290.

Las formas de determinante -1 y -2 están sujetas a ciertas excepciones, así que diremos un poco sobre ellas como caso particular. Empezamos con la observación general de que si φ y φ' son dos formas binarias equivalentes cualesquiera, (Θ) una transformación dada de la primera en la segunda, entonces combinando cualquiera de las representaciones de φ por la forma ternaria f con la sustitución (Θ), se obtiene una representación de la forma φ' por f. Además a partir de las representaciones propias de φ obtenemos las representaciones propias de la forma φ', a partir de representaciones distintas de φ obtenemos representaciones distintas de φ' y si tomamos todas las representaciones de la primera obtendremos todas las representaciones de la segunda. Todo esto se puede comprobar mediante cálculos muy sencillos. Por lo tanto una de las formas φ y φ' es representable por f de tantas maneras distintas como lo es la otra.

I. Primero sea $\varphi = t^2 + u^2$ y φ' una forma binaria positiva cualquiera de determinante -1, a la cual φ es equivalente. Sea $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ la sustitución que transforma φ en φ'. La forma φ se representa por la forma ternaria $f = x^2 + y^2 + z^2$, poniendo $x = t$, $y = u$, $z = 0$; permutando x, y, z resultan *seis* representaciones, y a partir de cada una de éstas, cuatro más cambiando los signos de t y u. Así pues habrá en total 24 representaciones que corresponden a sólo una descomposición en tres cuadrados. Es fácil ver que no habrá ninguna otra representación salvo éstas. Y se concluye que la forma φ' se puede descomponer en tres cuadrados de sólo una manera, a saber, $(\alpha t' + \beta u')^2$, $(\gamma t' + \delta u')^2$ y 0. Esta descomposición será equivalente a las 24 representaciones.

II. Sea $\varphi = t^2 + 2u^2$, φ' cualquier otra forma binaria positiva de determinante -2, en la cual se transforma φ mediante la sustitución $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. Entonces de manera similar que en el caso anterior concluimos que φ y también φ' se pueden descomponer en tres cuadrados de manera única, a saber, φ en $t^2 + u^2 + u^2$ y φ' en $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$; es obvio que esta descomposición es equivalente a las 24 representaciones.

De todo esto se sigue que las formas binarias de determinante -1 y -2 en cuanto al número de representaciones por la forma ternaria $x^2 + y^2 + z^2$ son completamente iguales a las otras formas binarias; puesto que en ambos casos tenemos $\mu = 0$, la fórmula dada en IV del artículo anterior dará las 24 representaciones. La razón para esto es que las dos excepciones a las cuales están sujetas estas formas se compensan mutuamente.

Por razones de brevedad omitiremos la aplicación, a la forma $x^2 + y^2 + z^2$, de la teoría general respecto a representaciones impropias dada en el artículo 284.

291.

El problema de encontrar todas las representaciones propias de un *número* positivo M por la forma $x^2 + y^2 + z^2$ se reduce primeramente en el artículo 281 a la investigación de las representaciones propias del número $-M$ por la forma $-x^2 - y^2 - z^2 = f$; por los métodos del artículo 280 éstas se pueden encontrar de la siguiente manera.

I. Encontramos todas las clases de formas binarias de determinante $-M$ cuyas formas se pueden representar propiamente por $X^2 + Y^2 + Z^2 = F$ (la cual tiene a f como adjunta). Cuando $M \equiv 0$, 4 ó 7 (mod. 8), por el artículo 288 no hay tales clases y entonces M no se puede descomponer en tres cuadrados que no tienen un divisor común *). Pero cuando $M \equiv 1$, 2, 5 ó 6, habrá un género positivo propiamente primitivo, y cuando $M \equiv 3$ uno impropiamente primitivo que incluye todas aquellas clases. Designemos el número de estas clases por k.

II. Ahora escoja arbitrariamente una forma de cada una de estas k clases y llámelas φ, φ', φ'', etc.; investigue todas las representaciones propias de cada una de éstas por F. El número de ellas será $3 \cdot 2^{\mu+3}k = K$, donde μ es el número de factores primos (impares) de M; finalmente a partir de cada una de estas representaciones, tales como

$$X = mt + nu, \qquad Y = m't + n'u, \qquad Z = m''t + n''u$$

derivamos la siguiente representación de M por $x^2 + y^2 + z^2$:

$$x = m'n'' - m''n', \qquad y = m''n - mn'', \qquad z = mn' - m'n$$

Todas las representaciones de M están contenidas en el conjunto, que designaremos por Ω, de estas K representaciones.

III. Sólo queda determinar si hay algunas representaciones en Ω que sean *idénticas*; y puesto que del artículo 280.III está claro que aquellas representaciones

*) Esta imposibilidad es también clara por el hecho de que la suma de tres cuadrados impares debe ser $\equiv 3$ (mod. 8); la suma de dos impares con uno par es $\equiv 2$ ó $\equiv 6$; la suma de un impar y dos pares es $\equiv 1$ ó $\equiv 5$; y finalmente la suma de tres pares es $\equiv 0$ ó $\equiv 4$; pero en el último caso la representación es claramente impropia.

