304.

El número de clases propiamente primitivas que corresponden a formas binarias con un determinante cuadrado positivo k^2 puede determinarse completamente a priori; hay tantas clases como números primos relativos a 2k y menores que él. De este hecho y siguiendo un razonamiento fácil, que omitimos aquí, deducimos que el número promedio de clases alrededor de k^2 que pertenecen a tales determinantes es aproximadamente $\frac{8k}{\pi^2}$. Al respecto, sin embargo, determinantes positivos no cuadrados presentan fenómenos singulares. A saber, hay sólo un número pequeño de clases para determinantes pequeños negativos o cuadrados, e.g., clasificación I. 1 ó I. 3 ó 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 sólo una clase está contenida en cada género. 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; sólo uno (37) tiene I. 3; dos (34 y 82) tienen II. 2; uno (79) tiene II. 3. Sin embargo, al aumentar los determinantes, aparecen números 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 clasificación 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 IV. 3; dos tienen IV. 4; cuatro tienen VIII. 2. Los 145 restantes tienen una clase en cada género. Es curioso y sería digno de un geómetra, investigar la ley que justifique el hecho de que los determinantes con una clase por cada género se hacen menos frecuentes. Hasta el momento no podemos asegurar teóricamente ni conjeturar por observación si hay un número finito de ellos (esto es poco probable) o si se hacen infinitamente raros o que su frecuencia tiende a un límite fijo. El número promedio de clases aumenta por una razón ligeramente mayor que la razón con que varía el número de géneros y más 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 número de clases sino este número multiplicado por el logaritmo de $t + u\sqrt{D}$ (t v u son los números menores, diferentes de 1 y 0, que satisfacen la ecuación $t^2 - Du^2 = 1$) el que es análogo al número de clases para un determinante negativo. No podemos explicar esto más a fondo, pero el valor promedio de ese producto es dado aproximadamente por una fórmula como $m\sqrt{D}-n$. Pero aun no hemos podido determinar teóricamente los valores de las constantes m y n. Si se permite llegar a una conclusión válida con base en la comparación de unas cuantas centenas, parece que m es aproximadamente $2\frac{1}{3}$. Reservamos para otra ocasión una discusión más completa de los principios detrás de la discusión anterior sobre los valores promedios de cantidades que no siguen una ley analítica, sino que se aproximan asintóticamente a una ley analítica. Pasamos ahora a otra investigación, la comparación de diferentes clases propiamente primitivas de un mismo determinante y así terminará esta larga sección.

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 progresión C, 2C, 3C, etc. lo suficiente, finalmente obtendremos una clase que es idéntica a K; y suponiendo que mC es la primera que es idéntica a K y que el número de clases en el género principal = n, entonces tendremos que m = n o que m será un factor de n.

Demostración. I. Puesto que todas las clases K, C, 2C, 3C, etc., necesariamente pertenecen al género principal (art. 247), las primeras n+1 clases de la serie K, C, 2C, 3C, ... nC no pueden ser todas diferentes. Entonces, K será idéntica a alguna de las clases C, 2C, 3C, ... nC o al menos dos de ellas serán idénticas entre sí. Sea rC = sC y r > s; se tendrá también

$$(r-1)C=(s-1)C,\quad (r-2)C=(s-2)C$$
 etc. y $(r+1-s)C=C$ por lo tanto $(r-s)C=K.$ Q. E. P.

