorema fueron dadas por German Landau (1877-1938) y otros. Luego, en 1932 Norbert Wiener dedujo una prueba mas simple a partir de algunos de sus descubrimientos que G. H. Hardy llamo los “teoremas Tauberianos”. Vease Kramer, Op. cit. pp. 503-504. Otros aspectos de la contribución de Gauss a la teoría analítica de numeros se estudia en un artículo poco conocido de E. Van der Blij, “Gauss and analytic number theory”, en Nieuw Tijdschr. Wisk. 64 (1976-1977), no. 4, pp. 184-187. [↑](#footnote-ref-81)
81. Sobre la historia del teorema del numero primo, puede verse el artículo relativamente reciente de L. J. Goldstein “A history of the prime number theorem”, Amer. Math. Monthly 80 (1973), pp. 599-615. [↑](#footnote-ref-82)
82. Vease Boyer, Op. cit. p. 547. [↑](#footnote-ref-83)
83. En 1901 este diario fue publicado por Felix Klein en un libro que celebraba el sesquicentenario de la Sociedad Científica de Gottingen. [↑](#footnote-ref-84)
84. Ibid. p. 554. [↑](#footnote-ref-85)
85. Por ejemplo, uno de los resultados más importantes que encontró Gauss y que no fue publicado es el de las funciones elípticas: al parecer Gauss conocía en 1797 la doble periodicidad de la funcion lemniscata, y a principios del siglo pasado ya conocía las funciones doblemente periodicas generales, con lo que se adelantaba a Abel en casi 25 años; vease Bell, E. T. Historia de las matemáticas, Mexico: Fondo de Cultura Economica, 1985; p. 411. (La primera edicián es de 1940 con el título The Development of Mathematics, New York, McGraw Hill Book Co.). [↑](#footnote-ref-86)
86. Citado en el libro de D. E. Smith: History of Mathematics, New York: Dover Publications, 1951; p. 504. (La primera edicion es de 1923). [↑](#footnote-ref-87)
87. Véase Bell, Op. cit. p. 236. [↑](#footnote-ref-88)
88. Aunque en la teoría de números el tratamiento fue aritmético, y no algebraico. [↑](#footnote-ref-89)
89. Cfr. Bell, Op. cit. p. 241. [↑](#footnote-ref-90)
90. *Idem.* [↑](#footnote-ref-91)
91. Ibid., p. 255. [↑](#footnote-ref-92)
92. Ibid., p. 256. [↑](#footnote-ref-93)
93. Ibid., pp. 240-241. [↑](#footnote-ref-94)
94. Incluso, se puede considerar a Gauss el primer matemático del siglo XIX que establece una clara distinción entre aritmetica y geometría; haciendo de la primera verdades logicas y de la segunda verdades fundamentadas en la experiencia; y contribuye con ello a una separacián entre las matematicas puras y las aplicadas. Vease esta opinián en el libro de Leon Brunschvicg: Les Etapes de la philosophie mathématique, Paris: Blanchard, 1981; p. 497. (La primera version es de 1912, en la Revue du Mois). La distincián que hace Gauss (que puede verse en una carta a Bessel del 9 de abril de 1830) no disminuye la extraordinaria unidad de dimensiones empíricas y teoricas presente en la practica matemática de Gauss y que, mas bien, no ha sido leída apropiadamente por muchos de los matematicos y filásofos de nuestros dáas. [↑](#footnote-ref-95)
95. Para una interesante discusion sobre la existencia de revoluciones en las matemáticas puede consultarse el libro de I. Bernard Cohen: Revolution in Science, Cambridge, E.U.A.: Harvard University Press, 1985; pp. 505-507. [↑](#footnote-ref-96)
96. Sobre los componentes de la practica científica necesarios para la interpretation historica, puede consultarse el artículo de Angel Ruiz Záñiga: “Problemas de metodo en la historia de la ciencia” en el libro editado por el mismo autor: Las Matemáticas en Costa Rica, Memorias del Tercer Congreso Nacional de Matematicas, San Jose: 1990. [↑](#footnote-ref-97)
97. Tal vez pueda señalarse a Lagrange como un precursor de la nueva visión de las matemáticas en su consideración abstracta y general de la mecánica, aunque no tuvo realmente exito. [↑](#footnote-ref-98)
98. Esta es la opinián de Bell en su libro Historia de las Matemáticas. [↑](#footnote-ref-99)
99. Sobre una nueva visián de la naturaleza de las matemáticas constructivista y empiricista, que afirma una relacion íntima de las matematicas con el mundo físico y social puede consultarse el libro de Angel Ruiz Zuñiga: Matemáticas y Filosofía, Estudios Logicistas, San Jose: Editorial Universidad de Costa Rica, 1990. [↑](#footnote-ref-100)
100. El modulo debe ser siempre tomado con el valor absoluto, a saber: sin ningún signo. [↑](#footnote-ref-101)
101. Adoptamos este símbolo por la gran analogía que se encuentra entre la igualdad y la congruencia. Por la misma razón, el ilustre Legendre, en su tratado, usó el mismo símbolo para la igualdad y la congruencia, lo que nosotros dudamos en imitar para que no se originara ninguna ambigüedad. [↑](#footnote-ref-102)
102. donde se toma el signo superior cuando el número de términos α, β, γ, ...λ, μ es par, y el inferior cuando es impar.

     2o. El orden de los números α, β, γ, etc. puede invertirse: [α, β, γ,...,λ, μ] = [μ, λ, ...,γ,β, α]. Omitimos las demostraciones sencillas. [↑](#footnote-ref-103)
103. Esta conclusión requiere demostración, pero la hemos suprimido aquí. Nada más resulta de nuestro analisis que las congruencias propuestas no pueden resolverse por otros valores de las incognitas x, y, etc. No hemos mostrado que estos valores de hecho la satisfacen. Aón es posible que no haya ninguna solucion. Un paralelismo ocurre en el tratamiento de las ecuaciones lineales. [↑](#footnote-ref-104)
104. Obviamente λ0 divide a todos los números A, B y C. Si no fuera el máximo común divisor, el múximo sería mayor que λ0. Ahora, puesto que este maximo divisor divide a A, B y C, tambien divide a kaA + kjB + jC, es decir, a λ0 mismo. Así un número grande divide a uno pequeño Q. E. A. Este resultado puede ser aún mas facilmente establecido del art. 18. [↑](#footnote-ref-105)
105. Si se conciben las permutaciones semejantes como escritas sobre una circunferencia, de modo que la ultima sea contigua a la primera, no habrá ninguna discrepancia puesto que ningUn lugar puede llamarse primero o último. [↑](#footnote-ref-106)
106. En un comentario anterior, el gran hombre todavía no había logrado su proposito. Comm. Petr. T. VI p. 106.— En una controversia famosa entre Maupertuis y Konig, surgida sobre el principio de la acción mínima, aunque muy pronto llevo a una variedad de cosas, Konig afirmo tener en su poder una carta de Leibniz, en la cual esta contenida una demostración de este teorema que concuerda con la primera de Euler. Appel au public. p. 106. No queremos negar la veracidad de este testimonio, ciertamente Leibniz nunca publico su hallazgo. Vea Hist. de l’Ac. de Prusse, 1750 p. 530. [↑](#footnote-ref-107)
107. Difieren en esto: en los logaritmos el número de sistemas es infinito; aquí hay tantos como el número de raíces primitivas. Obviamente, bases congruentes producen los mismos sistemas. [↑](#footnote-ref-108)
108. Se percibe con facilidad que no es necesario conocer estas potencias, puesto que el residuo mínimo puede obtenerse fácilmente de un residuo mínimo de la potencia anterior.

