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 matemática. Por esto vale la pena discutir algunas aplicaciones que merecen más amplio desarrollo, sin embargo, sin intentar agotar un tema que puede fácilmente llenar varios volúmenes. En esta sección trataremos primero de la descomposición de fracciones en otras más simples y de la conversión de fracciones comunes en decimales. Explicaremos luego un método de exclusión que será útil para la solución de ecuaciones indeterminadas de segundo grado. Finalmente, daremos nuevos métodos reducidos para distinguir números primos de números compuestos y para encontrar los factores de estos últimos. En la sección siguiente estableceremos la teoría general de una clase especial de funciones que tiene mucha importancia en todo el análisis y que está estrechamente vinculada con la aritmética superior. En particular agregaremos nuevos resultados a la teoría de secciones de un círculo. Hasta ahora sólo los primeros elementos de esta teoría han sido conocidos.

De la descomposición de fracciones en otras más simples

309.

PROBLEMA. *Descomponer la fracción* $\frac{m}{n}$*, 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 $\frac{x}{a}$ e $\frac{y}{b}$ las fracciones deseadas; se debe tener $bx + ay = m$; entonces x será una raíz de la congruencia $bx \equiv m \pmod{a}$ que puede ser encontrada por los métodos de la Sección II. Además y será $= \frac{m-bx}{a}$.

Es claro que la congruencia $bx \equiv m$ tiene infinitas raíces, todas conguentes relativas a a; pero hay únicamente una que es positiva y menor que a. También es posible que y sea negativo. Es apenas necesario hacer notar que podemos también encontrar y por la congruencia $ay \equiv m \pmod{b}$ y x por la ecuación $x = \frac{m-ay}{b}$. Por ejemplo, dada la fracción $\frac{58}{77}$, 4 será un valor de la expresión $\frac{58}{11} \pmod{7}$, por tanto $\frac{58}{77}$ se descompondrá en $\frac{4}{7} + \frac{2}{11}$.

310.

Si se propone la fracción $\frac{m}{n}$ 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 serán a y bcd, etc.; luego la segunda de éstas en dos fracciones con denominadores b y cd, etc.; la última de éstas en otras dos y así sucesivamente hasta que toda la fracción dada es reducida a la forma

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \text{ etc.}$$

Evidentemente se pueden tomar los numeradores α, β, γ, δ, etc., positivos y menores que sus denominadores, excepto para el último, 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 será ventajoso ponerlo en la forma $\frac{\varepsilon}{e} \mp k$ donde ε es positivo y menor que e y k es un entero. Y finalmente a, b, c, etc. pueden ser tomados como números primos o como potencias de números primos.

Ejemplo. La fracción $\frac{391}{924}$ cuyo denominador $= 4 \cdot 3 \cdot 7 \cdot 11$ es resuelta de esta manera en $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ en $\frac{2}{3} - \frac{38}{77}$; $\frac{-38}{77}$ en $\frac{1}{7} - \frac{7}{11}$ y escribiendo $\frac{4}{11} - 1$ por $-\frac{7}{11}$, tenemos $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311.

La fracción $\frac{m}{n}$ puede descomponerse *de una única manera,* en la forma $\frac{\alpha}{a} + \frac{\beta}{b} +$ etc. $\mp k$ tal que α, β, etc., sean positivos y menores que a, b etc.; esto es, suponiendo que

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{ etc.} \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \text{ etc.} \mp k'$$

y si α', β', etc., son también positivos y menores que a, b, etc., tendremos necesariamente $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, etc., $k = k'$. Porque si multiplicamos por $n = abc$ etc., tenemos $m \equiv \alpha bcd$ etc. $\equiv \alpha' bcd$ etc. (mod. a) y así, puesto que bcd etc. es primo relativo a a, necesariamente $\alpha \equiv \alpha'$ y por lo tanto $\alpha = \alpha'$ y entonces $\beta = \beta'$, 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 βacd etc. $\equiv m$ (mod. b), γ por γabd etc. $\equiv m$ (mod. c) etc. La suma de todas las fracciones así encontradas será igual a la fracción $\frac{m}{n}$ o la diferencia será el entero k. Esto nos da un medio de verificar el cálculo. Así en el artículo precedente los valores de la expresión $\frac{391}{231}$ (mod. 4), $\frac{391}{308}$ (mod. 3), $\frac{391}{132}$ (mod. 7), $\frac{391}{84}$ (mod. 11), proporcionarán inmediatamente los numeradores 1, 2, 1 y 4 correspondientes a los denominadores 4, 3, 7 y 11 y la suma de estas fracciones excederá a la fracción dada en una unidad.

La conversión de fracciones comunes en decimales.

312.

Definición. Si una fracción común es convertida en un decimal, a la serie de cifras decimales *) (excluyendo la parte entera si la hay), tanto si es finita o infinita, la llamaremos *mantisa* de la fracción. Aquí hemos tomado una expresión, que hasta ahora ha sido usada solamente para logaritmos, y extendido su uso. Así, e.g., la mantisa de la fracción $\frac{1}{8}$ es 125, la mantisa de la fracción $\frac{35}{16}$ es 1875, y la de la fracción $\frac{2}{37}$ es 054054 ... infinitamente repetida.

De la definición, es inmediatamente claro que fracciones del mismo denominador $\frac{l}{n}$ y $\frac{m}{n}$ tendrán la misma o diferente mantisa de acuerdo con que los numeradores

*) Por brevedad restringeremos la discusión siguiente al sistema decimal común, pero puede extenderse fácilmente a cualquiera otro.

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 $\frac{10m}{n}$ se obtiene desechando de la mantisa de la fracción $\frac{m}{n}$ la primera cifra y en general la mantisa de la fracción $\frac{10^\nu m}{n}$ se encuentra omitiendo las primeras ν cifras de la mantisa de $\frac{m}{n}$. La mantisa de la fracción $\frac{1}{n}$ 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 número de cifras de las cuales está formada es k, las primeras $k-1$ cifras de la mantisa de $\frac{1}{n}$ serán ceros y la k-ésima será significativa. Por lo tanto, si $\frac{l}{n}$ y $\frac{m}{n}$ tienen mantisas diferentes (i.e. si l y m no son congruentes según n), ellas de hecho no pueden tener las primeras k cifras idénticas, sino que deben diferir al menos en la k-ésima.

313.

PROBLEMA. *Dado el denominador de la fracción $\frac{m}{n}$ 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 10^k (u omita las últimas k cifras). Si el cociente es un entero (o todas las cifras omitidas son ceros), será evidentemente el número buscado y la mantisa dada estará completa; de otra forma el numerador que buscamos será el siguiente entero más grande, o el cociente aumentado en una unidad, después de omitir las siguientes cifras decimales. La razón de esta regla se entiende tan fácilmente a partir de lo establecido al final del artículo precedente que no es necesaria una explicación más 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 $23 \cdot 69 = 1587$. Desechando las últimas dos cifras y agregando una unidad, se produce el número 16 para el numerador buscado.

314.

Comenzamos con una consideración de fracciones cuyos denominadores son primos o potencias de primos, y posteriormente reduciremos las demás a este caso. Observamos inmediatamente que la mantisa de la fracción $\frac{a}{p^\mu}$ (suponemos que el numerador a no es divisible por el número primo p) es finita y consiste de μ cifras

cuando $p = 2$ ó $= 5$; en el primer caso esta mantisa, considerada como un entero será $= 5^\mu a$, en el último caso $= 2^\mu a$. Esto es tan obvio que no necesita explicación.

Pero si p es otro número primo, $10^r a$ nunca será divisible por p^μ, no importa cuán grande tomemos a r, y por lo tanto, la mantisa de la fracción $F = \frac{a}{p^\mu}$ debe ser infinita. Supongamos que 10^e es la menor potencia del número 10 que es congruente con la unidad relativo al módulo p^μ (cf. Sección III, donde probamos que e es o igual al número $(p-1)p^{\mu-1}$ o a un divisor de él.) Obviamente $10^e a$ es el primer número en la serie $10a$, $100a$, $1000a$, etc., que es congruente a a relativo al mismo módulo. Ahora ya que, de acuerdo con el artículo 312, obtenemos las mantisas de las fracciones $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$,... $\frac{10^e a}{p^\mu}$ suprimiendo la primera cifra de la fracción F, luego las dos primeras cifras, etc., hasta que se hayan suprimido las e primeras cifras, es evidente que únicamente después de las e primeras cifras, y no antes, las mismas se repetirán. Llamaremos a estas primeras e cifras que forman la mantisa por repetición infinita de ellas mismas el *período* de esta mantisa o de la fracción F. La magnitud del período, i.e. el número e de cifras en él, es completamente independiente del numerador a y es determinado sólo por el denominador. Así, e.g., el período de la fracción $\frac{1}{11}$ es 09 y el período de la fracción $\frac{3}{7}$ es 428571*).