en Ω que se obtienen de diferentes formas, e.g., de φ y φ' deben ser distintas, la única pregunta que queda es si diferentes representaciones de la misma forma e.g., φ por F pueden dar lugar a representaciones idénticas del número M por $x^2+y^2+z^2$. Ahora es inmediatamente evidente que si entre las representaciones de φ encontramos

$$X = mt + nu, \qquad Y = m't + n'u, \qquad Z = m''t + n''u \tag{r}$$

también encontraremos entre las mismas representaciones

$$X = -mt - nu, \qquad Y = -m't - n'u, \qquad Z = -m''t - n''u \tag{r'}$$

y a partir de cada una podemos obtener la misma representación de M que llamaremos (R); examinemos por lo tanto si la representación (R) puede obtenerse todavía de otras representaciones de φ. A partir del artículo 280.III, si hacemos que $\chi = \varphi$ y si exhibimos todas las transformaciones de la forma propia φ en sí misma por

$$t = \alpha t + \beta u, \qquad u = \gamma t + \delta u$$

podemos deducir que todas aquellas representaciones de la forma φ a partir de la cual se obtiene R serán expresadas por

$$\begin{aligned} x &= (\alpha m + \gamma n)t + (\beta m + \delta n)u \\ y &= (\alpha m' + \gamma n')t + (\beta m' + \delta n')u \\ z &= (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u \end{aligned}$$

Pero de la teoría de la transformación de formas binarias con determinante negativo como se explicó en el artículo 179, se sigue que en todos los casos, excepto cuando $M = 1$ y $M = 3$, hay sólo dos transformaciones propias de la forma φ es sí misma, a saber, α, β, γ, $\delta = 1, 0, 0, 1$ y $= -1, 0, 0, -1$ respectivamente (pues como φ es una forma primitiva, el número que designamos en el artículo 179 por m será ó 1 ó 2 y así, excepto en los casos que se excluyeron, 1) ciertamente será aplicable). Por lo tanto (R) puede aparecer sólo a partir de r, r' y cada una de las representaciones propias del número M se encontrará dos veces, y no más en Ω; y el número de representaciones propias de M será $\frac{1}{2}K = 3 \cdot 2^{\mu+2}k$.

En cuanto a los casos que se excluyeron, el número de transformaciones propias de φ en sí misma, con base en el artículo 179 serán 4 para $M = 1$ y 6 para $M = 3$; y es fácil comprobar que el número de representaciones propias de los números 1 y

3 es $\frac{1}{4}K$ y $\frac{1}{6}K$ respectivamente; eso es cada número se puede descomponer en tres cuadrados de una manera única, 1 en $1+0+0$, 3 en $1+1+1$. La descomposición de 1 proporciona seis, la descomposición de 3, ocho representaciones diferentes, ahora para $M = 1$ tenemos $K = 24$ (aquí $\mu = 0$, $k = 1$) y para $M = 3$ tenemos $K = 48$ (aquí $\mu = 1$, $k = 1$).

Sea h el número de clases en el género principal. Por artículo 252 será igual al número de clases en cualquier otro género propiamente primitivo. Observamos que $k = h$ para $M \equiv 1, 2, 5$ ó $6 \pmod 8$, pero $k = \frac{1}{3}h$ para $M \equiv 3 \pmod 8$, excepto en el caso de $M = 3$ (donde $k = h = 1$). Así, el número de representaciones, *en general*, de números de la forma $8n + 3$ es $= 2^{\mu+2}h$, puesto que para el número 3 las dos excepciones se compensan entre sí.

292.

Hemos distinguido la descomposición de números (y también de formas binarias) en tres cuadrados por representaciones de la forma $x^2+y^2+z^2$, de tal manera que en el primero nos preocupamos únicamente por la magnitud de los cuadrados y en el segundo también consideramos el orden de las raíces y sus signos. Así, consideramos que las representaciones $x = a$, $y = b$, $z = c$ y $x = a'$, $y = b'$, $z = c'$ son distintas a menos que $a = a'$, $b = b'$, $c = c'$ simultáneamente; y tomamos las descomposiciones en $a^2 + b^2 + c^2$ y en $a'^2 + b'^2 + c'^2$ como la misma si, sin considerar el orden, los cuadrados en una son iguales a los cuadrados en la otra. De esto es claro:

I. Que la descomposición del número M en $a^2 + b^2 + c^2$ es equivalente a 48 representaciones si ninguno de los cuadrados es $= 0$ y si todos son distintos entre sí; pero sólo a 24 si alguno es $= 0$ y los otros son distintos entre sí, *o* ninguno es $= 0$ y dos son iguales. Sin embargo, si en la descomposición de un número dado en tres cuadrados dos de los cuadrados $= 0$, *ó* uno $= 0$ y los restantes iguales entre sí, *o* todos son iguales entre sí, la descomposición será equivalente a 6 *o* 12 *o* 18 representaciones; pero esto no puede suceder a menos que tengamos el caso especial de $M = 1$ o 2 o 3, respectivamente, por lo menos si se quiere que las representaciones sean propias. Excluyendo estos tres casos, supongamos que el número de descomposiciones de un número M en tres cuadrados (que no tienen un divisor común) es E, y que entre ellas tenemos e descomposiciones en las cuales un cuadrado es 0, y e' en las cuales dos cuadrados son iguales; el primero se puede considerar como descomposiciones en dos cuadrados y el segundo como descomposiciones en un cuadrado y dos veces un cuadrado. Entonces el número de representaciones propias del número M por