     j) Del art. 18 se deriva como se puede hacer sin dificultad. Resuelvase y en factores que son o bien numeros primos diferentes, o bien potencias de námeros primos diferentes. Cada uno de ellos dividira a t o a u (o a ambos). Asígnense cada uno o a t o a u segán el cual el divida por el: cuando alguno divide a ambos, se le puede asignar arbitrariamente. Sea m el producto de los asignados a t, el de los otros = n. Esta claro que m divide a t, n divide a u, y mn = y. [↑](#footnote-ref-109)
109. Claramente determínense los números a, b, c, etc. de manera que a = 1 (mod. a“) y = 0 (mod. b3c7 etc.); b = 1 (mod. b3) y = 0 (mod. a“c7 etc.) etc. (vease art. 32), de donde serú a + b + c + etc. = 1 (mod. p — 1), (art. 19). Ahora, si cualquier raíz primitiva r se representa por el producto ABC etc., se tomara A = ra, B = rb, C = rc, etc., luego A pertenecerú al exponente a“, B al exponente b3, etc.; el producto de todos los números A, B, C, etc., serú = r (mod. p). Finalmente se ve con facilidad que A, B, C, etc., no pueden determinarse de ninguna otra manera. [↑](#footnote-ref-110)
110. En este caso, propiamente lo usamos con un sentido diferente al que hemos uasado hasta ahora. En efecto, conviene decir: r es un residuo del cuadrado a2 según el módulo m cuando r = a2 (mod. m). Pero, por brevedad, en esta sección decimos siempre que r es un residuo cuadratico de m mismo, para no tener ninguna ambigüedad. Entonces desde ahora en adelante no usaremos la expresion residuo para denotar un número congruente, salvo si se trata de residuos mínimos donde no pueda haber duda alguna. [↑](#footnote-ref-111)
111. Pronto mostraremos cómo podemos tratar con los módulos compuestos también. [↑](#footnote-ref-112)
112. Con respecto a los numeros divisibles por p, es claro que sus cuadrados serán divisibles por p2, de donde todos los numeros divisibles por p pero no por p2 seran no residuos de pn. En general, si se propone un numero pkA, donde A no es divisible por p, podemos distinguir los siguientes casos: [↑](#footnote-ref-113)
113. Puesto que hemos excluido el caso p = 2, hay que decir algo sobre el. Cuando el numero 2 es el modulo, cualquier numero sera un residuo y ninguno sera un no residuo. Pero cuando 4 es el modulo, todos los numeros impares de la forma 4k +1 serán residuos, mientras que todos los de la forma 4k + 3 serán no residuos. Finalmente, cuando 8 o una potencia mayor del numero 2 es el modulo, todos los números impares de la forma 8k +1 serún residuos, pero los restantes que son de las formas 8k + 3, 8k + 5, y 8k + 7 serún no residuos. La ultima parte de esta proposición es clara porque el cuadrado de cualquier numero impar, sea bien de la forma 4k +1, o bien de la forma 4k — 1, sera de la forma 8k +1. La primera parte la demostramos a continuation:

     1. Si la suma o diferencia de dos numeros es divisible por 2n-1, los cuadrados de dichos numeros serán congruentes segun el modulo 2n. Pues, si se pone uno de ellos = a, el otro sera de la forma 2n-1h ± a, cuyo cuadrado es = a2 (mod. 2n).
     2. Cualquier numero impar que es un residuo cuadrático de 2n, sera congruente a algun cuadrado cuya raíz es un numero impar y < 2n-2. Sea pues a2 cualquier cuadrado al cual el numero es congruente y sea el numero a = ±a (mod. 2n-1) de manera que a no supere la mitad del modulo (art. 4). Entonces tendremos a2 = a2,

     [↑](#footnote-ref-114)
114. Porque el número de enteros impares menores que 2n-2 es 2n-3. [↑](#footnote-ref-115)
115. Denotamos al conjunto de todos los residuos del número primo p, menores que p, excluyendo el residuo 0, por la letra C. Puesto que el numero de estos residuos siempre serú = Pp, es claro que serú par si p es de la forma 4n +1, pero impar si p es de la forma 4n + 3. Por semejanza con el art. 77 donde se hablaba sobre nuúmeros en general, se llaman residuos asociados a dos números cuyo producto ξ 1 (mod. p). De hecho, es claro que si r es un residuo, tambien 1 (mod. p) sera un residuo. Puesto que un mismo residuo no puede tener mas asociados entre los residuos C, es evidente que todos los residuos C pueden distribuirse en clases, de las cuales cada una contenga dos residuos asociados. Ahora, es claro, si no se presenta ningún residuo que no este asociado a sú mismo, i.e., si cada clase contuviera dos residuos diferentes, el nuúmero de todos los residuos sería el doble del número de todas las clases. Pero, si se presenta [↑](#footnote-ref-116)
116. Por eso, cuando hablamos de cualquier número, sea un residuo o no residuo de un número de la forma 4n + 1, podremos ignorar completamente el signo o bien emplear el signo doble ±. [↑](#footnote-ref-117)
117. Mediante una inducciún semejante a la de la tabla II se encuentran que —2 [↑](#footnote-ref-118)
118. Esto es considerando a —2 como producto de +2 y —1. Véase art. 111. [↑](#footnote-ref-119)
119. Mediante este metodo, no se puede descubrir nada con respecto a los números de la forma 12n + 1, por lo que exigen artificios particulares. Por una inducciún se deduce facilmente que +3 y —3 son residuos de todos los números primos de esta forma. Pero, es claro que debe demostrarse solamente que —3 es un residuo de tales numeros, ya que necesariamente +3 sera un residuo (art. 111). Sin embargo demostraremos mús generalmente que —3 es un residuo de cualquier número primo de la forma 3n +1.