315.

Así cuando se conoce el período de alguna fracción, se puede obtener la mantisa con tantas cifras como queramos. Ahora, si $b \equiv 10^\lambda a \pmod{p^\mu}$, podemos conseguir el período para la fracción $\frac{b}{p^\mu}$ si se escriben las primeras λ cifras del período de la fracción F (suponiendo que $\lambda < e$, lo cual es permisible) después de las restantes $e - \lambda$. Así, junto con el período de la fracción F, tendremos al mismo tiempo los períodos de todas las fracciones cuyos numeradores sean congruentes a los números $10a$, $100a$, $1000a$, etc., relativos al denominador p^μ. Así, e.g., ya que $6 \equiv 3 \cdot 10^2 \pmod 7$, el período de la fracción $\frac{6}{7}$ se puede deducir inmediatamente del período de la fracción $\frac{3}{7}$, y él es 857142.

Por lo tanto, siempre que 10 es una raíz primitiva (art. 57 y 89) para el módulo p^μ, del período de la fracción $\frac{1}{p^\mu}$ puede deducirse inmediatamente el período de cualquiera otra fracción $\frac{m}{p^\mu}$ (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

*) 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.

m cuando el número 10 es tomado como base. Así, es claro por qué en este caso el número 10 se tomó siempre como base en la Tabla 1 (ver art. 72).

Cuando 10 no es una raíz primitiva, los únicos períodos de fracciones que pueden ser derivados del período de la fracción $\frac{1}{p^\mu}$ son aquéllos cuyos numeradores son congruentes a alguna potencia de 10 según p^μ. Sea 10^e la más pequeña potencia de 10 que es congruente a la unidad según p^μ; sea $(p-1)p^{\mu-1} = ef$ 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 $\frac{1}{p^\mu}$ tendrán como índices f, $2f$, $3f$, $\ldots ef - f$; similarmente, del período de la fracción $\frac{r}{p^\mu}$, 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 fracción con numerador r^2 (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^i 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, r^2, r^3, $\ldots$, r^{f-1}, se puede obtener todos los otros por transposición sola con la ayuda de la siguiente regla: Sea i el índice del numerador m de una fracción dada $\frac{m}{p^\mu}$ en un sistema donde r es tomado como base (suponemos que i es menor que $(p-1)p^{\mu-1}$); dividiendo por f encontramos $i = \alpha f + \beta$, donde α y β son enteros positivos (ó 0) y $\beta < f$; teniendo esto, podemos encontrar el período de la fracción $\frac{m}{p^\mu}$ a partir del período de la fracción cuyo numerador es r^β (es 1 cuando $\beta = 0$), poniendo las primeras α cifras después de la restantes (cuando $\alpha = 0$ mantenemos el mismo período). Esto explica cómo en la construcción 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 p^μ menores que 1000, que publicaremos íntegramente o incluso con extensiones posteriores si una ocasión se presenta. Por ahora damos como una muestra la Tabla III, que se extiende únicamente hasta 100 y no necesita explicación. 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 demás, da los f períodos correspondientes a los numeradores 1, r, r^2, $\ldots$, r^{f-1} que se denominan por los números (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 más de 2). Ahora examinamos todos los períodos correspondientes al denominador dado, hasta que encontremos estas cifras iniciales, las cuales marcarán el inicio del período. Conviene advertir que estas cifras pueden ser separadas de modo que una (o más) aparezcan al final de un período y las otras al comienzo.

Ejemplo. Búsquese el período de la fracción $\frac{12}{19}$. Para el módulo 19, por Tabla I tenemos $\text{ind.}\, 12 = 2\,\text{ind.}\, 2 + \text{ind.}\, 3 = 39 \equiv 3 \pmod{18}$ (art. 57). Ya que para este caso existe únicamente un período correspondiente al numerador 1, es necesario transponer las primeras tres cifras al final y resulta el período buscado: 631578947368421052. Habría sido igualmente fácil encontrar el comienzo del período por las primeras dos cifras, 63.

Si uno desea el período de la fracción $\frac{45}{53}$, $\text{ind.}\, 45 = 2\,\text{ind.}\, 3 + \text{ind.}\, 5 = 49$, para el módulo 53. El número 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 posición final y el período buscado es 8490566037735. Las cifras iniciales, 84, están separadas en la tabla.

Observaremos aquí, como prometimos en el artículo 59, que con la ayuda de la Tabla III podemos también encontrar el número que corresponde a un índice dado para un módulo dado (en la tabla el módulo se lista como un denominador). Por esto es claro, de lo que precede, que se puede encontrar el período de una fracción 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 número correspondiente al índice dado.

317.

Por el método precedente, la mantisa de cualquier fracción cuyo denominador es un número primo o una potencia de un número primo dentro de los límites de la tabla, se puede determinar sin cálculo. Pero con la ayuda del resultado del comienzo de esta sección, podemos extender el uso de esta tabla más allá 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 éstas pueden ser convertidas en fracciones decimales con cualquier número 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, será apropiado computarlas a más cifras que las que se buscan para la fracción dada. Por ejemplo, consideremos la fracción $\frac{6099380351}{1271808720} = F$*), cuyo denominador es el producto de los números 16, 9, 5, 49, 13, 47 y 59. Por las reglas dadas arriba encontramos que $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$; estas fracciones individuales se convierten en decimales como sigue:

$$
\begin{array}{rlll}
1 &= 1 & & \\
\frac{11}{16} &= 0.6875 & & \\
\frac{4}{5} &= 0.8 & & \\
\frac{4}{9} &= 0.4444444444 & 4444444444 & 44 \\
\frac{22}{49} &= 0.4489795918 & 3673469387 & 75 \\
\frac{5}{13} &= 0.3846153846 & 1538461538 & 46 \\
\frac{7}{47} &= 0.1489361702 & 1276595744 & 68 \\
\frac{52}{59} &= 0.8813559322 & 0338983050 & 84 \\
\hline
F &= 4.7958315233 & 1271954166 & 17
\end{array}
$$

El error en esta suma es ciertamente menor que cinco unidades en la vigésima segunda cifra y así las primeras veinte son exactas. Llevando los cálculos a más cifras, encontramos en lugar de las últimas dos cifras, 17, el número 1893936.... Será obvio para todos que este método de convertir fracciones comunes en decimales es especialmente útil cuando buscamos una gran cantidad de cifras decimales; cuando

*) Esta es una de las fracciones que aproxima la raíz cuadrada de 23 y el exceso es menor que siete unidades en la vigésima cifra decimal.

unas pocas bastan, la división ordinaria o los logaritmos pueden ser usados con igual facilidad.

318.

De esta manera, ya que hemos reducido la resolución 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 también consistirá de períodos, porque en este caso la serie 10, 100, 1000, etc. llegará eventualmente a un término que es congruente a la unidad según el denominador. A la vez el exponente de este término, que puede fácilmente determinarse por los métodos del artículo 92, indicará el tamaño del período independientemente del numerador, siempre que sea primo relativo al denominador. Si el denominador es de la forma $2^\alpha 5^\beta N$, 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 fracción llegará a ser periódica después de las primeras α o β cifras (el que sea mayor) y los períodos tendrán la misma longitud que los períodos de fracciones que tienen denominador N. Esto es fácil de ver, ya que la fracción es resoluble en otras dos con denominadores $2^\alpha 5^\beta$ y N, y la primera de ellas cesa enteramente después de las primeras α o β cifras. Podemos fácilmente agregar muchas otras observaciones concernientes a este asunto, especialmente en lo que se refiere a artificios para la construcción de una tabla como la III. Sin embargo omitiremos esta discusión, 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 $x^2 \equiv A$ por el método de exclusión.

319.

Con respecto a la congruencia $x^2 \equiv A \pmod{m}$, la cual es equivalente a la ecuación indeterminada $x^2 = A + my$, en Sección IV (art. 146) hemos tratado su *posibilidad* de una manera que no parece requerir ningún estudio adicional. Para encontrar la incógnita misma, sin embargo, observamos antes (art. 152) que los métodos indirectos son preferibles a los directos. Si m es un número primo (los otros casos pueden ser reducidos fácilmente a éste), podemos usar la tabla de índices 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 método general y conciso placerá a los aficionados de la aritmética.