$x^2 + y^2 + z^2$ será

$$= 24(e + e') + 48(E - e - e') = 48E - 24(e + e')$$

Pero de la teoría de formas binarias es fácil ver que e será $= 0$ ó $= 2^{\mu-1}$, según -1 sea un no residuo o sea un residuo cuadrático de M, y que e' será $2^{\mu-1}$ ó $= 0$ según -2 sea o no un residuo de M. Aquí μ es el número de factores primos (impar) de M (ver art. 182; omitimos aquí una exposición más completa). De todo esto tenemos

$$E = 2^{\mu-2}k, \quad \text{si ambos } -1 \text{ y } -2 \text{ son no residuos de } M;$$
$$E = 2^{\mu-2}(k+2), \quad \text{si ambos números son residuos;}$$
$$E = 2^{\mu-2}(k+1), \quad \text{si uno es un residuo y el otro un no residuo.}$$

En los casos excluidos donde $M = 1$ y $M = 2$ esta fórmula haría que $E = \frac{3}{4}$, mientras que debió haber sido $E = 1$. Sin embargo, para $M = 3$ obtenemos el valor correcto, $E = 1$, porque las excepciones se compensan mutuamente.

Por lo tanto si M es un número primo, resulta $\mu = 1$ y así $E = \frac{1}{2}(k+2)$ cuando $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k+1)$ cuando $M \equiv 3$ ó $M \equiv 5$. Estos teoremas especiales fueron descubiertos por el ilustre Legendre por métodos de inducción y fueron publicados por él en aquel comentario espléndido que hemos citado a menudo, *Hist. de l'Ac. de Paris* 1785, *p.* 530 y siguientes. Si lo presentó de manera un poco distinta es porque no distinguió entre equivalencias propias e impropias y así mezcló clases opuestas.

II. Para encontrar todas las descomposiciones de un número M en tres cuadrados (sin un divisor común) no es necesario obtener todas las representaciones propias de todas las formas φ, φ' y φ''. En efecto, es fácil comprobar que todas las (48) representaciones de la forma φ que corresponden al mismo valor de la expresión $\sqrt{-(p,-q,r)}$ (donde $\varphi = (p,q,r)$) darán la misma descomposición del número M, así es suficiente si tenemos una de ellas, o lo que es lo mismo, si conocemos todas las descomposiciones *) diferentes de la forma φ en tres cuadrados. Lo mismo es cierto para las restantes φ', φ'', etc. Ahora si φ pertenece a una clase no ambigua, es permitido ignorar la forma que fue escogida de la clase opuesta; eso es, es suficiente considerar sólo una de las dos clases opuestas. Pues, ya que es completamente arbitrario cuál forma seleccionamos de una clase, supongamos que se escoge la forma

*) Siempre debemos entender la palabra "propia" si queremos transferir esta expresión de representaciones a descomposiciones.

φ' de la clase opuesta a la que contiene φ, la cual es opuesta a la forma φ. Entonces no es difícil mostrar que si se representan las descomposiciones propias de la forma φ por la expresión general

$$(gt + hu)^2 + (g't + h'u)^2 + (g''t + h''u)^2$$

todas las descomposiciones de la forma φ' serán expresadas por

$$(gt - hu)^2 + (g't - h'u)^2 + (g''t - h''u)^2$$

y la misma descomposición del número M se obtendrá de ambas. Finalmente, para el caso en el cual φ es de una clase ambigua, pero no de la clase principal ni equivalente a la forma $(2, 0, \frac{1}{2}M)$ o $(2, 1, \frac{1}{2}(M+1))$ (según M sea par o impar), es permitido omitir la mitad de los valores de la expresión $\sqrt{-(p, -q, r)}$; pero para brevedad no daremos los detalles de esta simplificación. También podemos utilizar estas simplificaciones cuando queremos todas las representaciones propias de M por $x^2 + y^2 + z^2$, puesto que esto se puede obtener muy fácilmente a partir de las descomposiciones.

Como ejemplo investigaremos todas las descomposiciones del número 770 en tres cuadrados. Aquí $\mu = 3$, $e = e' = 0$ y así $E = 2k$. Puesto que es fácil utilizar las normas del artículo 231 para clasificar las formas binarias positivas de determinante -770, omitiremos esta operación para brevedad. Encontramos que el número de clases positivas es $= 32$. Todas ellas son propiamente primitivas y están distribuidas entre ocho géneros de modo que $k = 4$ y $E = 8$. El género cuyo número característico es -1 claramente tiene los caracteres particulares $R5$; $N7$; $N11$ con respecto a los números 5, 7 y 11, y por el artículo 263 concluimos que su carácter respecto al número 8 debe ser 1 y 3, 8. Ahora, en el género con carácter 1 y 3, 8; $R5$; $N7$; $N11$ encontramos cuatro clases. De ellas escogemos las siguientes como representantes $(6, 2, 129)$, $(6, -2, 129)$, $(19, 3, 41)$, $(19, -3, 41)$ y rechazamos la segunda y cuarta puesto que son opuestos de la primera y tercera. En el artículo 289 dimos cuatro descomposiciones de la forma $(19, 3, 41)$. A partir de éstas obtenemos las descomposiciones del número 770 en $9 + 361 + 400$; $16 + 25 + 729$, $81 + 400 + 289$, $576 + 169 + 25$. Similarmente podemos encontrar cuatro descomposiciones de la forma $6t^2 + 4tu + 129u^2$ en

$$\begin{array}{ll} (t - 8u)^2 + (2t + u)^2 + (t + 8u)^2, & (t - 10u)^2 + (2t + 5u)^2 + (t + 2u)^2 \\ (2t - 5u)^2 + (t + 10u)^2 + (t + 2u)^2, & (2t + 7u)^2 + (t - 8u)^2 + (t - 4u)^2 \end{array}$$

Estos provienen directamente de los valores $(48, 369)$, $(62, -149)$, $(92, -159)$, $(202, 61)$ de la expresión $\sqrt{-(6, -2, 129)}$. Como resultado tenemos la descomposición del número 770 en $225 + 256 + 289$, $1 + 144 + 625$, $64 + 81 + 625$, $16 + 225 + 529$. Y no hay descomposiciones fuera de estas ocho.