     Sea p un primo de este tipo y a un número que, para el módulo p, pertenece al exponente 3 (los cuales existen por el art. 54, ya que 3 es divisor de p — 1). Por eso sera a3 ξ 1 (mod. p), i.e., a3 — 1 o sea (a2 + a +1)(a — 1) serú divisible por p. Pero es claro que a no puede ser ξ 1 (mod. p), ya que 1 pertenece al exponente 1, por lo que a — 1 no sera divisible por p, pero a2 + a + 1 lo serú, y de allú tambien 4a2 + 4a + 4, i.e., sera (2a + 1)2 ξ —3 (mod. p) o sea —3 es un residuo de p. Q. E. D. [↑](#footnote-ref-120)
120. Por inducción se descubre facilmente que +5 y —5 son residuos de todos los números primos de la forma 20n +1 o 20n + 9. Ahora bien, si esto es cierto en general, se tendrá una ley elegante, +5 es un residuo de todos los números primos que sean residuos de 5 (pues estos estún contenidos en una u otra de las formas 5n + 1 o 5n + 4, o en una de estas otras 20n + 1, 9, 11, 19, de las cuales la tercera y la cuarta ya se han tratado), pero es un no residuo de todos los números impares que son no residuos de 5, como ya lo hemos demostrado antes. Ahora es claro que este teorema es suficiente para juzgar si +5 (y tambien —5 si se considera como producto de +5 y —1) es un residuo o un no residuo de cualquier numero dado. Finalmente se observa la analogía de este teorema con aquel que presentamos en el art. 120 sobre el residuo —3. [↑](#footnote-ref-121)
121. Es claro que +1 debe ser excluido. [↑](#footnote-ref-122)
122. Art. 98. De hecho a2 es un residuo de q no divisible por q, pues de lo contrario el número primo p tambien sería divisible por q. Q.E.A. [↑](#footnote-ref-123)
123. En efecto, si fuera r = —f = +f (mod. p), 2f sería divisible por p; por lo tanto, también 2a (puesto que f2 = a (mod. p)). Pero esto es posible Unicamente cuando p = 2, pues por hipótesis a es primo a p. Pero sobre este caso ya hemos hablado por separado.

     j) De hecho, b2 — r2 = (b — r)(b + r) estará compuesto de dos factores, uno de los cuales es divisible por p (hipátesis) y el otro por 2 (puesto que tanto b como r son impares); de donde b2 — r2 es divisible por 2p. [↑](#footnote-ref-124)
124. Demostraremos en seguida que lo que descubrimos por induccioún tiene lugar en general. Pero, antes de entrar en este trabajo, serú necesario extraer todo lo que sigue de este teorema, si se supone verdadero. Enunciamos el teorema mismo así:

     Si p es un numero primo de la forma 4n +1, +p será un residuo o no residuo de cualquier numero primo que, tomado positivamente, es un residuo o no residuo del mismo p. Si p es un número primo de la forma 4n + 3, —p tendra la misma propiedad.

     Ya que casi todo lo que puede decirse sobre los residuos cuadrúticos se apoya en este teorema, la denomination teorema fundamental que usaremos en lo que sigue no sera inconveniente.

     Para poder presentar nuestro razonamiento lo mús brevemente posible, denotaremos por a, a', a", etc. los numeros primos de la forma 4n + 1, por b, b', b", etc. los numeros primos de la forma 4n + 3; por A, A', A", etc. los numeros cualesquiera de la forma 4n + 1, por B, B', B'', etc. los numeros cualesquiera de [↑](#footnote-ref-125)
125. Sea l = 1 si ambos P, Q = 3 (mod. 4); si no, sea l = 0, y sea m = 1 si ambos P y Q son negativos, y m = 0 en el caso contrario. Así la relación depende de l + m. [↑](#footnote-ref-126)
126. Segundo caso. Cuando T + 1 es de la forma 4n +1 (= a), p de la forma 4n + 3, y ±pR(T + 1), no puede ser ni +(T + 1)Np ni — (T + 1)Rp. Este caso fue el quinto arriba.

     Sea como antes e2 = p + fa, donde e es par y < a. [↑](#footnote-ref-127)
127. Séptimo caso. Cuando T +1 es de la forma 4n + 3 (= b), p de la misma forma, y +pNb o —pRb, no pueden ser +bNp, ni —bRp. (Cuarto caso arriba).

     Sea —p = e2 (mod. b), y e par y < b.

     I. Cuando e no es divisible por p. Sea —p = e2 — bf, y f sera positivo, de la forma 4n +1, primo a p y menor que b (ya que ciertamente e no es mayor que b — 1, p < b — 1, por lo que tendremos bf = e2 + p < b2 — b i.e., f < b — 1). Ademas tendremos —pRf, de esto (proposición 10, art. 132) +fRp, de +bfRp tendremos +bRp, o —bNp. [↑](#footnote-ref-128)
128. Si no hubiera factores de una clase, debería escribirse 1 en vez del producto de ellos. [↑](#footnote-ref-129)
129. Residuo en el sentido del art. 4. En general conviene tomar el menor residuo absoluto. [↑](#footnote-ref-130)
130. De este modo, simplemente llamaremos a estos números los divisores de x2 — A; es claro cuales son los no divisores. [↑](#footnote-ref-131)
131. A saber, que sean primos a A. [↑](#footnote-ref-132)
132. Desechado el factor t. [↑](#footnote-ref-133)
133. A saber, existen números r, r', r", etc., n, n', n", etc., todos diferentes y < 4A tales que todos los divisores primos de x2 — A estén contenidos en alguna de las formas 4Ak + r, 4Ak + r', etc. y todos los no divisores primos en alguna de estas 4Ak + n, 4Ak + n', etc. (donde k es un número indeterminado). [↑](#footnote-ref-134)
134. Como él mismo confiesa, l. c. p. 216: “Una demostración de este muy elegante teorema se desea todavía, aunque se ha investigado en vano durante mucho tiempo. Por tal razón sera considerado excelentísimo el que tenga el exito de encontrar la demostracion de este teorema.” Con cuanto ardor este hombre inmortal buscaba la demostracion de este teorema y de otros que son solamente casos especiales del teorema fundamental, puede verse en muchos otros lugares, e.g., Opuscula Analytica, I, (Additamentum ad Diss. VIII) y II, (Diss. XIII) y en varias disertaciones en Comm. acad. Petrop. que hemos citado en varias ocasiones. [↑](#footnote-ref-135)
135. Es claro por el análisis anterior que esta proposición también es válida para formas cuyo determinante es = 0. Pero no se debe extender la ecuacion (αδ — βγ)2 = 1 a este caso. [↑](#footnote-ref-136)
136. f) De esto se deduce fácilmente