Primero observamos que es suficiente conocer solamente aquellos valores de x que son positivos y no mayores que $\frac{1}{2}m$, ya que los otros serán congruentes módulo m a uno de éstos, tomado ya sea positiva o negativamente. Para un tal valor de x, el valor de y está necesariamente contenido dentro de los límites $-\frac{A}{m}$ y $\frac{1}{4}m - \frac{A}{m}$. Por ende el método 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 éste, V) y retenemos solamente aquellos valores para los cuales V es un cuadrado. Cuando m es un número pequeño (e.g. abajo de 40), el número de pruebas es tan pequeño 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 cuadráticos diferentes (i.e. no congruentes según E); y sean α, β, γ, etc. las raíces de las congruencias

$$A + my \equiv a, \qquad A + my \equiv b, \qquad A + my \equiv c, \quad \text{etc.}$$

según el módulo E, con todas estas raíces positivas y menores que E. Si y es un valor congruente a uno de los números α, β, γ, etc., entonces el valor resultante de $V = A + my$ será congruente a uno de los números a, b, c, etc. y así será un no residuo de E y no podrá ser un cuadrado. Así, inmediatamente, pueden excluirse como inservibles todos los valores en Ω que están contenidos en las formas $Et + \alpha$, $Et + \beta$, $Et + \gamma$, etc.; será suficiente examinar a los demás y llamaremos a este conjunto Ω'. En esta operación el número E puede llamarse número *excluyente.*

Tomando otro número excluyente E' apropiado, del mismo modo se encuentran tantos números α', β', γ', etc. como no residuos cuadráticos diferentes haya; y no puede ser congruente a ellos según el módulo E'. Ahora se puede remover de nuevo de Ω' todos los números contenidos en las formas $E't + \alpha'$, $E't + \beta'$, $E't + \gamma'$, etc. De esta manera se puede continuar excluyendo números hasta que aquellos contenidos en Ω sean reducidos hasta el punto que no haya más dificultad en examinar los restantes que en construir nuevas exclusiones.

Ejemplo. Dada la ecuación $x^2 = 22 + 97y$, los límites de los valores de y serán $-\frac{22}{97}$ y $24\frac{1}{4} - \frac{22}{97}$. Así (ya que el valor 0 es obviamente inútil) Ω incluirá los números 1, 2, 3, ... 24. Para $E = 3$ hay únicamente un no residuo, $a = 2$; así $\alpha = 1$. Excluyendo de Ω todos los números de la forma $3t + 1$, Ω' contendrá los 16 números restantes. Similarmente, para $E = 4$ resulta $a = 2$, $b = 3$, y así $\alpha = 0$, $\beta = 1$; y debemos desechar los números de la forma $4t$ y $4t + 1$. Los ocho números restantes son 2, 3, 6, 11, 14, 15, 18 y 23. Igualmente, para $E = 5$ se debe desechar los números de la forma $5t$ y $5t + 3$ y se quedan 2, 6, 11 y 14. Tomando $E = 6$, se deben remover los números de la forma $6t + 1$ y $6t + 4$, pero éstos ya habían sido removidos (ya que son números de la forma $3t + 1$). Tomando $E = 7$, desechamos los números de la forma $7t + 2$, $7t + 3$, $7t + 5$ y se dejan 6, 11 y 14. Si sustituimos y por éstos, dan $V = 604$, 1089 y 1380 respectivamente. Unicamente el segundo valor es un cuadrado, así $x = \mp 33$.

321.

Como la operación con el número excluyente E desecha de los valores de V correspondientes a los valores de y en Ω, todos aquéllos que son no residuos cuadráticos de E, pero no toca los residuos del mismo número, 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. Así, si usamos sucesivamente los números 3, 4, 5, etc. como excluyentes, podemos omitir los números $\equiv 2 \pmod 4$, es decir 6, 10, 14, etc., como superfluos. La doble operación, usando E y E' como excluyentes, remueve todos aquellos valores de V que son no residuos de ambos E y E' o de uno de ellos y deja todos los que son residuos de ambos. Ahora, ya que en el caso en que E y E' no tienen un divisor común, los números desechados son todos no residuos y los que permanecen son residuos del producto EE', es evidente que, usando el excluyente EE', se obtendrá en efecto el mismo resultado que usando los dos E y E' y su uso es, por lo tanto, superfluo. Así, es permisible omitir todos aquellos números excluyentes que pueden ser resueltos en dos factores relativamente primos, y es suficiente usar aquéllos que son o primos (no divisores de m) o potencias de primos. Finalmente es claro que, después de usar el número excluyente p^μ que es una potencia del número primo p, los números excluyentes p y p^ν con $\nu < \mu$ son superfluos. Pues, ya que p^μ deja solamente sus residuos de entre los valores de V, ciertamente no habrá no residuos de p o de una potencia menor p^ν. Si p o p^ν fueron usados antes que p^μ, el último evidentemente puede desechar solamente aquellos valores de V que son al

mismo tiempo residuos de p (o p^ν) y no residuos de p^μ; por lo tanto es suficiente tomar para a, b, c, etc., únicamente tales no residuos de p^μ.

322.

El cálculo de los números α, β, γ, etc. correspondientes a cualquier excluyente dado E, puede ser en gran parte abreviado por las siguientes observaciones. Sean $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. raíces de las congruencias $my \equiv a$, $my \equiv b$, $my \equiv c$, etc. (mod. E) y k una raíz de $my \equiv -A$. Es claro que $\alpha \equiv \mathfrak{A} + k$, $\beta \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k$, etc. Ahora, si fuera necesario encontrar $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. resolviendo estas congruencias, este método de encontrar α, β, γ, etc. no sería más 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 cuadrático de E, es claro por el artículo 98 que $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., i.e., los valores de las expresiones $\frac{a}{m}$, $\frac{b}{m}$, $\frac{c}{m}$, etc. (mod. E), son no residuos diferentes de E y así son idénticos con α, β, γ, etc., si no prestamos atención a su orden, el cual de todas formas no importa aquí. Si en la misma suposición m es un no residuo de E, los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., son idénticos con todos los residuos cuadráticos, excluyendo el 0. Si E es el cuadrado de un número primo (impar), $= p^2$, 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 p^2 que son residuos de p, i.e. los números p, $2p$, $3p$, $\ldots p^2 - p$ (todos los números menores que p^2 que son divisibles por p, excepto 0); entonces para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., debemos obtener exactamente los mismos números pero en diferente orden. Similarmente, si se pone $E = p^3$ después de aplicar los números excluyentes p y p^2, será suficiente tomar para a, b, c, etc. los productos de cada uno de los no residuos de p por p^2. Como un resultado obtendremos para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., o los mismos números o los productos de p^2 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 p^μ, después de aplicar todas las potencias menores, obtendremos para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. los productos de $p^{\mu-1}$ 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 $\mathfrak{A}$, $\mathfrak{B}$, o 2 y 3 o 2 y 1, según sea $m \equiv 1$ ó $\equiv 3$ (mod. 4). Si después de usar el excluyente 4, ponemos $E = 8$ tendremos $\alpha = 5$ y $\mathfrak{A}$ sería 5, 7, 1, 3 según sea $m \equiv 1, 3, 5, 7$ (mod. 8). En general, si E es una potencia más alta de 2, digamos 2^μ, y todas las potencias menores ya han sido aplicadas, debe ponerse $a = 2^{\mu-1}$, $b = 3 \cdot 2^{\mu-2}$ cuando μ es par. Esto nos da $\mathfrak{A} = 2^{\mu-1}$ y $\mathfrak{B} = 3 \cdot 2^{\mu-1}$ o

$= 2^{\mu-2}$ según sea $m \equiv 1$ o $\equiv 3$. Pero cuando μ es impar, debemos poner $a = 5 \cdot 2^{\mu-3}$ y $\mathfrak{A}$ será igual al producto del número $2^{\mu-3}$ por 5, 7, 1 o 3 según sea $m = 1$, 3, 5 o 7 (mod. 8).

Pero un matemático experto fácilmente encontrará un método para desechar *mecánicamente* los valores de y inservibles que están en Ω después 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 $mx^2 + ny^2 = A$ por exclusiones.

323.

En la sección V dimos un método general para encontrar todas las representaciones de un A dado por la forma binaria mx^2+ny^2 o sea para encontrar las soluciones de la ecuación indeterminada $mx^2 + ny^2 = A$. El método no deja nada que desear desde el punto de vista de brevedad si ya tenemos todos los valores de la expresión $\sqrt{-mn}$ 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 solución que es mucho más corta que la directa cuando aquellos valores no hayan sido computados. Supongamos que los números m, n y A son positivos y primos entre sí, ya que el otro caso puede fácilmente ser reducido a éste. Será suficiente deducir valores positivos de x e y, ya que los otros pueden ser reducidos a éstos por un sencillo cambio de signos.