En cuanto a la descomposición de números en tres cuadrados que tienen divisores comunes, se sigue tan fácilmente a partir del teorema general del artículo 281 que no hace falta recordarlo aquí.

Demostración de los Teoremas de Fermat: todo entero puede descomponerse en tres números triangulares o cuatro cuadrados.

293.

Los argumentos anteriores también proveen una demostración de aquel famoso teorema: *cualquier entero positivo puede descomponerse en tres números triangulares* que fue descubierto por Fermat, pero cuya prueba rigurosa se deseaba hasta ahora. Es claro que cualquier descomposición del número M en números triangulares

$$\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$$

producirá la descomposición del número $8M + 3$ en tres cuadrados impares

$$(2x+1)^2 + (2y+1)^2 + (2z+1)^2$$

y vice versa. Por la teoría anterior, cualquier entero positivo $8M+3$ se puede resolver en tres cuadrados que necesariamente serán impares (ver nota del artículo 291); y el número de resoluciones depende tanto del número de factores primos de $8M + 3$ como del número de clases entre las cuales están distribuidas las formas binarias de determinante $-(8M + 3)$. Habrá el mismo número de descomposiciones del número M en tres números triangulares. Sin embargo, hemos supuesto que para cualquier valor entero de x el número $\frac{1}{2}x(x+1)$ se ve como un número triangular; y si preferimos excluir al cero el teorema debe cambiarse como sigue: Cualquier entero positivo es o triangular o resoluble en dos o tres números triangulares. Un cambio similar se tendría que realizar en el siguiente teorema si quisiéramos excluir al cero como un cuadrado.

A partir de los mismos principios se demuestra otro teorema de Fermat que dice que *cualquier entero positivo se puede descomponer en cuatro cuadrados.* Si

restamos de un número de la forma $4n+2$ cualquier cuadrado (menor que el número), de un número de la forma $4n+1$ un cuadrado par, de un número de la forma $4n+3$ un cuadrado impar, el residuo en todos estos casos será resoluble en tres cuadrados, y el número dado, por lo tanto, en cuatro. Finalmente, un número de la forma $4n$ puede representarse como $4^{\mu}N$ de tal manera que N pertenezca a una de las tres formas anteriores; y cuando N está resuelto en cuatro cuadrados, $4^{\mu}N$ será también resoluble. Podríamos también remover de un número de la forma $8n+3$ el cuadrado de un raíz $\equiv 0 \pmod 4$, de un número de la forma $8n+7$ el cuadrado de un raíz $\equiv 2 \pmod 4$, de un número de la forma $8n+4$ un cuadrado impar y el residuo será resoluble en tres cuadrados. Pero este teorema ya ha sido probado por el ilustre Lagrange, *Nouv. Mém. de l'Ac. de Berlin*, 1770, *p.* 123. Y el ilustre Euler lo explicó mucho más completamente (de manera diferente de la nuestra) en *Acta Ac. Petr.* II, *p.* 48. Hay otros teoremas de Fermat que son como continuaciones de los anteriores. Dicen que cualquier entero es resoluble en cinco números pentagonales, seis hexagonales, siete heptagonales, etc. Pero aún les hace falta la prueba y parecen necesitar principios distintos para su resolución.

Solución de la ecuación $ax^2 + by^2 + cz^2 = 0$.

294.

TEOREMA. *Si los números a, b y c son primos relativos y ninguno* $= 0$ *ni es divisible por un cuadrado, la ecuación*

$$ax^2 + by^2 + cz^2 = 0 \ldots (\Omega)$$

no se puede resolver con enteros (excepto cuando $x = y = z = 0$*, lo cual no vamos a considerar), a menos que* $-bc$*,* $-ac$ *y* $-ab$ *respectivamente sean residuos cuadráticos de a, b y c y estos números tengan signos diferentes; pero cuando estas cuatro condiciones se cumplen,* (Ω) *se podrá resolver con enteros.*

Demostración. Si (Ω) es realmente resoluble por enteros, será también resoluble por valores de x, y y z que no tienen un divisor común; pues cualesquiera valores que satisfacen la ecuación (Ω) también la satisfarán si se dividen por su máximo común divisor. Ahora supongamos que $ap^2 + bq^2 + cr^2 = 0$ y que p, q y r no tienen un divisor común, también serán primos relativos dos a dos, pues si q y r tuvieran un divisor común μ, sería primo relativo a p, pero μ^2 dividiría a ap^2 y así también a a, contrario a la hipótesis, similarmente p, r; p, q deben ser primos relativos. Por esto

$-ap^2$ se representa por una forma binaria $by^2 + cz^2$ asignando a y y z los valores q y r, primos relativos; así su determinante $-bc$ será un residuo cuadrático de ap^2 y así también de a (art. 154); de la misma manera tendremos $-acRb$, $-abRc$. En cuanto a la condición de que (Ω) no admite una resolución si a, b y c tienen el mismo signo, es tan obvio que no necesita una explicación.