     AeU = (δγ0 — γ S’)m 2BeU = (αδ0 — δα + γβ0 — βγ0)m CeU = (βα0 — αβ 0)m [↑](#footnote-ref-137)
137. Si todos α + α',γ + γ0,β + β',δ + δ' fueran = 0, la razón sería indeterminada, y por ende el metodo no aplicable. Pero con cuidado se puede mostrar que esto no puede darse con nuestras suposiciones; pues sería αδ — βγ = α'δ' — β'γ' i.e. e = e', porque e = —e',e = e' = 0. Tambien B'2 — A'C', i.e. el determinante de la forma F' sería = 0. Tales formas las hemos excluido por completo. [↑](#footnote-ref-138)
138. Conviene observar que, si el primer o el último término a ó a' de alguna forma dada (a, b, a') fuera = 0, su determinante sería un cuadrado positivo; por lo cual esto no puede ocurrir en este caso. Por la misma razón no pueden existir signos opuestos de los terminos de ambos lados a y a' para la forma de un determinante negativo. [↑](#footnote-ref-139)
139. El námero de formas reducidas que tienen un determinante dado — D siempre es finito y relativamente pequeno en relacián con el námero D. Estas mismas [↑](#footnote-ref-140)
140. Si se rechaza una u otra de dos formas no identicas pero propiamente equivalentes entre todas las formas reducidas de un determinante dado, las formas [↑](#footnote-ref-141)
141. Tenemos aquó una tabla de formas para ciertos determinantes negativos, según las cuales todas las restantes del mismo determinante pueden separarse en clases. Seguón la observacioón del artóculo anterior, listamos uónicamente la mitad, a saber, [↑](#footnote-ref-142)
142. δη = ±[h, -h",h"',... ± hn]

     donde los signos ambiguos deben ser +—; ++; ; —+, según n sea de la forma 4k + 0; 1; 2; 3.

     Pero dado que esto puede confirmarse fácilmente por sí mismo, la brevedad no permite exponerlo con amplitud. [↑](#footnote-ref-143)
143. PROBLEMA. Si las formas F y f son equivalentes, hallar todas las transfor­maciones de la forma F en f.

     Solución. Si las formas F y f son equivalentes de una sola manera, i.e., solamente propiamente o solamente impropiamente, por el artículo precedente bósquese alguna transformacion de la forma F en f. Es claro que no pueden darse otras mas que aquellas semejantes a esta. Si, por otro lado las formas F y f son equivalentes tanto propia como impropiamente, busquense dos transformaciones: la una propia y la otra impropia. Sea la forma F = (A,B, C), B2 - AC = -D, y el maximo comun divisor de los numeros A, 2B, C = m. Entonces es claro del artículo 162 que, en el primer caso, todas las transformaciones de la forma F en f pueden deducirse de una transformacion; y en el segundo, todas las propias de una propia y todas las impropias de una impropia, si se tuvieran todas las soluciones de la ecuacion t2 + Du2 = m2. Por lo tanto, encontradas estas, el problema se habría resuelto.

     Se tiene, sin embargo, D = AC - B2, 4D = 4AC - 4B2; por lo cual = 4() — (—)2 sera un entero. Ahora, si

     m2 v m2 ' v m / 5 [↑](#footnote-ref-144)
144. Puede demostrarse que la forma (A, B, C) necesariamente equivaldrá a la segunda; pero esto no es necesario aquí. [↑](#footnote-ref-145)
145. Es claro que este caso está contenido en (2) del artículo 180. [↑](#footnote-ref-146)
146. Si se pudiera reconocer la equivalencia de dos formas reducidas de determi­nante positivo con la misma facilidad que en el caso de aquellas de determinante negativo (art. 172) se reconocería sin dificultad la equivalencia de dos formas cua­lesquiera de determinante positivo. Pero aquí el asunto es muy diferente, y puede suceder que muchas formas reducidas sean equivalentes entre sí. Antes de dedicarnos a este problema, sera necesario inquirir mas detalladamente en la naturaleza de las [↑](#footnote-ref-147)
147. Donde los signos son ambiguos, siempre vale el superior cuando a0 es positivo, el inferior cuando a0 es negativo. [↑](#footnote-ref-148)
148. Para b =1, —78 no puede resolverse en dos factores que sin considerar el signo estén situados entre y/79 + 1 y y/79 — 1; por lo cual este valor es omitido, y, por la misma razón, los valores 2 y 6. [↑](#footnote-ref-149)
149. Aquí el índice necesariamente será impar; puesto que los primeros términos de las formas F y f tienen signos opuestos (vease la observación 2 arriba). [↑](#footnote-ref-150)
150. No puede haber otros casos ya que, según el artículo anterior, αδ — βγ = ±1, y entonces los dos límites no pueden tener signos opuestos ni ser simultaneamente cero. [↑](#footnote-ref-151)
151. No importa que el orden en (II) sea el mismo que en (I), u opuesto a él, i.e. que en (I) (m) este a la izquierda de L o a la derecha de el. [↑](#footnote-ref-152)
152. PROBLEMA. Dadas dos formas cualesquiera Φ y φ del mismo determinante, determinar cuando son o no equivalentes. [↑](#footnote-ref-153)
153. PROBLEMA. Dadas dos formas propiamente equivalentes Φ y φ: encontrar una transformación propia de una en la otra.

     Solucion. Por el metodo del artículo 183 podran encontrarse dos series de

     formas

     Φ, Φ0, Φ", ...Φη y φ, φ0, φ00, ...φν [↑](#footnote-ref-154)
154. Ψ se deriva de Φ intercambiando el primer y el último términos y asignando el signo opuesto al termino del medio. Lo mismo vale para los otros miembros de la serie. [↑](#footnote-ref-155)
155. PROBLEMA. Encontrar los números menores t y u que satisfacen la ecuación indeterminada t2 - Du2 = m2 si se da alguna forma (M, N, P) cuyo determinante es D y si m es el máximo común divisor de M, 2N y P.