Claramente x debe ser tal que $\frac{A-mx^2}{n}$, el cual designaremos por V, es positivo, entero, y cuadrado. La primera condición requiere que x no sea mayor que $\sqrt{\frac{A}{m}}$; la segunda se tiene cuando $n = 1$, de otro modo requiere que el valor de la expresión $\frac{A}{m}$ (mod. n) sea un residuo cuadrático de n. Si designamos todos los diferentes valores de la expresión $\sqrt{\frac{A}{m}}$ (mod. n) por $\pm r$, $\pm r'$, etc., x deberá estar contenido en una de las formas $nt + r$, $nt - r$, $nt + r'$, etc. La manera más simple será sustituir x por todos los números de estas formas abajo del límite $\sqrt{\frac{A}{m}}$ (llamaremos a este conjunto Ω) y conservar únicamente aquéllos para los cuales V es un cuadrado. En el siguiente artículo mostraremos cómo reducir el número de estas pruebas tanto como deseemos.

324.

El método de exclusiones por el cual efectuamos esto, tal como en la discusión precedente, consiste en tomar arbitrariamente varios números que nuevamente llamaremos números *excluyentes*, en buscar los valores de x para los cuales el valor

V se convierte en un no residuo de estos números excluyentes y en desechar de Ω estos valores de x. El razonamiento aquí es totalmente análogo al del artículo 321, y así deberemos usar como números excluyentes solamente aquéllos 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 número primo, si es que comenzamos la exclusión con éstas.

Por lo tanto, sea $E = p^\mu$ el número excluyente (incluyendo también el caso donde $\mu = 1$) con p un número primo que no divide m, y supongamos *) que p^ν es la mayor potencia de p que divide a n. Sean a, b, c, etc. no residuos cuadráticos de E (todos ellos cuando $\mu = 1$; los necesarios, i.e. aquéllos que son residuos de potencias inferiores, cuando $\mu > 1$). Compute las raíces α, β, γ, etc. de las congruencias $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$, etc. (mod. $Ep^\nu = p^{\mu+\nu}$). Es fácil ver que si para algún valor de x resulta $x^2 \equiv \alpha \pmod{Ep^\nu}$, el correspondiente valor de V será $\equiv a \pmod{E}$, esto es, un no residuo de E y similarmente para los restantes números β, γ, etc. Recíprocamente, es igualmente fácil ver que si un valor de x produce $V \equiv a \pmod{E}$, para el mismo valor se hace $x^2 \equiv \alpha \pmod{Ep^\nu}$. Así, todos los valores de x para los cuales x^2 no es congruente a alguno de los números α, β, γ, etc. (mod. Ep^ν) 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 cuadráticos g, g', g'', etc. de Ep^ν. Compute los valores de las expresiones $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, etc. (mod. Ep^ν) y desígnelos como $\pm h$, $\pm h'$, $\pm h''$, etc. Habiendo hecho esto, todos los números de las formas $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$, 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 después de esta exclusión. Además es evidente que valores de x en Ω no pueden producir tales valores de V cuando ninguno de los números α, β, γ, etc. es un residuo cuadrático de Ep^ν. 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 números en Ω a voluntad.

Veamos ahora si es permisible usar primos que dividen a m o potencias de tales números primos como números excluyentes. Sea B un valor de la expresión $\frac{A}{n} \pmod{m}$; es claro que V será siempre congruente a B según el módulo m, no importa que valor se tome para x. Así, para que la ecuación propuesta sea posible, es necesario que B sea un residuo cuadrático de m. Si p es un divisor primo e impar de

*) 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 $\nu = 0$.

m, por hipótesis, no divide a n o a A y por eso no divide a B. Para cualquier valor de x, V será un residuo de p y así también 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 ecuación propuesta, se requiere que $B \equiv 1 \pmod 8$ y así, para cualquier valor de x, V será $\equiv 1 \pmod 8$ y las potencias de 2 no serán idóneas como excluyentes. Sin embargo, cuando m es divisible por 4 pero no por 8, por la misma razón debemos tener $B \equiv 1 \pmod 4$ y el valor de la expresión $\frac{A}{n} \pmod 8$ será o 1 o 5 y lo designaremos por C. Para un valor par de x tendremos $V \equiv C$; para un valor impar $V \equiv C + 4 \pmod 8$. 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 expresión $\frac{A}{n} \pmod 8$ que será 1, 3, 5 o 7; y sea D un valor de $\frac{\frac{1}{2}m}{n} \pmod 4$ el cual será 1 o 3. Ahora, ya que el valor de V es siempre $\equiv C - 2Dx^2 \pmod 8$ y así para x par, $\equiv C$, para x impar, $\equiv C - 2D$, se sigue que todos los valores impares de x deben ser desechados cuando $C = 1$, todos los valores pares cuando $C = 3$ y $D = 1$ o $C = 7$ y $D = 3$. Todos los valores restantes producirán $V \equiv 1 \pmod 8$; 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 $C = 7$ y $D = 1$, tenemos $V \equiv 3, 5 \text{ o } 7 \pmod 8$, no importa si x es impar o par. Se sigue en estos casos que la ecuación propuesta no tiene solución del todo.

Ahora, de la misma forma en que encontramos x por el método de exclusión, podemos también encontrar y. Así, hay siempre dos maneras de aplicar el método de exclusión para la solución de un problema dado (a menos que $m = n = 1$, cuando los dos coinciden). Deberíamos usualmente escoger aquél para el cual el número de términos Ω es menor, lo que se puede estimar fácilmente por adelantado. Es apenas necesario observar que si, después de un número de exclusiones, *todos* los números en Ω son desechados, esto debe ser considerado como una indicación segura de la imposibilidad de la ecuación propuesta.

325.

Ejemplo. Sea la ecuación dada $3x^2 + 455y^2 = 10857362$. La resolveremos de dos maneras, *primero* investigando los valores de x y luego los valores de y. El límite en x aquí es $\sqrt{3619120\frac{2}{3}}$, el cual cae entre 1902 y 1903; el valor de la expresión $\frac{A}{3} \pmod{455}$ es 354 y los valores de la expresión $\sqrt{354} \pmod{455}$ 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 exclusión porque divide a m. Para el número excluyente 4, tenemos $a = 2$, $b = 3$ así $\alpha = 0$, $\beta = 3$, $g = 0$ y los valores de la expresión $\sqrt{g}$ (mod. 4) son 0 y 2; así, todos los números de la forma $4t$ y $4t + 2$, i.e. todos los números pares, deben ser desechados de Ω; denotaremos los 16 restantes por Ω'. Para $E = 5$, el cual también divide a n, las raíces de las congruencias $mz \equiv A - 2n$ y $mz \equiv A - 3n$ (mod. 25) son 9 y 24, ambos residuos de 25. Los valores de las expresiones $\sqrt{9}$ y $\sqrt{24}$ (mod. 25) son ± 3, ± 7. Cuando desechamos de Ω' todos los números de las formas $25t \pm 3$, $25t \pm 7$, allí permanecen estos diez (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Para $E = 7$ las raíces de las congruencias $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) son 32, 39, 18, todas ellas residuos de 49, y los valores de las expresiones $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) son ± 9, ± 23, ± 19. Cuando desechamos de Ω'' los números de las formas $49t \pm 9$, $49t \pm 19$ y $49t \pm 23$, estos cinco (Ω''') permanecen: 537, 737, 1083, 1213, 1517. Para $E = 8$ tenemos $a = 5$, así $\alpha = 5$, 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 números a, b, etc. se convierten en 2, 6, 7, 8, 10; $\nu = 0$; así los números α, β, etc. = 8, 10, 5, 0, 1. Tres de ellos, 0, 1, 5 son residuos de 11 y por esta razón desechamos de Ω''' los números de las formas $11t$, $11t \pm 1$, $11t \pm 4$. Permanecen los números 537, 1083, 1213. Usando éstos obtenemos para V los valores 21961, 16129, 14161 respectivamente. Solamente el segundo y el tercero son cuadrados. Así 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 incógnita de esta misma ecuación por exclusiones, intercambiamos x e y y la escribimos como $455x^2 + 3y^2 = 10857362$, así que podemos retener la notación de los artículos 323 y 324. El límite para los valores de x cae entre 154 y 155; el valor de la expresión $\frac{A}{m}$ (mod. n) es 1; los valores de $\sqrt{1}$ (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 $9t \pm 4$; $4t$, $4t \pm 2$, o sea todos los pares; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, 17 ± 5, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. Después de que todos éstos han sido suprimidos, hemos dejado los números 119 y 127, que dan

a V un valor cuadrado y producen las mismas soluciones que obtuvimos arriba.

326.