Para demostrar la proposición inversa que constituye la segunda parte del teorema, mostraremos *primero*, cómo encontrar una forma ternaria que sea equivalente a $\left(\begin{smallmatrix} a, & b, & c \\ 0, & 0, & 0 \end{smallmatrix}\right) \ldots f$ y escogida tal que los coeficientes segundo, tercero y cuarto sean divisibles por abc; y *segundo*, deduciremos una solución de la ecuación (Ω) a partir de esto.

I. Se buscan tres enteros A, B y C que no tengan un divisor común y escogidos de tal manera que A sea primo relativo a b y c; B sea primo relativo a a y c y C primo relativo a a y b. Entonces $aA^2 + bB^2 + cC^2$ será divisible por abc según se ve de lo siguiente. Sean $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ respectivamente valores de las expresiones $\sqrt{-bc} \pmod{a}$, $\sqrt{-ac} \pmod{b}$ y $\sqrt{-ab} \pmod{c}$ que necesariamente serán primos relativos a a, b y c respectivamente. Ahora escoja tres enteros arbitrarios $\mathfrak{a}, \mathfrak{b}$ y $\mathfrak{c}$ con la única condición de que sean primos relativos a a, b y c respectivamente (e.g. sean todos $= 1$) y determine A, B y C tales que

$$\begin{aligned} A &\equiv \mathfrak{b}c \pmod{b} \quad \text{y} \quad \equiv \mathfrak{c}\mathfrak{C} \pmod{c} \\ B &\equiv \mathfrak{c}a \pmod{c} \quad \text{y} \quad \equiv \mathfrak{a}\mathfrak{A} \pmod{a} \\ C &\equiv \mathfrak{a}b \pmod{a} \quad \text{y} \quad \equiv \mathfrak{b}\mathfrak{B} \pmod{b} \end{aligned}$$

Entonces resulta

$$aA^2 + bB^2 + cC^2 \equiv \mathfrak{a}^2(b\mathfrak{A}^2 + cb^2) \equiv \mathfrak{a}^2(b\mathfrak{A}^2 - \mathfrak{A}^2 b) \equiv 0 \pmod{a}$$

Así será divisible por a y similarmente por b y por c y también por abc . Además es evidente que A necesariamente es primo relativo a b y c; B a a y c; y C a a y b. Ahora, si los valores A, B y C resultan tener un (máximo) común divisor μ, éste necesariamente será primo relativo a a, b y c, y también a abc; por lo tanto si dividimos estos valores por μ obtendremos nuevos valores que no tienen un divisor común y que producirán un valor de $aA^2 + bB^2 + cC^2$ que aún será divisible por abc, y así satisface a todas las condiciones.

II. Si determinamos los números A, B y C de esta manera, los números Aa, Bb y Cc tampoco tendrán un divisor común. Pues si tuvieran un divisor común μ,

necesariamente tendría que ser primo relativo a a (el cual, de hecho, es primo relativo a Bb y Cc) y similarmente a b y c; por lo tanto μ también tendría que ser divisor de A, B y C contrario a la hipótesis. Por lo tanto podrán encontrarse enteros α, β y γ tales que $\alpha Aa + \beta Bb + \gamma Cc = 1$. Además, búsquense seis enteros α', β', γ', α'', β'' y γ'' tales que

$$\beta'\gamma'' - \gamma'\beta'' = Aa, \qquad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \qquad \alpha'\beta'' - \beta'\alpha'' = Cc$$

Ahora f se transformará por la sustitución

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

en $\left(\begin{smallmatrix} m, & m', & m'' \\ n, & n', & n'' \end{smallmatrix}\right) = g$ (que será equivalente a f) y digo que m', m'' y n serán divisibles por abc. Pues, sea

$$\begin{aligned} \beta''\gamma - \gamma''\beta = A', \qquad & \gamma''\alpha - \alpha''\gamma = B', \qquad & \alpha''\beta - \beta''\alpha = C' \\ \beta\gamma' - \gamma\beta' = A'', \qquad & \gamma\alpha' - \alpha\gamma' = B'', \qquad & \alpha\beta' - \beta\alpha' = C'' \end{aligned}$$

y tendremos

$$\begin{aligned} \alpha' = B''Cc - C''Bb, \qquad & \beta' = C''Aa - A''Cc, \qquad & \gamma' = A''Bb - B''Aa \\ \alpha'' = C'Bb - B'Cc, \qquad & \beta'' = A'Cc - C'Aa, \qquad & \gamma'' = B'Aa - A'Bb \end{aligned}$$

Si sustituimos estos valores en las ecuaciones

$$\begin{aligned} m' &= a\alpha'^2 + b\beta'^2 + c\gamma'^2 \\ m'' &= a\alpha''^2 + b\beta''^2 + c\gamma''^2 \\ n &= a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma'' \end{aligned}$$

tenemos, según el módulo a

$$\begin{aligned} m' &\equiv bcA''^2(B^2b + C^2c) \equiv 0 \\ m'' &\equiv bcA'^2(B^2b + C^2c) \equiv 0 \\ n &\equiv bcA'A''(B^2b + C^2c) \equiv 0 \end{aligned}$$

i.e. m', m'' y n serán divisibles por a; de manera similar se muestra que los mismos números son divisibles por b y por c y así que son divisibles por abc *Q. E. P.*