     Solucion. Tomemos a voluntad la forma reducida (a, b, -a0) ...f con deter­minante D, en la cual el maximo comun divisor de los numeros a, 2b, a0 sea m. Es claro de ahí que esa existe porque puede encontrarse una forma reducida equivalente a la forma (M, N, P), la cual por el artículo 161 esta dotada con esta propiedad. Pero para nuestro presente proposito, cualquier forma reducida que satisface esta condicion puede ser usada. Calculemos el período de la forma f, el cual supon­dremos consiste de n formas. Reteniendo la notacion que hemos usado en el artículo [↑](#footnote-ref-156)
156. Las cantidades que en el artículo 162 eran α,β,γ,δ; α1, β’, y', δ0; C; a,b, c; e,

     aquí son 1,0,0,1; an,βη,yn,δη; a, b,—a'; a,b,—a'; 1. [↑](#footnote-ref-157)
157. Solamente en estas cuatro expresiones y en la ecuación [1] e denota el exponente de la potencia; en las restantes las letras escritas arriba siempre designan el índice. [↑](#footnote-ref-158)
158. n

     Q. E. A. ; porque la primera parte de la primera cantidad es menor que la primera parte de la segunda cantidad y la segunda parte de la primera es menor que la segunda parte de la ultima. Por lo tanto la suposición es inconsistente y las sucesiones t0, t0, t", etc., u0, u0, u", etc., exhibirón todos los valores posibles de t y u.

     Ejemplo. Para D = 61 y m = 2 encontramos que los valores positivos menores de t y u, son 1523 y 195, así pues todos los valores positivos serán expresados por la fórmula [↑](#footnote-ref-159)
159. En este comentario el algoritmo que consideramos en el artículo 27 se presenta con una notación similar. No lo reconocimos así en aquel momento. [↑](#footnote-ref-160)
160. Lo que Wallis, pp. 427-28, propuso para este objetivo no tiene peso. El paralogismo consiste en que, en la p. 428, línea 4, el presupone que, dada una cantidad p, pueden encontrarse enteros a y z tal que a sea menor que p y que la diferencia sea menor que un numero asignado. Esto es cierto cuando la diferencia asignada es una cantidad dada pero no cuando, como sucede en el presente caso, depende de a y z, y entonces es variable. [↑](#footnote-ref-161)
161. PROBLEMA. Dadas dos formas propiamente equivalentes F y F' con deter­minante h2, encontrar una transformacién propia de una en la otra.

     Solucién. Sea Φ una forma reducida propiamente equivalente a la forma F, que por hipotesis seró tambien propiamente equivalente a la forma F'. Por el articulo 206 buscaremos una transformation propia α, β, γ, δ, de la forma F en Φ [↑](#footnote-ref-162)
162. TEOREMA. Si dos formas reducidas (a, h, 0), (a0,h,0) son impropiamente equivalentes, resultará aa0 ξ m2 (mod. 2mh), donde m es el máximo común divisor [↑](#footnote-ref-163)
163. En efecto se transforma en (m; K) por la sustitución m, K, 0, n. Vea artículo 159. [↑](#footnote-ref-164)
164. Más concisamente, todas las transformaciones propias se incluyen en la formula 10t + 55«, t + 2u, — 15t — 55u, —t — 3u donde t y u son todos los enteros que satisfacen la ecuacián t2 — 11«2 = 1. [↑](#footnote-ref-165)
165. Si se propusiera una ecuación en la cual el segundo, cuarto o quinto coeficiente no fuera par, su multiplication por 2 produciría la forma que suponemos aquí. [↑](#footnote-ref-166)
166. Ilustramos con un ejemplo el caso del articulo 217 (pues este es el mas difícil). Sea x2 + 8xy + y2 + 2x — 4y + 1 = 0 la ecuacion dada. Por la introduction de otros indeterminados p = 15x — 9 y q = 15y + 6, se deriva la ecuacion p2 + 8py + q2 = —540. [↑](#footnote-ref-167)
167. Mediante esta clasificacion, formas que son propiamente equivalentes pueden separarse completamente de todas las demas. Dos formas con el mismo determinante seran propiamente equivalentes si ellas pertenecen a la misma clase; cualquier numero [↑](#footnote-ref-168)
168. Hemos escogido aquí los términos propiamente e impropiamente porque no hay otros más convenientes. Deseamos prevenir al lector de no buscar alguna conexión entre este caso y el del artículo 157 porque no existe ninguna. Pero ciertamente no se debería temer la ambigüedad. [↑](#footnote-ref-169)
169. Usando, por brevedad, las formas representantes en lugar de sus clases. [↑](#footnote-ref-170)
170. TEOREMA. Sea F una forma primitiva con determinante D y p un número primo que divide a D: entonces los números no divisibles por p que pueden

     representarse por la forma F son todos residuos cuadrúticos de p o todos no residuos.

     Demostracion. Sea F = (a, b,c), y sean m y m' dos números cualesquiera no divisibles por p que pueden ser representados por la forma F; o sea

     m = ag2 + 2bgh + ch2, m' = ag'2 + 2bg'h' + ch'2

     Entonces tendremos

     mm' = [agg' + b(gh' + hg') + chh']2 — D[gh' — hg']2 [↑](#footnote-ref-171)
171. Si el determinante es divisible por 8 se ignorará su relación con el número 4 pues en este caso ya se encuentra contenida en la relaciún con 8. [↑](#footnote-ref-172)
172. El conjunto de todos los caracteres particulares de una clase o forma dada constituyen el carácter completo de esta forma o clase. Asá, p. ej., el carácter completo de la forma (10, 3, 17) o de la clase completa que ella representa será 1, 4; N7; N23. De manera análoga el carácter completo de la forma (7,1, -17) sera 7, 8; R3; N5. Omitimos el carácter particular 3, 4 en este caso porque esta se halla contenida en el caraácter 7, 8. A partir de estos resultados derivaremos una subdivisiáon del orden completo de clases propiamente primitivas (positivas cuando el determinante es negativo) de un determinante dado en muchos diferentes géneros, colocando todas las clases que poseen el mismo caráacter completo en el mismo gáenero, y en diferentes generos aquellos que poseen diferentes caracteres completos. Asignaremos a cada genero aquellos caracteres completos que poseen las clases contenidas en ellos. Asá, [↑](#footnote-ref-173)
173. Tomando a como a0, b como b0 etc. Pero es claro que la misma ecuación es válida cuando λ = μ ó λ > μ. [↑](#footnote-ref-174)
174. En esta expresión debemos poner mucho cuidado en el orden de los coeficientes p, p1, etc. y de las formas f y f ’. Es fócil ver que si el orden de las formas f y f ’ se cambia tal que la primera se convierte en la segunda, los coeficientes p0 y q1 deben intercambiarse con p” y q” y los otros deben permanecer iguales. [↑](#footnote-ref-175)
175. Esta manera de derivar la ecuación Δ2 = dd0 es suficiente para nuestros propósitos actuales. Podríamos haber deducido directamente de las ecuaciones [1] a [11] que 0 = (Δ2 - dd0)2. Este podría haber sido un analisis mas elegante pero demasiado prolongado en este punto. [↑](#footnote-ref-176)
176. El lector puede verificar este análisis fácilmente. Lo omitimos en aras de la brevedad. [↑](#footnote-ref-177)
177. PROBLEMA. Dadas dos formas cuyos determinantes son iguales o por lo menos difieren por factores cuadrados: encontrar una forma compuesta por estas dos. [↑](#footnote-ref-178)
178. TEOREMA. Si la forma F es transformable en el producto de dos formas f y f', y la forma f' implica la forma f'', entonces F también será transformable en el producto de las formas f y f".