Los métodos 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 discusión 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 análogo o reducidos a éste. 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 $\frac{A}{m}$, $-\frac{na}{m}$, $-\frac{nb}{m}$, $-\frac{nc}{m}$, etc. (mod. p) son k, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. respectivamente, se obtienen los números α, β, γ, etc. de las congruencias $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$, etc. (mod. p). Los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. pueden ser determinados, sin calcular las congruencias, por un artificio muy parecido al que usamos en el artículo 322, y serán idénticos con todos los no residuos o con todos los residuos de p (excepto 0), de acuerdo con el valor de la expresión $-\frac{m}{n}$ (mod. p), o (lo que es la misma cosa) según sea el número $-mn$ un residuo o un no residuo de p. Así, en el ejemplo II del artículo precedente, para $E = 17$ tenemos $k = 7$; $-mn = -1365 \equiv 12$ es un no residuo de 17; así, los números $\mathfrak{A}$, $\mathfrak{B}$, etc. serán 1, 2, 4, 8, 9, 13, 15, 16 y los números α, β, etc. serán 8, 9, 11, 15, 16, 3, 5, 6. Los residuos entre ellos son 8, 9, 15 y 16, así $\pm h$, h', etc. se convierten en ± 5, 3, 7, 4. Quienes hayan resuelto a menudo problemas de este tipo encontrarán esto extremadamente útil si calculan para varios números primos p los valores de h, h', etc. correspondientes a valores individuales de k (1, 2, 3, $\ldots p-1$) bajo la doble suposición (a saber, donde $-mn$ es un residuo y donde es un no residuo de p). Observamos que hay siempre $\frac{1}{2}(p-1)$ números h, $-h$, h', etc. cuando los números k y $-mn$ son ambos residuos o ambos no residuos de p; $\frac{1}{2}(p-3)$ números cuando el primero es un residuo y el último un no residuo; $\frac{1}{2}(p+1)$ números cuando el primero es un no residuo y el último un residuo; pero debemos omitir la demostración 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 número primo (impar) que divide o no divide a n. Trataremos todos estos casos juntos y, reteniendo la notación del artículo 324, pondremos $n = n'p^\nu$ tal que n' no es divisible por p. Los números a, b, c, etc. serán los productos del número $p^{\mu-1}$ por todos los números menores que p (excepto 0) o por todos los no residuos de p menores que p, según μ sea par o

impar. Expresamos esto indefinidamente por $up^{\mu-1}$. Sea k el valor de la expresión $\frac{A}{m} \pmod{p^{\mu+\nu}}$, el cual no será divisible por p porque A no lo es. Todos los α, β, γ, etc. serán congruentes a k módulo p, y así p^μ no excluirá nada de Ω si kNp. Si realmente kRp y así también $kRp^{\mu+\nu}$, sea r un valor de la expresión $\sqrt{k} \pmod{p^{\mu+\nu}}$ que no es divisible por p, y sea e el valor de $-\frac{n'}{2mr} \pmod{p}$. Entonces tendremos $\alpha \equiv r^2 + 2erap^\nu \pmod{p^{\mu+\nu}}$ y claramente α es un residuo de $p^{\mu+\nu}$ y los valores de la expresión $\sqrt{\alpha} \pmod{p^{\mu+\nu}}$ se convierten en $\pm(r + eap^\nu)$, así, todos los h, h', h'', etc. son expresados por $r + uep^{\mu+\nu-1}$. Finalmente concluimos que los números h, h', h'', etc. provienen de la adición del número r con los productos del número $p^{\mu+\nu-1}$ por todos los números 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 $-2mrn'Rp$; o por todos los residuos (excepto 0) cuando μ es impar y $-2mrn'Np$.

Pero exactamente como encontramos los números h, h', etc. para cada uno de los números excluyentes, será posible ejecutar la misma exclusión por operaciones mecánicas que el experto puede desarrollar fácilmente si esto le parece útil.

Finalmente debemos observar que cualquier ecuación $ax^2 + 2bxy + cy^2 = M$ en la que $b^2 - ac$ es negativo, digamos $-D$, puede ser fácilmente reducida a la forma que consideramos en el artículo precedente. Porque si hacemos m el máximo común divisor de los números a y b, y ponemos

$$a = ma', \qquad b = mb', \qquad \frac{D}{m} = a'c - mb'^2 = n, \qquad a'x + b'y = x'$$

la ecuación será equivalente a $mx'^2 + ny^2 = a'M$. Esto puede ser resuelto por las reglas que dimos antes. Solamente van a ser retenidas aquellas soluciones en las cuales $x' - b'y$ es divisible por a', i.e. las que dan valores enteros de x.

Otro método de resolver la congruencia $x^2 \equiv A$ para el caso en que A es negativo.

327.

La solución directa de la ecuación $ax^2 + 2bxy + cy^2 = M$ contenida en la sección V asume que conocemos los valores de la expresión $\sqrt{b^2 - ac} \pmod{M}$. Recíprocamente, en el caso donde $b^2 - ac$ es negativo, la solución indirecta anterior da un método muy rápido de encontrar tales valores y es preferible al método del artículo 322 y siguientes, especialmente para un valor muy grande de M. Pero supondremos que M es un número primo o, al menos, si es compuesto, que sus factores son empero

desconocidos. Pues si fuera claro que el número primo p divide a M y si $M = p^\mu M'$ de tal forma que M' no involucre el factor p, sería más conveniente explorar los valores de la expresión $\sqrt{b^2 - ac}$ para los módulos p^μ y M' separadamente (obteniendo el primero de los valores según el módulo p, art. 101) y luego deducir los valores según el módulo M de su combinación (art. 105).

Entonces, es necesario buscar todos los valores de la expresión $\sqrt{-D}$ (mod. M) donde D y M son positivos, y M está contenido en una forma de los divisores de $x^2 + D$ (art. 147 y siguientes). De otro modo sería a priori evidente que no hay números que satisfagan la expresión dada. Los valores buscados serán siempre opuestos dos a dos. Sean ellos $\pm r$, $\pm r'$, $\pm r''$, etc., y $D + r^2 = Mh$, $D + r'^2 = Mh'$, $D + r''^2 = Mh''$, etc.; posteriormente designe las clases a las cuales corresponden las formas (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''), $(M, -r'', h'')$, etc. respectivamente por $\mathfrak{C}$, $-\mathfrak{C}$, $\mathfrak{C}'$, $-\mathfrak{C}'$, $\mathfrak{C}''$, $-\mathfrak{C}''$, etc. y al conjunto de ellas por $\mathfrak{G}$. Hablando en general, estas clases son las que serán consideradas como incógnitas. Sin embargo es claro *primero,* que todas ellas son positivas y propiamente primitivas, *segundo,* que ellas corresponden al mismo género cuyo *carácter* es fácilmente reconocible a partir de la naturaleza del número 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 está contenido en una forma de los divisores de $x^2 + D$, sabemos a priori que de seguro hay un género positivo propiamente primitivo de determinante $-D$ para este carácter aún cuando no haya valores de la expresión $\sqrt{-D}$ (mod. M). Ya que, por lo tanto, este género es conocido, se puede encontrar todas las clases contenidas en él. Desígnense como C, C', C'', etc. y el conjunto de ellas por G. Es claro entonces que las clases individuales $\mathfrak{C}$, $-\mathfrak{C}$, etc. deben ser idénticas con clases en G; también puede suceder que varias clases en $\mathfrak{G}$ sean idénticas unas a otras y con la misma clase en G; y cuando G contiene solamente una clase, de seguro todas las clases en $\mathfrak{G}$ coincidirán con ella. Por lo tanto si de las clases C, C', C'', etc. seleccionamos las (más simples) formas f, f', f'', etc. (una de cada una), de entre éstas aparecerá una forma de cada clase en $\mathfrak{G}$. Ahora, si $ax^2 + 2bxy + cy^2$ es una de las formas contenidas en $\mathfrak{C}$, existirán dos representaciones del número M correspondiendo al valor r por esta forma, y si una es $x = m$, $y = n$, la otra será $x = -m$, $y = -n$. La única excepción 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 número M por las formas individuales f, f', f'', etc. (usando el método indirecto de los artículos precedentes) y deducimos de éstos los valores de la expresión $\sqrt{-D}$ (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 $\mathfrak{G}$ 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.

I. Las representaciones del número M por las formas f, f', etc. que usamos aquí son aquéllas en las cuales los valores de las incógnitas son primos relativos; si aparecen otras en las que estos valores tienen un divisor común μ (esto puede suceder solamente cuando μ^2 divide a M, y sucede con seguridad cuando $-DR\frac{M}{\mu^2}$), ellas serán completamente desatendidas para nuestros presentes propósitos, aún cuando pueden ser útiles en otros contextos.

II. Siendo otras cosas iguales, es obvio que la labor implicada será más fácil cuando el número de clases f, f', f'', etc. sea menor. Por consiguiente, esto es lo más corto posible cuando D es uno de los 65 números tratados en el artículo 303, porque tienen solamente una clase en cada género.