II. También sigue directamente de esto que m = n o que m < n, y sólo queda demostrar que en el segundo caso m es un factor de n. Puesto que las clases

$$K, C, 2C, \dots (m-1)C$$

las cuales designaremos como \mathfrak{C} , no agotan el género principal, sea C' una clase de este género que no está contenida en \mathfrak{C} . Ahora sea \mathfrak{C}' el conjunto de clases que resulta de la composición de C' con las clases individuales de \mathfrak{C} , a saber

$$C'$$
, $C' + C$, $C' + 2C$, $C' + (m-1)C$

Ahora, obviamente todas las clases en \mathfrak{C}' serán diferentes entre sí, serán diferentes de todas las clases en \mathfrak{C} y pertenecerán al género principal; si \mathfrak{C} y \mathfrak{C}' agotan completamente este género, entonces tendremos n=2m; si no, 2m< n. En el segundo caso sea C'' cualquier clase del género principal que no está comprendida ni en \mathfrak{C} ni en \mathfrak{C}' y designaremos por \mathfrak{C}'' el conjunto de clases que resulta de la composición de la clase C'' con las clases individuales de \mathfrak{C} ; i.e.

$$C''$$
, $C'' + C$, $C'' + 2C$, ... $C'' + (m-1)C$

y es claro que todas éstas son diferentes entre sí y diferentes de todas las clases en \mathfrak{C} y \mathfrak{C}' , y pertenecen al género principal. Ahora, si \mathfrak{C} , \mathfrak{C}' y \mathfrak{C}'' agotan este género, tendremos que n=3m; si no, n>3m. En este caso hay otra clase C''' del género principal que no está comprendida en \mathfrak{C} , \mathfrak{C}' , \mathfrak{C}'' . De manera similar encontramos que n=4m o n>4m y así sucesivamente. Ahora puesto que n y m son finitos, el género principal debe agotarse eventualmente y n será un múltiplo de m, o m un factor de n. Q. E. S.

Ejemplo. Sea D = -356, $C = (5, 2, 72)^*$). 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 \mathfrak{C}' serán (9, -2, 40), (9, 2, 40), (8, -2, 45), (17, 1, 21) y (17, -1, 21).

306.

La demostración del teorema anterior es análoga a las demostraciones en los artículos 45 y 49, y de hecho la teoría de multiplicación de clases es muy afín con el argumento dado en la sección III. Pero las limitaciones de este trabajo no permiten proseguir el tratamiento más profundo que merece esta teoría y sólo agregaremos algunas observaciones, dejando para otra ocasión aquellas demostraciones que requieren mucho detalle.

I. Si la serie K, C, 2C, 3C, ... etc. se extiende más allá de (m-1)C, obtendremos las mismas clases de nuevo.

$$mC = K$$
, $(m+1)C = C$, $(m+2)C = 2C$ etc.

^{*)} Siempre expresamos las clases por las formas (más sencillas) que contienen.

y en general (tomando K como 0C), las clases gC y g'C serán idénticas o diferentes según g y g' sean congruentes o no respecto al módulo m. Por lo tanto la clase nC siempre será idéntica a la clase principal K.

II. El conjunto de clases K, C, 2C, ... (m-1)C que designamos anteriormente como $\mathfrak C$ se llamará el período de la clase C. Esto no debe confundirse con los períodos de formas reducidas de un determinante no cuadrado positivo como se trató en el artículo 186 y siguientes. Es claro por lo tanto que la composición de cualquier número de clases contenidas en el mismo período dará una nueva clase que también estará comprendida en el mismo período

$$gC + g'C + g''C$$
 etc. = $(g + g' + g'' + \text{ etc.})C$

III. Puesto que C + (m-1)C = K, las clases C y (m-1)C serán opuestas, así también 2C y (m-2)C, 3C y (m-3)C etc. Por lo tanto, si m es par, la clase $\frac{1}{2}mC$ será opuesta a sí misma y así, ambigua; recíprocamente si en $\mathfrak C$ aparece alguna clase además de K que sea ambigua, por ejemplo gC, tendremos gC = (m-g)C y así $g = m - g = \frac{1}{2}m$. Se sigue que si m es par no puede haber una clase ambigua en $\mathfrak C$ excepto K y $\frac{1}{2}mC$; si m es impar, ninguna excepto K.