     Demostración. Para las formas F, f y f' todas las notaciones del artáculo 235 se mantienen; sea f'' = (a'',b0',c0') y sea f' transformado en f'' mediante la sustitucion α, β, γ, δ. Entonces F se transformará en ff'' mediante la sustitucion

     ap + 7p', βp + áp', ap'' + yp''', βp'' + áp'''

     aq + 7q', βq + áq', aq'' + yq''', βq'' + áq''' Q. E. D. [↑](#footnote-ref-179)
179. TEOREMA. Si la forma F está contenida en la forma F' y es transformable en el producto de las formas f y f'; entonces la forma F' será transformable en el mismo producto.

     Demostracián. Si para las formas F, f y f' se retiene la misma notación que en el caso anterior y si se supone ademas que la forma F' se transforma en F mediante la sustitucion α, β, γ, δ, es facil ver que, mediante la sustitucion

     ap + βq, ap' + β((, ap' + βq", ap'' + βq'''

     γρ + δq, γp + δ^, γp' + δq'', γp'''+ δ^" [↑](#footnote-ref-180)
180. TEOREMA. Si la forma F está compuesta por las formas f y f0, cualquier otra forma que sea transformable en el producto ff0 de la misma manera que F, implicará a F propiamente.

     Demostración. Si mantenemos la notacion del artículo 235 para las formas F, f y f0, las ecuaciones Ω tambien tendrán lugar aquí. Supongamos que la forma [↑](#footnote-ref-181)
181. \*) El significado actual de estos símbolos no debe confundirse con su significado en el artículo [↑](#footnote-ref-182)
182. pues los números que se expresan mediante estos signos aquí corresponden más bien a los del artículo 234 que son multiplicados por números denotados por símbolos similares. [↑](#footnote-ref-183)
183. Observe que podríamos deducir otras 18 ecuaciones similares a Ψ reemplazando los factores a, 2b, c por a0, 2b0, c0; a00, 2b00, c00; pero puesto que no son necesarias para nuestros propositos, las omitiremos.

     j) Esto sigue de la ecuación 10 del artículo 235 ff. La cantidad Vdd0 se hace = Dnn0 = Dnn0N2 = Dnn0. [↑](#footnote-ref-184)
184. Si tenemos una forma como F o F0 que resulta de la composicioún de una de tres formas dadas con otra la cual es la composicioún de las dos formas restantes, diremos que esta compuesta por estas tres formas. Queda claro del artúculo anterior que no importa el orden en el cual se componen las tres formas. Similarmente, si tenemos cualquier número de formas f, f', f'', f''', etc. (y los cocientes de sus determinantes son cuadrados) y se compone la forma f con f', la forma resultante con f'' y la resultante con f000, etc.: diremos que la uúltima forma que se obtiene de esta operaciúon esta compuesta por todas las formas f, f', f'', f''', etc. Y es fúcil mostrar aquú [↑](#footnote-ref-185)
185. De las ecuaciones [↑](#footnote-ref-186)
186. Podemos lograrlo siempre utilizando las congruencias [↑](#footnote-ref-187)
187. o sea, de la expresión (mod. hx ν), de donde B = b - ctb+b, = ^+60/11 (mod. A).

     hv hv ( [↑](#footnote-ref-188)
188. PROBLEMA. Dadas dos formas cualesquiera, f y f0 de las cuales F está compuesta: determinar el gánero de la forma F a partir de aquellos de las formas f

     y f0.

     Solución. Sean f = (a, b, c), f0 = (a0, b0, c0) y F = (A, B, C); de seguido,

     desígnase por m el maximo comán divisor de los numeros a, b, c y por m0 el maximo comán divisor de los námeros a0, b0, c0, de modo que las formas f y f0 sean derivadas de las formas primitivas (m, m, m) y (mm, m7), las que designaremos por f y f0 respectivamente. Ahora si al menos una de las formas f o f0 es propiamente primitiva, el maximo comán divisor de los námeros A, B, C será mm0, y por ende F sera derivado de la forma primitiva (mm?, mm, mm7) · ·· F y es claro que el genero de la forma F dependerá del de la forma F. Es facil ver que si F es transformado en ff0 por la misma sustitucion que transforma a F en ff0 y de tal modo que F esta compuesto por f y f0, su genero puede ser determinado por el problema del artículo 246. Pero si ambas f y f0 son impropiamente primitivas, el máximo común divisor de los numeros A, B, C sera 2mm0, y la forma F, que está todavía compuesta por f y f0, sera manifiestamente derivada de la forma propiamente primitiva (2mm7, 2mm7, 2mm7). El genero de esta [↑](#footnote-ref-189)
189. Si D es un námero divisible por m2 (suponemos a m positivo), habrá un orden de formas de determinante D derivado del orden propiamente primitivo del determinante m (cuando D es negativo habrá dos de ellos, uno positivo y uno negativo); manifiestamente la forma (m, 0, — m) pertenecerá a aquel orden (el [↑](#footnote-ref-190)
190. PROBLEMA. La clase propiamente primitiva K de determinante D surge a partir de la duplicación de una clase propiamente primitiva k del mismo determi­nante. Se buscan todas las clases similares cuya duplicación produzca a K.