III. 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 $\sqrt{-D}$ (mod. M), y el número de todos los valores diferentes será igual al número de tales representaciones (siempre exceptuando el caso cuando $D = 1$ donde el primer número será la mitad del segundo).

IV. 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 número M por una forma contenida en la clase C, i.e. si $\mathfrak{C} = C$, 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 será 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 $ax^2 + 2bxy + cy^2$ de C y el valor r es producido por la representación $x = m$, $y = n$, el valor $-r$ resultará de la representación $x = -m - \frac{2bn}{a}$, $y = n$.

V. Para el caso donde $D = 1$, existe únicamente una clase, de la cual podemos seleccionar la forma $x^2 + y^2$. Si el valor r resulta de la representación $x = m$, $y = n$, resultará también de $x = -m$, $y = -n$; $x = n$, $y = -m$; $x = -n$, $y = m$ y el opuesto, $-r$, resultará de $x = m$, $y = -n$; $x = -m$, $y = n$; $x = n$, $y = m$; $x = -n$, $y = -m$. Así de estas ocho representaciones que constituyen únicamente una descomposición, una es suficiente en tanto que asociemos el valor opuesto con el que resulta de nuestra investigación.

VI. El valor de la expresión $\sqrt{-D}$ (mod. M) al cual corresponde la representación $M = am^2 + 2bmn + cn^2$ es, por artículo 155, $\mu(mb + nc) - \nu(ma + nb)$ o cualquier número congruente a él según M, donde los números μ y ν satisfacen $\mu m + \nu n = 1$. Designando este valor por v, tendremos

$$mv \equiv \mu m(mb+nc) - \nu(M - mnb - n^2c) \equiv (\mu m + \nu n)(mb+nc) \equiv mb+nc \pmod{M}$$

Así, es claro que si v es un valor de la expresión $\frac{mb+nc}{m}$ (mod. M); similarmente se encuentra que es un valor de la expresión $-\frac{ma+nb}{n}$ (mod. M). Estas fórmulas son muy a menudo preferidas a aquélla de la cual fueron deducidas.

328.

Ejemplos. I. Búsquense todos los valores de la expresión $\sqrt{-1365}$ (mod. $5428681 = M$); el número M es $\equiv 1, 1, 1, 6, 11$ (mod. 4, 3, 5, 7, 13) y así está contenido en una forma de los divisores de $x^2 + 1$, $x^2 + 3$, $x^2 - 5$ y en una forma de los no divisores de $x^2 + 7$, $x^2 - 13$ y por lo tanto en una forma de los divisores de $x^2 + 1365$; el carácter del género en el cual se encontrarán las clases $\mathfrak{G}$, es 1, 4; $R3$; $R5$; $N7$; $N13$. Existe solamente una clase contenida en este género y de ésta seleccionaremos la forma $6x^2+6xy+229y^2$. Para encontrar todas las representaciones del número M por esta forma, ponemos $2x + y = x'$ y tenemos $3x'^2 + 455y^2 = 2M$. Esta ecuación admite cuatro soluciones en las que y es positivo, a saber $y = 127$,

$x' = \pm 1083$, $y = 119$, $x' = \pm 1213$. De éstas obtenemos cuatro soluciones de la ecuación $6x^2 + 6xy + 229y^2 = M$ 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 $\frac{30517}{478}$ o $\frac{-3249}{127}$ (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.

II. Si queremos los valores de la expresión $\sqrt{-286}$ (mod. $4272943 = M$), el carácter del género en el que están contenidas las clases $\mathfrak{G}$, será 1 y 7, 8; $R11$; $R13$. Este será por lo tanto el género principal en el cual están contenidas tres clases, representadas por las formas $(1, 0, 286)$, $(14, 6, 23)$ y $(14, -6, 23)$. Se puede omitir la tercera de éstas, ya que es opuesta a la segunda. Por la forma $x^2 + 286y^2$ encontramos dos representaciones del número M en las que y es positivo, a saber, $y = 103$, $x = \pm 1113$. 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 ésos son los únicos valores.

III. Dada la expresión $\sqrt{-70}$ (mod. 997331), las clases $\mathfrak{G}$ deben estar contenidas en el género cuyo carácter es 3 y 5, 8; $R5$; $N7$. Hay únicamente una clase y su forma representante es $(5, 0, 14)$. Después de un cálculo se encuentra que el número 997331 no es representable por la forma $(5, 0, 14)$ y así -70 será necesariamente un no residuo cuadrático de ese número.

Dos métodos para distinguir números compuestos de números primos y para determinar sus factores.

329.

El problema de distinguir números primos de números compuestos y de resolver estos últimos en sus factores primos es conocido como uno de los más importantes y útiles en aritmética. Ha ocupado la industria y la sabiduría de geómetras antiguos y modernos a tal grado que sería superfluo discutir el problema detenidamente. No obstante debemos admitir que todos los métodos que han sido propuestos hasta ahora son o restringidos a casos muy especiales o tan laboriosos y prolijos que aún para números que no exceden los límites de tablas construidas por hombres estimables, i.e., para números que no requieren métodos ingeniosos, ponen a prueba la paciencia hasta de los calculistas experimentados. Y estos métodos a duras

penas pueden ser usados para números grandes. Aún cuando las tablas, que están disponibles para quien quiera y las cuales esperamos continuarán 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 números grandes a sus factores de modo que esto lo compensará por el tiempo consumido. Luego, la dignidad de la ciencia misma parece requerir que todos los medios posibles para la solución de un problema tan elegante y tan célebre sean explorados. Por esta razón, no dudamos que los dos métodos siguientes, cuya eficacia y brevedad podemos confirmar a partir de una larga experiencia, resultarán gratificantes a los aficionados a la aritmética. Está en la naturaleza del problema que *cualquier* método se hará más prolijo a medida que los números se hacen mayores. No obstante, en los siguientes métodos, las dificultades crecen algo lentamente, y números con siete, ocho o aún más dígitos han sido manipulados con éxito y rapidez más allá de la esperada, especialmente por el segundo método. Las técnicas que fueron previamente conocidas requerirían un trabajo intolerable aún para el calculista más infatigable.

Antes de considerar los siguientes métodos, es siempre muy útil tratar de dividir el número dado por algunos de los primos más pequeños, digamos por 2, 3, 5, 7, etc. hasta 19 o un poco más allá, a fin de eludir el uso de métodos sutiles y artificiales cuando la sola división puede ser más sencilla *); y también, porque cuando la división no es exitosa, la aplicación del segundo método utiliza con gran beneficio los *residuos* derivados de estas divisiones. Así, e.g., si el número 314159265 se va a resolver en sus factores, la división por 3 es exitosa dos veces, y después, las divisiones por 5 y por 7. Así tenemos $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$ y es suficiente examinar por medios más sutiles el número 997331, el cual no es divisible por 11,13,17 ni 19. Similarmente, dado el número 43429448, podemos remover el factor 8 y aplicar los métodos más 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 cuadrático de otro número M, es también un residuo de cualquier divisor de M.* Cualquiera sabe que si M no es divisible por ningún número primo abajo de $\sqrt{M}$, M es de seguro primo; pero si todos

*) 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.

los números primos abajo de este límite que dividen a M son p, q, etc., el número M está compuesto por éstos *solamente* (o por sus potencias), o existe únicamente *un* factor primo mayor que $\sqrt{M}$. 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 $\sqrt{M}$ (excluyendo a aquéllos que ya sabemos que no dividen al número) por Ω, evidentemente será suficiente encontrar todos los divisores de M contenidos en Ω. Ahora, si de alguna manera se constata que un número r (no cuadrado) es un residuo cuadrático de M, de seguro ningún número primo del cual r es un no residuo puede ser un divisor de M; por consiguiente se pueden remover de Ω todos los números primos de este tipo (ellos usualmente conformarán alrededor de la mitad de los números de Ω). Y si llega a ser claro que otro número r' no cuadrado es un residuo de M, podemos excluir de los restantes números primos en Ω aquellos para los cuales r' es un no residuo. De nuevo reducimos estos números 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 números 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*), 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 será ciertamente un número primo, o quedarán tan pocos (obviamente todos los divisores primos de M aparecerán entre ellos, si existe alguno) que la división por ellos puede ser probada sin demasiada dificultad. Para un número que no excede un millón aproximadamente, usualmente seis o siete exclusiones serán suficientes; para un número 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 número suficiente de ellos, *entonces* efectuar la exclusión de la manera más conveniente. Pero invertiremos el orden de las cuestiones porque lo segundo nos mostrará cuales residuos son los más apropiados para este propósito.

331.