IV. Si suponemos que el período de cualquier clase hC contenida en $\mathfrak C$ es

$$K$$
, hC , $2hC$, $3hC$, ... $(m'-1)hC$

es claro que m'h es el menor multiplo de h divisible por m. Entonces, si h y m son primos relativos, se tendrá m'=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 $m'=\frac{m}{\mu}$. Así es claro que el número de clases comprendidas en el período de cualquier clase de $\mathfrak C$ será m o un factor de m; de hecho habrá tantas clases en $\mathfrak C$ de período m como números en la serie $0, 1, 2, \ldots m-1$ que son primos relativos a m, o sea φm , utilizando la simbología del artículo 39, y en general, habrá tantas clases en $\mathfrak C$ con período $\frac{m}{\mu}$ como números de la serie $0, 1, 2, \ldots m-1$ que tienen a μ como el máximo común divisor de ellos y m. Es fácil ver que el número de ellas será $\varphi \frac{m}{\mu}$. Si por lo tanto m=n o sea el género principal completo está contenido en $\mathfrak C$, habrá φn clases en este género cuyos períodos incluyen todo el género y φe clases cuyos períodos son de e términos, donde e es cualquier divisor de n. Esta conclusión es verdadera cuando existe una clase del género principal cuyo período es de n términos.

V. Bajo la misma suposición, la mejor manera de hacer un arreglo de un sistema de clases del género principal es tomar como base una clase de período n, colocando las clases del género 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 resultará de la composición de cualquiera de las clases del género principal. Aquí sigue un ejemplo para el determinante -356, donde tomamos la clase (9,2,40) como la base:

VI. Aunque tanto una analogía con la sección III como una inducción con más de 200 determinantes negativos y aún más determinantes positivos no cuadrados parecen justificar que la suposición es válida para todo determinante, tal conclusión sería falsa y se refutaría por una extensión de la tabla de clasificaciones. Para brevedad llamaremos regulares a aquellos determinantes para los cuales el género principal completo puede incluirse en un período, e irregulares a aquéllos para los que esto no es posible. Podemos ilustrar con sólo unas pocas observaciones este asunto, el cual depende de los misterios más profundos de la aritmética superior e involucra una investigación difícil. Empezaremos con la siguiente relación general.

VII. Si C y C' son clases del género principal con períodos de m y m' clases, y si M es el menor número divisible por m y m', entonces habrá clases en el mismo género cuyos períodos serán de M términos. Resuelva M en dos factores r y r' primos entre sí, donde uno (r) divide a m, y el otro (r') divide a m' (ver art. 73), y la clase $\frac{m}{r}C+\frac{m'}{r'}C'=C''$ tendrá la propiedad deseada. Pues, supongamos que el período de la clase C'' consiste de q términos, resultará

$$K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C'$$

de donde $\frac{grm'}{r'}$ debe ser divisible por m' o gr por r' y así g por r'. De modo semejante se encuentra que g será divisible por r y por lo tanto por rr' = M. Pero, puesto que MC'' = K, M será divisible por g, y necesariamente M = g. Se sigue que el mayor número de clases (para un determinante dado) contenido en algún período es

divisible por el número de clases en cualquier otro período (de una clase del mismo género principal). Aquí también puede determinarse un método para encontrar la clase que tiene el mayor período (para un determinante regular este período incluye todo el género principal). Este método es completamente análogo al de los artículos 73 y 74, pero en la práctica puede acortarse el trabajo mediante algunos artificios. El cociente del número n por el número de clases en el período mayor será 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 llamará el exponente de irregularidad.

VIII. 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; será suficiente entonces agregar algunas observaciones particulares. Cuando se encuentran más de dos clases ambiguas en el género principal, el determinante es irregular y el exponente de irregularidad es par; pero cuando el género tiene sólo uno o dos, el determinante será regular o al menos el exponente de irregularidad será 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 válido para los determinantes negativos de la forma -(1000k + 75) y -(1000k + 675), con la excepción 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 será divisible por p^2 , de donde sigue que si n no admite divisor cuadrado, el determinante es de seguro regular. Es sólo para determinantes positivos cuadrados e^2 que puede determinarse a priori si son regulares o irregulares; son regulares si e es 1 ó 2 o un número primo impar o una potencia de un número primo impar; en todos los otros casos son irregulares. Para determinantes negativos, conforme aumentan los determinantes, los irregulares se hacen más 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 décimo 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; más allá 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 razón constante respecto a la frecuencia de los

regulares. La determinación de esta razón sería realmente digna de las habilidades de un geómetra. Para determinantes positivos no cuadrados, los irregulares son mucho más escasos; ciertamente hay un número 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.