     Solución. Sea H la clase principal de determinante D y sean H0, H00, H000, etc. las otras clases ambiguas propiamente primitivas del mismo determinante; k+H0, k + H00, k + H000, etc. son las clases que surgen a partir de la composicion de estas con k. Las designaremos como k0, k00, k000, etc. Ahora bien, todas las clases k0, k00, k000, etc. serán propiamente primitivas de determinante D y diferentes entre sí; y la clase K resultara de la duplicacion de cualquiera de ellas. Si denotamos por R a cualquier clase propiamente primitiva de determinante D que produzca a la clase K cuando sea duplicada, necesariamente estará contenida entre las clases k, k0, k00, etc. Pues, supongase que R = k + H, de tal modo que H es una clase propiamente primitiva de determinante D (art. 249), entonces 2k + 2H = 2R = K = 2k y, por tanto, 2H coincide con la clase principal, H es ambigua y, por ende, esta contenida entre H, [↑](#footnote-ref-191)
191. Por esta razón, siempre que hablamos simplemente acerca de las formas binarias y ternarias, queremos decir formas binarias o ternarias de segundo grado. [↑](#footnote-ref-192)
192. Trataremos el teorema propuesto en el artículo previo, el cual dice que todas las formas ternarias de un determinante dado pueden ser distribuidas en un nuámero finito de clases, por un metodo analogo al que usamos en el caso de las formas binarias. Primero mostraremos como cada forma ternaria puede ser reducida a una forma mas simple y luego mostraremos que el nuámero de las formas máas simples (que resulta de tales reducciones) es finito para un determinante dado. Supongamos, en general, que [↑](#footnote-ref-193)
193. [↑](#footnote-ref-194)
194. β 7

     0, 1, 70

     0, 0, 1

     tendremos

     m = α, m = α0 + 2b" β + αβ2, m00 = a" + 2b7 + 2b'γ + αγ2 + 2b00 770 + αγ02 n = b + α0γ0 + b0 β + b00( γ + βγ0) + αβγ, n' = b0 + αγ + β'γ', n" = b00 + αβ

     y luego

     M00 = A00, N = B - A00γ0, N0 = B0 - Νβ - Α00γ. [↑](#footnote-ref-195)
195. Si las incognitas de una forma ternaria son x, x' y x", la forma representará námeros dando valores determinados a x, x' y x'' y representara formas binarias mediante las sustituciones

     x = mt + nu, x = mt + n u, x = m t + n u

     donde m, n, m', etc. son numeros a determinar y t y u las incognitas de la forma binaria. Ahora, para completar la teoría de formas ternarias necesitamos una solucion de los siguientes problemas. I. Encontrar todas las representaciones de un numero [↑](#footnote-ref-196)
196. ^—1(19, —3,41) (mod. 770).

     Se sigue de esto que si Δ(ρ, —q, r) no es un residuo cuadrótico de D, φ no podraó representarse propiamente por ninguna forma ternaria de determinante Δ; entonces, en el caso donde Δ y D son primos relativos, Δ tendró que ser el numero característico de la forma φ. [↑](#footnote-ref-197)
197. Obtenemos la transformación de la forma g en la forma f a partir de la transformación de la forma f en la forma g; a partir de esto y de la transformation de la forma f en la forma g obtenemos la transformation de la forma g en la forma g; y a partir de esta, por transposición, la transformation de G en G. [↑](#footnote-ref-198)
198. Representaciones impropias de la forma binaria φ con determinante D por la forma ternaria f, cuya adjunta es F, son aquellas de las cuales deducimos representaciones impropias del numero D por la forma F. Por lo tanto, es claro que φ no se puede representar impropiamente por f a menos que D tenga factores cuadrados. Supongamos que todos los cuadrados (excepto 1) que son divisores de D son e2, e' , e'' , etc. (el numero de ellos es finito ya que hemos excluido la posibilidad de tener D = 0). Toda representación impropia de la forma φ por f daró una representacióon del nuómero D por F, en la cual los valores de las incoógnitas tendróan [↑](#footnote-ref-199)
199. Si pudiéramos tratar más ampliamente este problema, podríamos abreviar, en gran medida, la solución. Es inmediatamente obvio que para χ necesitamos considerar solamente aquellos divisores de e cuyos cuadrados dividen el primer coeficiente de la forma y. Reservaremos para una ocasión mas apropiada un estudio mas profundo de este problema. Note que podemos deducir de el soluciones mas sencillas de los problemas de los artículos 213 y 214. [↑](#footnote-ref-200)
200. Podemos dar aquí solo algunos detalles respecto al tercer problema (al cual hemos reducido los dos primeros); o sea respecto a la manera de juzgar si dos formas ternarias dadas del mismo determinante son o no equivalentes y, si lo son, de que manera encontrar todas las transformaciones de una en la otra. La razon es que la solucion completa, tal como las obtenidas para problemas análogos de formas binarias, presentaría mayores dificultades aquí. Por lo tanto limitaremos nuestra discusion a algunos casos particulares pertinentes a esta divagacion.

     I. Para el determinante +1 mostramos anteriormente que todas las formas ternarias estan repartidas en dos clases, una que contiene todas las formas indefinidas, la otra que contiene todas las formas definidas (negativas). Inmediatamente se concluye que dos formas ternarias cualesquiera de determinante 1 son equivalentes si ambas son definidas o ambas indefinidas; si una es definida y la otra indefinida, no son equivalentes (es claro que la áltima parte de la proposition es valida para el caso general de formas de cualquier determinante). Similarmente, dos formas cualesquiera con determinante —1 son ciertamente equivalentes si ambas son definidas o ambas indefinidas. Dos formas definidas con determinante 2 son siempre equivalentes; dos [↑](#footnote-ref-201)
201. Los otros casos en los que f es una forma definida se pueden reducir a éste; pero si f es una forma indefinida, debe usarse un metodo completamente diferente y el número de transformaciones será infinito. [↑](#footnote-ref-202)
202. PROBLEMA. Dado un número positivo M, encontrar los requisitos que formas binarias primitivas negativas de determinante —M deben satisfacer para que sean residuos cuadráticos de M, eso es, para que tengan 1 como un número característico. [↑](#footnote-ref-203)
203. Esta imposibilidad es también clara por el hecho de que la suma de tres cuadrados impares debe ser ξ 3 (mod. 8); la suma de dos impares con uno par es ξ 2 ó ξ 6; la suma de un impar y dos pares es ξ 1o ξ 5; y finalmente la suma de tres pares es ξ 0 ó ξ 4; pero en el óltimo caso la representación es claramente impropia. [↑](#footnote-ref-204)
204. Siempre debemos entender la palabra “propia” si queremos transferir esta expresión de representaciones a descomposiciones. [↑](#footnote-ref-205)
205. m = aü + bβ + cγ

     n = as» + bβ β + cγ γ

     tenemos, segun el mádulo a

     m0 = bcA002(B2b + C2c) = 0 m00 = bcA02(B2b + C 2c) = 0 n = bcA0A00(B2b + C2c) ξ 0 [↑](#footnote-ref-206)
206. Examinando cuidadosamente la demostracion anterior cualquier persona puede ver fíacilmente que los casos I y II son totalmente completos, de modo que nadie puede objetarlos. Pero las demostraciones de los casos restantes se apoyan en la existencia de nímeros auxiliares, y puesto que su existencia hasta el momento no se ha comprobado, el metodo claramente pierde toda su fuerza. Aunque estas [↑](#footnote-ref-207)
207. PROBLEMA. Dados tres números cualesquiera a, b y c diferentes de cero; encontrar las condiciones para la solubilidad de la ecuación

     ax2 + by2 + cz2 = 0... (ω)