III. Pongamos, por razones de elegancia, d igual al determinante de las formas f y g, i.e. el número $-abc$. Entonces

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N''$$

Está claro que f se transforma por la sustitución (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

en la forma ternaria $\left(\begin{smallmatrix} Md, M'd, M''d \\ Nd, N'd, N''d \end{smallmatrix}\right) = g'$ de determinante d^3 que por lo tanto estará contenida en f. Ahora digo que la forma $\left(\begin{smallmatrix} d, 0, 0 \\ d, 0, 0 \end{smallmatrix}\right) = g''$ es necesariamente equivalente a g'. Pues es claro que $\left(\begin{smallmatrix} M, M', M'' \\ N, N', N'' \end{smallmatrix}\right) = g'''$ es una forma ternaria de determinante 1; además, puesto que por hipótesis a, b y c no pueden tener el mismo signo, f será una forma indefinida y fácilmente se concluye que g' y g'' también deben ser indefinidas; por lo tanto g''' será equivalente a la forma $\left(\begin{smallmatrix} 1, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$ (art. 277), y se podrá encontrar una transformación (S') de g''' en sí misma; es claro sin embargo que (S') dará una transformación de g' en g''. Por lo tanto g'' también estará contenida en f y mediante una combinación de las sustituciones (S) y (S') se deduce una transformación de f en g''. Si esta transformación es

$$\begin{matrix} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{matrix}$$

claramente tenemos una doble solución de la ecuación (Ω), a saber $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$ y $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; de manera similar es claro que no todos estos valores pueden ser $= 0$ a la vez, puesto que debemos tener

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d \quad Q.\ E.\ S.$$

Ejemplo. Sea $7x^2 - 15y^2 + 23z^2 = 0$ la ecuación propuesta. Es resoluble porque $345R7$, $-161R15$, $105R23$. Aquí los valores $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ serán 3, 7 y 6;

haciendo $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$ encontramos que $A = 98$, $B = -39$ y $C = -8$. De esto obtenemos la sustitución $\left\{\begin{matrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{matrix}\right\}$ mediante la cual f se transforma en $\left(\begin{matrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{matrix}\right) = g$. Y como resultado tenemos

$$(S) = \left\{\begin{matrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{matrix}\right\}, \quad g''' = \begin{pmatrix} 3670800, & 6, & -3 \\ & -1, -1246, & 4735 \end{pmatrix}$$

La forma g''' se transforma en $\left(\begin{matrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{matrix}\right)$ mediante la sustitución

$$\left\{\begin{matrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{matrix}\right\} \ldots (S')$$

Si combinamos esto con (S) obtenemos:

$$\left\{\begin{matrix} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3 \end{matrix}\right\}$$

que transformará f en g''. Tenemos entonces una solución doble de la ecuación propuesta $x = 11$, $y = 9$, $z = 4$ y $x = 12$, $y = -9$, $z = 3$; la segunda solución se simplifica dividiéndola por su divisor común 3 y tenemos $x = 4$, $y = -3$, $z = 1$.

295.

La segunda parte del teorema de la sección anterior también se puede resolver como sigue. Se busca un entero h tal que $ah \equiv \mathfrak{C} \pmod{c}$ (le asignamos los mismos significados a los caracteres $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$, que en el artículo anterior) y resulta $ah^2 + b = ci$. Es fácil ver que i es un entero y que $-ab$ es el determinante de la forma binaria $(ac, ah, i) \ldots \varphi$. Ciertamente esta forma no será positiva (puesto que como por hipótesis a, b y c no tienen el mismo signo, ab y ac no pueden ser positivos simultáneamente); además tendrá el número característico -1, que mostramos sintéticamente como sigue. Determine los enteros e y e' tales que

$$e \equiv 0 \pmod{a} \text{ y } \equiv \mathfrak{B} \pmod{b}; \quad ce' \equiv \mathfrak{A} \pmod{a} \text{ y } \equiv h\mathfrak{B} \pmod{b}$$

y (e, e') será un valor de la expresión $\sqrt{-(ac, ah, i)}$ (mod. $-ab$). Pues según el módulo a tenemos

$$e^2 \equiv 0 \equiv -ac, \qquad ee' \equiv 0 \equiv -ah$$
$$c^2 e'^2 \equiv \mathfrak{A}^2 \equiv -bc \equiv -c^2 i \quad \text{entonces} \quad e'^2 \equiv -i$$

y según el módulo b tenemos

$$e^2 \equiv \mathfrak{B}^2 \equiv -ac, \qquad cee' \equiv h\mathfrak{B}^2 \equiv -ach \quad \text{entonces} \quad ee' \equiv -ah$$
$$c^2 e'^2 \equiv h^2 \mathfrak{B}^2 \equiv -ach^2 \equiv -c^2 i \quad \text{entonces} \quad e'^2 \equiv -i$$

y las mismas tres congruencias que son válidas según cada uno de los módulos a y b por separado también serán válidos según el módulo ab. Entonces, por el teorema de formas ternarias, es fácil concluir que φ es representable por la forma $\left(\begin{smallmatrix} -1, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$. Suponga entonces que

$$act^2 + 2ahtu + iu^2 = -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Multiplicando por c obtenemos

$$a(ct + hu)^2 + bu^2 = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Ahora si le damos a t y u valores tales que ó $\gamma t + \delta u$ ó $\varepsilon t + \zeta u$ sea $= 0$, habrá una solución de la ecuación (Ω) que será satisfecha por