IX. Por brevedad, no se puede tratar aquí la disposición más cómoda del sistema de clases contenida en un género principal con determinante irregular; sólo observamos que, puesto que una base no es suficiente, hay que tomar dos o más clases, y a partir de su multiplicación y composición producir todas las demás. Así nacen *índices dobles o múltiples* que tendrán la misma función que los índices simples en el caso de determinantes regulares. Pero trataremos este tema en otra ocasión con más detalle.

X. Finalmente hacemos notar que, puesto que todas las propiedades consideradas en este artículo y el anterior dependen especialmente del número n, el cual juega un papel similar al de p-1 en la Sección III, este número merece atención cuidadosa. Es muy deseable por lo tanto determinar la relación general entre este número y el determinante al cual pertenece. No debemos desesperarnos para encontrar la respuesta, puesto que ya hemos logrado establecer (art. 302) la fórmula del valor promedio del producto de n por el número de géneros (que puede determinarse a priori), por lo menos para determinantes negativos.

307.

Las investigaciones de los artículos anteriores sólo toman en cuenta las clases del género principal y así, son suficientes para determinantes positivos cuando hay sólo un género y para determinantes negativos cuando hay sólo un género positivo si no queremos considerar el género negativo. Sólo queda agregar unos cuantos comentarios respecto a los géneros restantes (propiamente primitivos).

I. Cuando G' es un género diferente del género principal G (del mismo determinante) con alguna clase ambigua, habrá tantas en éste como en G. Sean L, M, N, etc. las clases ambiguas en G (entre las cuales estará la clase principal K) y L', M', N', etc., las de G' y designe el primer conjunto por A y el segundo por A'. Puesto que es claro que todas las clases L + L', M + L', N + L', etc., son ambiguas y diferentes entre sí y pertenecen a G', y así también deben estar contenidas en A',

el número de clases en A' no puede ser menor que el número en A, y similarmente, puesto que las clases L' + L', M' + L', N' + L' etc., son diferentes entre sí y ambiguas y pertenecen a G, y por lo tanto están contenidas en A, el número de clases en A no puede ser menor que el número en A'; por esto el número de clases en A y A' son necesariamente iguales.

II. Puesto que el número de todas las clases ambiguas es igual al número de géneros (art. 261, 287.III), es claro que si hay sólo una clase ambigua en G, debe haber una clase ambigua en cada género; si hay dos clases ambiguas en G, habrá dos en la mitad de todos los géneros y ninguna en los restantes; finalmente si hay varias clases en G, digamos a de ellas*), la a-ésima parte de todos los géneros contendrá clases ambiguas, el resto no contendrá ninguna.

III. En el caso donde G contiene dos clases ambiguas, sean G, G', G'', etc., los géneros que contienen dos, y H, H', H'', etc., los géneros que no contienen ninguna, y designe el primer conjunto por \mathfrak{G} y el segundo por \mathfrak{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 composición de dos géneros de \mathfrak{G} siempre da un género de \mathfrak{G} . Además, la composición de un género de \mathfrak{G} con un género de \mathfrak{H} de un género de \mathfrak{H} ; pues, si por ejemplo G'+H no pertenece a \mathfrak{H} sino a \mathfrak{G} , G'+H+G' debe estar en \mathfrak{G} Q. E. A., puesto que G'+G'=G y así G'+H+G'=H. Finalmente los géneros G+H, G''+H, etc. y H+H, H''+H, H''+H, etc. son todos diferentes y así, tomados juntos, deben ser idénticos con \mathfrak{G} y \mathfrak{H} ; pero por lo que acabamos de mostrar los géneros G+H, G''+H, G''+H, G''+H, etc. pertenecen todos a \mathfrak{H} y agotan este conjunto; por lo tanto, necesariamente los restantes G0 y siempre da un género de G1.