     Solución. Sean α2, β2 y γ2 los maximos divisores cuadrados de bc, ac y ab respectivamente y sea aa = βγΑ, βb = αγΒ, qc = αβΟ. Entonces A, B y C serón enteros primos relativos entre s í; la ecuacion (ω) sera resoluble o no segun

     AX2 + BY2 + CZ2 = 0... (Ω)

     admita o no una solucion de acuerdo con las normas del artículo 294. [↑](#footnote-ref-208)
208. 1 ...1, 2, 3,4, 7

     I. 3 ...11,19, 23, 27, 31,43,67,163

     I. 5 ...47, 79,103,127

     1. 7 ...71,151, 223, 343,463,487

     [↑](#footnote-ref-209)
209. 1... 5, 6, 8, 9,10,12,13,15,16,18, 22, 25, 28, 37, 58 [↑](#footnote-ref-210)
210. Mientras esto estaba en impresión calculamos la tabla hasta -3000 completamente y también para todo el decimo milenio, para muchas centenas separadas y para muchos determinantes individuales cuidadosamente seleccionados. [↑](#footnote-ref-211)
211. Siempre expresamos las clases por las formas (más sencillas) que contienen. [↑](#footnote-ref-212)
212. Esto puede suceder sólo para determinantes irregulares y a será siempre una potencia de 2. [↑](#footnote-ref-213)
213. Por brevedad restringeremos la discusión siguiente al sistema decimal común, pero puede extenderse facilmente a cualquiera otro. [↑](#footnote-ref-214)
214. Robertson (Theory of Circulating Fractions, Philos. Trans. 1769 p. 207) indica el comienzo y el final del período por medio de un punto encima de la primera y de la última cifra, algo que no encontramos necesario aquí. [↑](#footnote-ref-215)
215. Esta es una de las fracciones que aproxima la raíz cuadrada de 23 y el exceso es menor que siete unidades en la vigesima cifra decimal. [↑](#footnote-ref-216)
216. Por brevedad consideraremos juntos los dos casos en los cuales n es divisible y no divisible por p; en el segundo caso es necesario hacer ν = 0. [↑](#footnote-ref-217)
217. Aún más, puesto que, generalmente hablando, entre cualesquiera seis números dados difícilmente habrá uno que no sea divisible por uno de los números 2, 3, 5, ... 19. [↑](#footnote-ref-218)
218. Si el producto de cualquier cantidad de números r, r0, r", etc. es un cuadrado, cada uno de ellos, e.g. r, sera un residuo de cualquier número primo (que no divida a ninguno de ellos) que sea un residuo de los otros, r0, r00, etc. Así, para que los residuos sean independientes, ningún producto de pares o triples, etc. de ellos puede ser cuadrado. [↑](#footnote-ref-219)
219. El autor ha construido para su propio uso una gran parte de la tabla descrita aquí y la habría publicado gustosamente si el pequeño numero de aquellos para quienes sería util bastase para justificar tal empresa. Si hay algún devoto de la aritmetica que comprende los principios involucrados y desea construir una tabla como esta por sí mismo, el autor encontrara gran placer en comunicarle mediante carta todos los procedimientos y artificios que uso. [↑](#footnote-ref-220)
220. En lo que sigue también es posible llamar a la suma el valor numérico del período, o simplemente el período, cuando no haya ambigüedad. [↑](#footnote-ref-221)
221. Funciones invariables son aquéllas en las que todas las incógnitas están contenidas del mismo modo, o, mas claramente, funciones que no cambian no importa la forma en que se presenten las incágnitas; tales son por ejemplo, la suma de las incognitas, su producto, la suma de productos de pares de ellas, etc. [↑](#footnote-ref-222)
222. La base real de este artificio es el hecho, fácil de prever, que el producto no contiene sumas de cuatro terminos sino únicamente sumas de ocho terminos. El matematico entrenado puede comprender facilmente la razún de esto. Por brevedad la omitiremos aquí. [↑](#footnote-ref-223)
223. De esta forma damos una nueva demostración del teorema que dice que —1 es un residuo de todos los nómeros primos de la forma 4k + 1 y un no residuo de todos los de la forma 4k + 3. Antes (art. 108, 109 y 262) probamos esto de varias maneras diferentes. Si es preferible asumir este teorema, no habrá necesidad de distinguir entre los dos casos porque β y γ ya serán enteros. [↑](#footnote-ref-224)
224. Esta proposición puede probarse mucho más directamente a partir de los principios de la sección V. [↑](#footnote-ref-225)
225. \*) Evidentemente M no puede ser de la forma 3z por que, de lo contrario, sería divisible por [↑](#footnote-ref-226)
226. Con respecto a la ambigüedad de si b — c debe ser = N o = — N, es innecesario considerar la cuestión aquí, y por la naturaleza del caso no se puede determinar porque depende de la elección de la raíz primitiva g. Para algunas raíces primitivas la diferencia b — c sera positiva y para otras sera negativa.

     j) Corolario. Sea ε una raíz de la ecuacion x3 — 1 = 0. Tendremos (p + ερ' + ε2ρ'')3 = n (M + NV —27). Sean = cos φ y ^)427 = sen φ y como resultado

     12 1

     p = —— + - cos - φ\Ρη ; M = +1 (mod. 3) ; 1 = M (1 · 2 · 3 ...m)3 (mod. n)

     1. 3 3

     Si se hace 3x + 1 = y, entonces resulta y3 — 3ny — Mn = 0. [↑](#footnote-ref-227)
227. Dos ángulos coinciden en este aspecto si su diferencia es igual a la circunferencia o a un múltiplo de ella. Podemos decir que son congruentes según la circunferencia si queremos usar el termino congruencia en un sentido extendido [↑](#footnote-ref-228)
228. El lector necesita ser escasamente advertido de que nuestras formas ternarias no deben ser confundidas con las que Lagrange llama forme trinaire d’un nombre. Por esta expresión el denota la descomposicion de un número en tres cuadrados. [↑](#footnote-ref-229)