En la sección IV hemos mostrado detenidamente como distinguir números

*) Si el producto de cualquier cantidad de números r, r', r'', etc. es un cuadrado, cada uno de ellos, e.g. r, será un residuo de cualquier número primo (que no divida a ninguno de ellos) que sea un residuo de los otros, r', r'', etc. Así, para que los residuos sean independientes, ningún producto de pares o triples, etc. de ellos puede ser cuadrado.

primos para los cuales un r dado es un residuo (podemos suponer que no es divisible por un cuadrado) de aquéllos para los cuales es un no residuo; es decir, como distinguir los divisores de la expresión $x^2 - r$ de los no divisores. Todos los divisores están contenidos bajo fórmulas como $rz + a$, $rz + b$, etc. o como $4rz + a$ y $4rz + b$, etc. y los otros bajo fórmulas semejantes. Siempre que r es un número muy pequeño, con la ayuda de estas fórmulas podemos llevar a cabo las exclusiones satisfactoriamente; e.g. cuando $r = -1$ todos los números de la forma $4z + 3$ serán excluidos; cuando $r = 2$ se excluyen todos los números de las formas $8z + 3$ y $8z + 5$, etc. Pero puesto que no siempre es posible encontrar residuos como éstos para un número M dado, y la aplicación de las fórmulas no es muy conveniente cuando el valor de r es grande, se ganará mucho y el trabajo de exclusión se reducirá sobremanera si tenemos una *tabla* para una cantidad suficientemente grande de números (r) tanto positivos como negativos que no sean divisibles por cuadrados. La tabla deberá distinguir números primos que tengan a cada uno (r) como residuo de aquéllos 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 propósitos presentes, los números primos (módulos) en el margen deben ser continuados mucho más lejos, a 1000 o 10000. Sería aún más conveniente si los números compuestos y negativos también fueran listados hasta el tope, aunque esto no es absolutamente necesario, como es claro de la sección IV. La máxima utilidad resultaría si las columnas verticales individuales fueran removibles y pudieran ser rearmadas sobre placas o varillas (como las de Napier). Entonces aquéllos que son necesarios en cada caso, i.e. los que corresponden a r, r', r'', etc., los residuos de los números dados, pueden ser examinados separadamente. Si éstos son colocados *correctamente* junto a la primera columna de la tabla (que contiene al módulo), i.e. de manera que la posición en cada una de las varillas que corresponden al mismo número en la primera columna es puesta en la línea horizontal correspondiente, aquellos números primos que permanecen después de las exclusiones de Ω correspondientes a los residuos r, r', r'', etc. pueden ser inmediatamente reconocidos por inspección. Ellos son los números 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 ilustrará esto suficientemente bien. Si de algún modo sabemos que los números -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 número 997, i.e. hasta el mayor número primo menor que $\sqrt{997331}$) y las columnas que tengan como tope los números -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 después de todas las exclusiones con los residuos −6, 13, etc. únicamente permanece en Ω el número 127. El esquema total extendido hasta el número 997 mostraría que no hay otro número en Ω. Cuando probamos esto, encontramos que 127 efectivamente divide a 997331. De esta manera encontramos que este número puede ser resuelto en los factores primos $127 \cdot 7853$*).

De este ejemplo es suficientemente claro que aquellos residuos especialmente útiles 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 allá de los números a la cabeza de las columnas, y el uso indirecto sólo incluye aquellos números que pueden ser resueltos en factores contenidos en la tabla.

*) El autor ha construido para su propio uso una gran parte de la tabla descrita aquí y la habría publicado gustosamente si el pequeño número de aquéllos para quienes sería útil bastase para justificar tal empresa. Si hay algún devoto de la aritmética que comprende los principios involucrados y desea construir una tabla como ésta por sí mismo, el autor encontrará gran placer en comunicarle mediante carta todos los procedimientos y artificios que usó.

332.

Daremos tres métodos para encontrar residuos de un número M dado, pero antes de explicar esto queremos hacer dos observaciones que nos ayudarán a determinar residuos más simples cuando los que tenemos no son bastante idóneos. *Primero,* si el número ak^2 que es divisible por el cuadrado k^2 (que es relativamente primo a M) es un residuo de M, a será también un residuo. Por esta razón, residuos que son divisibles por cuadrados grandes son precisamente tan útiles como los residuos pequeños, y suponemos que todos los factores cuadrados se han eliminado de todos los residuos suministrados por los siguientes métodos. *Segundo,* si dos o más números son residuos, su producto también será un residuo. Combinando esta observación 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 razón 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 será mejor entendida mediante ejemplos y el uso frecuente que mediante reglas.

I. El método más simple y el más conveniente, para aquéllos que han adquirido alguna destreza a través del ejercicio frecuente, consiste en descomponer M o más 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 será un residuo de M; pues $-ab \equiv a^2 \equiv b^2 \pmod{M}$ y así $-ab \mathrm{R} M$. Los números a y b deben ser tomados de modo que su producto sea divisible por un cuadrado grande y su cociente sea pequeño 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 número pequeño o al menos por un número que pueda ser resuelto en factores apropiados. Así, e.g., $997331 = 999^2 - 2\cdot 5\cdot 67 = 994^2 + 5\cdot 11\cdot 13^2 = 2\cdot 706^2 + 3\cdot 17\cdot 3^2 = 3\cdot 575^2 + 11\cdot 31\cdot 4^2 = 3\cdot 577^2 - 7\cdot 13\cdot 4^2 = 3\cdot 578^2 - 7\cdot 19\cdot 37 = 11\cdot 299^2 + 2\cdot 3\cdot 5\cdot 29\cdot 4^2 = 11\cdot 301^2 + 5\cdot 12^2$ etc. Así tenemos los siguientes residuos: $2\cdot 5\cdot 67$, $-5\cdot 11$, $-2\cdot 3\cdot 17$, $-3\cdot 11\cdot 31$, $3\cdot 7\cdot 13$, $3\cdot 7\cdot 19\cdot 37$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$. La última descomposición produce el residuo $-5\cdot 11$ el cual ya tenemos. Para los residuos $-3\cdot 11\cdot 31$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$ podemos sustituir $3\cdot 5\cdot 31$, $2\cdot 3\cdot 29$ que resulta de su combinación con $-5\cdot 11$.

II. El segundo y tercer método 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 $\pm kM$ pertenecen al mismo género, los números AA', AC' y $A'C$ son residuos de kM; esto no es difícil de ver ya que cualquier número característico, digamos m, de una forma es también un número característico de la otra, y así 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 más general kM, y $(a',\ b',\ a'')$, $(a'',\ b'',\ a''')$, etc. son formas en su período, éstas serán equivalentes a ella y ciertamente contenidas en el mismo género. Los números aa', aa'', aa''', etc. serán todos residuos de M. Se puede computar un gran número de formas en tal período con la ayuda del algoritmo del artículo 187. Ordinariamente los residuos más simples resultan de poner $a = 1$ y se omiten aquellos que tengan factores que son demasiado grandes. Aquí están los inicios de los períodos de las formas $(1,\ 998,\ -1327)$ y $(1,\ 1412,\ -918)$ cuyos determinantes son 997331 y 1994662:

$(\ \ 1, 998, -1327)$	$(\ \ 1, 1412, -918)$
$(-1327, 329, \ \ 670)$	$(\ -918, 1342, \ \ 211)$
$(\ \ 670, 341, -1315)$	$(\ \ 211, 1401, -151)$
$(-1315, 974, \ \ 37)$	$(\ -151, 1317, 1723)$
$(\ \ 37, 987, -626)$	$(\ 1723, 406, -1062)$
$(\ -626, 891, \ \ 325)$	$(-1062, 656, 1473)$
$(\ \ 325, 734, -1411)$	$(\ 1473, 817, -901)$
$(-1411, 677, \ \ 382)$	$(\ -901, 985, 1137)$
$(\ \ 382, 851, -715)$	etc.

Por consiguiente todos los números -1327, 670, etc. son residuos del número 997331; olvidando aquéllos que tengan factores demasiado grandes, tenemos éstos: $2 \cdot 5 \cdot 67$, 37, 13, $-17 \cdot 83$, $-5 \cdot 11 \cdot 13$, $-2 \cdot 3 \cdot 17$, $-2 \cdot 59$, $-17 \cdot 53$; hemos encontrado arriba el residuo $2 \cdot 5 \cdot 67$ así como $-5 \cdot 11$ que resulta de una combinación del tercero y el quinto.