IV. Si E es una clase del género V, diferente del género 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 términos, es claro que en la serie E, 2E, 3E, etc. la clase 2mE, y ninguna antes que ella, será idéntica a K; eso es, el período de la clase E contendrá 2m términos. Así pues, el número de términos en el período de cualquier clase de un género que no sea el principal será 2n o un factor de 2n, donde n representa el número de clases en todos los géneros.

^{*)} Esto puede suceder sólo para determinantes irregulares y a será siempre una potencia de 2.

V. 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, K', K'', 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 llamará Ω . El número de estas clases será igual al número de clases ambiguas o sea el número de géneros. Habrá tantas clases en Ω que pertenecen al género V como clases ambiguas en G. Por lo tanto, representando este número por a, en cada género habrá a clases de Ω o bien ninguna. Como resultado, cuando a=1, cada género contendrá una clase de Ω ; cuando a=2, la mitad de todos los géneros contendrá dos clases de Ω , el resto ninguna. De hecho, la mitad coincidirá totalmente con $\mathfrak G$ (según el significado planteado en III) y la segunda mitad con $\mathfrak H$ o vice versa. Cuando a es mayor, la a-ésima parte de todos los géneros incluirá clases de Ω (a clases en cada uno).

VI. Supongamos ahora que C es una clase cuyo período contiene n términos. 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 $2r\equiv 1\pmod{n}$ Q. E. A.). Por lo tanto, puesto que G pertenece a \mathfrak{G} , todas las clases de Ω deben distribuirse entre los géneros \mathfrak{H} . De aquí, puesto que (para un determinante regular) hay en total φn clases en G con períodos de n términos, para el caso cuando a=2 habrá en total $2\varphi n$ clases en cada género de \mathfrak{H} con períodos de 2n términos que incluirán tanto su propio género como el género principal. Cuando a=1 habrá φn de estas clases en cada género excepto el principal.

VII. Dadas esas observaciones, ahora establecemos el siguiente método 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 términos. Este período incluirá tanto su propio género que llamamos V como el género principal G; distribuya las clases de estos dos géneros como se presentan en aquel período. El trabajo estará terminado cuando no hay otros géneros salvo estos dos, o cuando no parece ser necesario agregar el resto de ellos (e.g., para un determinante negativo que posee sólo dos géneros positivos). Pero cuando hay cuatro o más géneros, los restantes se tratarán de la siguiente manera. Sea V' uno cualquiera de ellos, y V + V' = V''. En V' y V'' habrá dos clases ambiguas (una en cada uno o dos en uno y ninguna en el otro). Seleccione una de éstas, 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 agotarán completamente estos géneros; por lo tanto estos géneros también se pueden ordenar. Si hay otros géneros además de estos cuatro, sea V''' uno de los restantes y V'''', V'''''' y V'''''' los géneros que resultan de la composición de V''' con V, V' y V''. Estos cuatro géneros $V''' \dots V'''''''$ 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 $V''' \dots V'''''''$. Si aún hay más géneros restantes, continúe de la misma manera hasta que todos desaparezcan. Obviamente si el número de géneros construidos es 2^{μ} , necesitaremos $\mu - 1$ clases ambiguas en total, y cada clase de estos géneros se puede generar mediante una multiplicación de la clase E o componiendo una clase que resulta de tal multiplicación con una o más de las clases ambiguas. Siguen dos ejemplos de este procedimiento; no diremos más sobre el uso de tal construcción o de los artificios mediante los cuales se puede facilitar el trabajo.

I. El determinante -161.
Cuatro géneros positivos, cuatro clases cada uno

II. El determinante -546
Ocho géneros positivos; tres clases en cada uno