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha\delta - \beta\gamma$$

y por

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha\zeta - \beta\varepsilon$$

Es evidente que no todos los valores en cualquiera de los dos conjuntos puede ser $= 0$ simultáneamente, pues si $\delta c - \gamma h = 0$, $\gamma = 0$, tendríamos también $\delta = 0$ y $\varphi = -(\alpha t + \beta u)^2$, resultando $ab = 0$, contrario a la hipótesis y similarmente para los otros valores. En nuestro ejemplo encontramos que la forma φ es $(161, -63, 24)$, que el valor de la expresión $\sqrt{-\varphi}$ (mod. 105) $= (7, -51)$, y que la representación de la forma φ por $\left(\begin{smallmatrix} -1, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$ es

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$$

Esto nos da las soluciones $x = 7$, $y = 11$, $z = -8$; $x = 20$, $y = 15$, $z = -5$, o dividiendo por 5 e ignorando el signo de z, $x = 4$, $y = 3$, $z = 1$.

De los dos métodos para resolver la ecuación (Ω), el segundo es preferible porque utiliza números pequeños con más frecuencia; el primero, sin embargo, que puede acortarse mediante varios artificios que omitiremos aquí, parece ser más elegante, especialmente porque los números a, b y c se tratan de la misma manera y los cálculos no se alteran al permutarlos. Por otra parte, es en el segundo método donde tenemos los cálculos más convenientes si dejamos que a sea el menor y c el mayor de los tres números, como hicimos en nuestro ejemplo.

Sobre el método con el cual Legendre trató de demostrar su teorema fundamental.

296.

El elegante teorema que hemos explicado en los artículos anteriores fue descubierto por primera vez por el ilustre Legendre, *Hist. de l'Ac. de Paris*, 1785, *p.* 507, y lo justificó con una demostración bella (enteramente diferente de las dos nuestras). A la vez este geómetra sobresaliente trató de obtener a partir de ello una demostración de proposiciones que se ajustan al teorema fundamental de la sección anterior, pero ya hemos dicho en el artículo 151 que parecía no ser apropiado para este propósito. Entonces, éste es el lugar para explicar esta demostración (extremadamente elegante en sí) de manera breve y dar las razones de nuestra opinión. Empezamos con la siguiente observación: *si los números a, b y c, son todos* $\equiv 1 \pmod 4$, *la ecuación* $ax^2 + by^2 + cz^2 = 0 \ldots (\Omega)$ *no es resoluble.* En efecto, es fácil ver que en este caso el valor de $ax^2 + by^2 + cz^2$ necesariamente será ó $\equiv 1$, ó $\equiv 2$, ó $\equiv 3 \pmod 4$, excepto si todos los x, y y z son pares a la vez; por lo tanto, si Ω fuera soluble, esto no podría suceder excepto por valores pares de x, y y z, *Q. E. A.*, puesto que cualesquiera que sean los valores que satisfacen la ecuación Ω la seguirán satisfaciendo al dividirse por su máximo común divisor, así que por lo menos uno de los valores debe ser impar. Ahora se obtienen los diferentes casos del teorema por demostrar mediante las consideraciones siguientes.

I. Si p y q son números primos (diferentes y positivos) de la forma $4n + 3$, no podemos tener pRq y qRp a la vez. En efecto, si fuera posible, claramente al poner que $1 = a$, $-p = b$, $-q = c$, todas las condiciones para resolver la ecuación $ax^2 + by^2 + cz^2 = 0$ se cumplirán (art. 294); pero mediante la observación anterior, esta ecuación no tiene solución; por lo tanto, nuestra suposición es inconsistente. De esto sigue inmediatamente la proposición 7 del artículo 131.

II. Si p es un número primo de la forma $4n+1$ y q es un número primo de la forma $4n+3$, no se puede tener simultáneamente qRp y pNq. En efecto, tendríamos $-pRq$ y la ecuación $x^2 + py^2 - qz^2 = 0$ sería resoluble. De esto obtenemos los casos 4 y 5 del artículo 131.

III. Si p y q son números primos de la forma $4n + 1$, no se puede tener simultáneamente pRq y qNp. Sea r otro número primo de la forma $4n+3$ que sea un residuo de q y del cual p sea un no residuo. Entonces por los casos (II) ya demostrados tendremos qRr y rNp. Por lo tanto, si tenemos pRq y qNp tendríamos $qrRp$, $prRq$, $pqNr$ y luego $-pqRr$. Esto haría que la ecuación $px^2 + qy^2 - rz^2 = 0$ fuera resoluble, contrario a la observación anterior; y la suposición sería inconsistente. De esto siguen los casos 1 y 2 del artículo 131.

Este caso se puede tratar más elegantemente de la siguiente manera. Sea r un número primo de la forma $4n+3$ para el cual p sea un no residuo. Entonces tendremos rNp y por lo tanto (suponiendo pRq, qNp) $qrRp$; además, tenemos $-pRq$, $-pRr$, y así también $-pRqr$ y la ecuación $x^2 + py^2 - qrz^2 = 0$ sería resoluble contrario a la observación anterior, etc.