III. Sea C cualquier clase, diferente de la clase principal, de formas de un determinante negativo $-M$ o más generalmente $-kM$ y sea su período $2C$, $3C$, etc. (art. 307). Las clases $2C$, $4C$, etc. pertenecerán al género principal; $3C$, $5C$, etc. al mismo género que C. Si por consiguiente (a, b, c) es la (más simple) forma en C y $(a',\ b',\ c')$ una forma en alguna clase del período, digamos nC, o a' o aa' será un residuo de M según que n sea par o impar (en el primer caso c' será también un residuo, en el último caso ac', ca' y cc' lo serán). El cálculo del período, i.e. de las formas más simples en sus clases, es sorprendentemente fácil cuando a es muy pequeño, especialmente cuando es $= 3$, lo que es siempre permisible cuando

$kM \equiv 2 \pmod 3$. He aquí el inicio del período de la clase que contiene a la forma (3, 1, 332444):

$C\,(\ \ 3,\ \ 1, 332444)$	$6C\,(\ 729, -209, 1428)$
$2C\,(\ \ 9, -2, 110815)$	$7C\,(\ 476,\ \ 209, 2187)$
$3C\,(\ 27,\ \ 7,\ \ 36940)$	$8C\,(1027,\ \ 342, 1085)$
$4C\,(\ 81,\ 34,\ \ 12327)$	$9C\,(\ 932, -437, 1275)$
$5C\,(243,\ 34,\ \ \ 4109)$	$10C\,(\ 425,\ \ \ 12, 2347)$

Después de eliminar aquéllos que no son útiles, tenemos los residuos $3 \cdot 476$, 1027, 1085, 425 o (removiendo los factores cuadrados) $3 \cdot 7 \cdot 17$, $13 \cdot 79$, $5 \cdot 7 \cdot 31$, 17. Si combinamos juiciosamente éstos con los ocho residuos encontrados en II se encuentran los doce siguientes, $-2 \cdot 3$, 13, $-2 \cdot 7$, 17, 37, -53, $-5 \cdot 11$, 79, -83, $-2 \cdot 59$, $-2 \cdot 5 \cdot 31$ y $2 \cdot 5 \cdot 67$. 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 aquí.

333.

El segundo metodo para resolver un número dado M en factores depende de una consideración de los valores de la expresión $\sqrt{-D} \pmod M$, junto con las siguientes observaciones.

I. Cuando M es un número primo o una potencia de un primo (impar y que no divide a D), $-D$ será un residuo o un no residuo de M de acuerdo con que M esté contenido en una forma de los divisores o de los no divisores de $x^2 + D$. En el primer caso la expresión $\sqrt{-D} \pmod M$ tendrá únicamente dos valores diferentes, que serán opuestos.

II. Cuando M es compuesto, es decir, $= pp'p''$, etc., donde los números p, p', p'', etc. son primos (distintos, impares y que no dividen a D) o potencias de tales números: $-D$ será un residuo de M solamente cuando es un residuo de cada uno de los p, p', p'', etc., i.e. cuando todos estos números están contenidos en formas de los divisores de $x^2 + D$. Designando los valores de la expresión $\sqrt{-D}$ según los módulos p, p', p'', etc. respectivamente por $\pm r$, $\pm r'$, $\pm r''$, etc. aparecen todos los valores de la misma expresión según el módulo M al determinar los números que son $\equiv r$ o $\equiv -r$ según p, aquéllos que son $\equiv r'$ o $\equiv -r'$ según p', etc. Su número será $= 2^\mu$, donde μ es el número de factores p, p', p'', etc. Ahora, si estos valores son R, $-R$, R', $-R'$, R'', etc., se ve inmediatamente que $R \equiv R$ según todos los números p, p', p'', etc.,

pero que según cualquiera de ellos no se tiene $R \equiv -R$. 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 idénticos ni opuestos, e.g. R y R', deben ser congruentes según uno o varios de los números p, p', p'', etc. pero no según todos ellos y según los otros tendremos $R \equiv -R'$. Así el producto de los primeros será el máximo común divisor de los números M y $R - R'$, y el producto de los últimos será el máximo 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 $\sqrt{-D}$ (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 números. *De esta forma, por lo tanto, podrán determinarse los números p, p', p'', etc. de los valores de esa expresión.*

Ahora, ya que el método del artículo 327 reduce estos valores a los valores de expresiones de la forma $\frac{m}{n}$ (mod. M) con el denominador n primo relativo a M, no es necesario, para nuestros propósitos presentes, computarlos. El máximo común divisor del número M y la diferencia entre R y R', que corresponden a $\frac{m}{n}$ y $\frac{m'}{n'}$, será obviamente también el máximo común divisor de los números M y $nn'(R - R')$, o de M y $mn' - m'n$, ya que el último es congruente a $nn'(R - R')$ según el módulo M.

334.

Podemos aplicar las observaciones precedentes a nuestro problema de dos maneras; la primera no sólo 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 cálculos más rápidos, pero, a menos que se repita una y otra vez, no produce los factores de los números compuestos, sin embargo los distingue de los números primos.

I. Se busca primero un número negativo $-D$ que sea un residuo cuadrático de M; para este fin se pueden usar los métodos dados en I y II del artículo 332. En sí, la selección del residuo es arbitraria, ni hay aquí como en el método precedente ninguna necesidad de que D sea un número pequeño. Pero el cálculo será más corto a medida que el número de clases de formas binarias contenidas en cada género propiamente primitivo del determinante $-D$ sea más pequeño. Por consiguiente será conveniente tomar residuos que estén contenidos entre los 65 enumerados en el artículo 303 si alguno de éstos se halla allí. Así, para $M = 997331$ el residuo -102 será el más idóneo de todos los residuos negativos dados arriba. Aparecen todos los valores diferentes de la expresión $\sqrt{-D}$ (mod. M). Si hay solamente dos (opuestos),

M será de seguro un número primo o una potencia de un primo; si hay varios, digamos 2^μ, M estará compuesto de μ números primos o potencias de primos y estos factores pueden ser encontrados por el método 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 $\sqrt{-D}$ indicará todos los primos cuyas potencias dividen a M. Puesto que si M es divisible por el cuadrado de un número primo π, el cálculo de seguro producirá una o más representaciones del número $M = am^2 + 2bmn + cn^2$, en las que el máximo común divisor de los números m y n es π (porque en este caso $-D$ es también un residuo de $\frac{M}{\pi^2}$). Pero cuando no existen representaciones en las cuales m y n tengan un divisor común, ésta es una indicación 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 método dado antes se encuentra que existen cuatro valores de la expresión $\sqrt{-408}$ (mod. 997331) que coinciden con los valores de las expresiones $\pm\frac{1664}{113}$ y $\pm\frac{2824}{3}$; los máximos comunes divisores de 997331 con $3 \cdot 1664 - 113 \cdot 2824$ y $3 \cdot 1664 + 113 \cdot 2824$ o con 314120 y 324104 son 7853 y 127, así $997331 = 127 \cdot 7853$ como antes.

II. Tómese un número negativo $-D$ tal que M está contenido en una forma de los divisores de x^2+D; en sí es arbitrario qué número de este tipo se selecciona, pero es ventajoso tener el número de clases en el género del determinante $-D$ tan pequeño como sea posible. No existe dificultad en encontrar un tal número; puesto que entre cualquier cantidad de números probados aproximadamente existen tantos para los que M está contenido en una forma de los divisores como existen para los cuales M está contenido en una forma de los no divisores. Por consiguiente será conveniente comenzar con los 65 números del artículo 303 (comenzando con los más grandes) y si sucede que ninguno de éstos es idóneo (en general esto sucederá solamente una vez en 16384 casos), podemos pasar a otros en los cuales solamente hay dos clases contenidas en cada género. Entonces se investigarán los valores de la expresión $\sqrt{-D}$ (mod. M) y si alguno se encuentra, los factores de M pueden ser deducidos de él, del mismo modo que antes; pero si no se obtienen valores, es decir, si $-D$ es un no residuo de M, ciertamente M no será número primo ni potencia de un número primo. Si en este caso se desean los factores mismos, habremos de repetir la misma operación, usando otro valor para D o ensayando otro método.

Así, e.g., se encuentra que 997331 está contenido en una forma de los no divisores de $x^2 + 1848$, $x^2 + 1365$, $x^2 + 1320$ pero está contenido en una forma de

los divisores de $x^2 + 840$; para los valores de la expresión $\sqrt{-840}$ (mod. 997331) se encuentran las expresiones $\pm\frac{1272}{163}$ y $\pm\frac{3288}{125}$ y de éstos deducimos los mismos factores que antes. Para más ejemplos consulte los del artículo 328, que muestran primero que $5428681 = 307 \cdot 17863$; segundo que 4272943 es un número primo; tercero, que 997331 está ciertamente compuesto de más de un número primo.

Los límites del presente trabajo nos permite insertar aquí únicamente los principios básicos de cada método de hallazgo de factores; guardaremos para otra ocasión una discusión más detallada, junto con tablas auxiliares y otras ayudas.