IV. Si p es un número primo de la forma $4n + 1$ y q un primo de la forma $4n + 3$, no se puede tener pRq y qNp simultáneamente. Sea r un número primo auxiliar de la forma $4n+1$ que es un no residuo de ambos p y q. Entonces tendremos (por II) qNr y (por III) pNr; por lo tanto $pqRr$; por lo tanto si pRq, qNp también tendríamos $prNq$, $-prRq$, $qrRp$; así pues la ecuación $px^2 - qy^2 + rz^2 = 0$ sería resoluble, *Q. E. A.* De esto obtenemos los casos 3 y 6 del artículo 131.

V. Si p y q son números primos de la forma $4n + 3$, no podemos tener pNq y qNp simultáneamente. En efecto, si se supone que esto es posible y se toma un número primo auxiliar r de la forma $4n + 1$ que sea un no residuo de ambos p y q, tendremos $qrRp$, $prRq$; además (por II) pNr, qNr y por lo tanto $pqRr$ y $-pqRr$; así que la ecuación $-px^2 - qy^2 + rz^2 = 0$ es posible, contrario a la observación anterior. De esto obtenemos el caso 8 del artículo 131.

297.

Examinando cuidadosamente la demostración anterior cualquier persona puede ver fácilmente que los casos I y II son totalmente completos, de modo que nadie puede objetarlos. Pero las demostraciones de los casos restantes se apoyan en la existencia de números auxiliares, y puesto que su existencia hasta el momento no se ha comprobado, el método claramente pierde toda su fuerza. Aunque estas

suposiciones son tan aparentes que parecen no requerir una demostración, y aunque ciertamente dan el más alto grado de *probabilidad* al teorema que estamos tratando de demostrar, no obstante, si queremos rigor geométrico no podemos simplemente aceptarlas de manera gratuita. En cuanto a la suposición en IV y V de que existe un número primo r de la forma $4n+1$ que es un no residuo de los otros primos dados p y q, es fácil concluir de la Sección IV que todos los números menores que $4pq$ y primos relativos con él (su número es $2(p-1)(q-1)$) se pueden distribuir equitativamente en cuatro clases. Una de ellas contendrá los no residuos de p y q y las tres restantes los residuos de p que son no residuos de q, los no residuos de p que son residuos de q y los residuos de ambos p y q; y en cada clase la mitad de los números serán de la forma $4n+1$ y la otra mitad de la forma $4n+3$. Entre ellos por lo tanto habrá $\frac{1}{4}(p-1)(q-1)$ que son no residuos de p y q de la forma $4n+1$. Los designaremos por g, g', g'', etc., y los restantes $\frac{7}{4}(p-1)(q-1)$ números por h, h', h'', etc. Todos los números contenidos en las formas $4pqt+g$, $4pqt+g'$, $4pqt+g''$, etc. $\ldots(G)$ también serán no residuos de p y q de la forma $4n+1$. Ahora está claro que para establecer nuestra suposición es necesario solamente establecer que las formas (G) contienen *números primos*. Y esto parece ser muy plausible puesto que estas formas junto con las formas $4pqt+h$, $4pqt+h'$, etc. $\ldots(H)$ contienen todos los números que son primos relativos a $4pq$ y son por lo tanto todos números primos absolutos (excepto 2, p y q); y no hay razón por la cual pensar que esta serie de números primos no sea distribuida equitativamente entre las formas de modo que un octavo pertenezca a (G) y el resto a (H). Pero obviamente este razonamiento está lejos del rigor geométrico. El ilustre Legendre mismo confesó que la demostración de un teorema que asegura que números primos ciertamente están contenidos en una forma $kt+l$ (donde k y l son números primos relativos dados y t indefinido) es bastante difícil y sugiere un método que puede ser útil. Nos parece que son necesarias muchas investigaciones preliminares antes de poder llegar a una demostración rigurosa por este camino. En cuanto a la otra suposición (III, segundo método) de que existe un número primo r de la forma $4n+3$ del cual otro número primo dado p de la forma $4n+1$ sea un no residuo, Legendre no agrega nada. Hemos mostrado anteriormente (art. 129) que ciertamente hay números primos para los cuales p es un no residuo, pero nuestro método no parece idóneo para mostrar que existen tales números primos *que sean además de la forma* $4n+3$ (como se requiere aquí pero no en nuestra primera demostración). Sin embargo, podemos probar fácilmente la validez de esta proposición como sigue. Por el artículo 287 existe un género positivo de formas binarias de determinante $-p$ cuyo carácter es 3,4; Np. Sea (a,b,c) tal forma y a impar (esto es permitido). Entonces a será de

la forma $4n + 3$ y primo en sí o al menos divisible por un factor primo r de la forma $4n + 3$. Sin embargo, tenemos $-pRa$ y así también $-pRr$ y como resultado pNr. Pero debemos notar cuidadosamente que las proposiciones de los artículos 263 y 287 dependen del teorema fundamental, y así tendríamos un círculo vicioso si basaramos alguna parte de esta discución en ellos. Finalmente, la suposición del primer método en III es tanto más gratuita que no hay razón por la cual añadir más sobre ella aquí.

Agreguemos una observación sobre el caso V que verdaderamente no ha quedado suficientemente comprobado por el método anterior; sin embargo será resuelto satisfactoriamente por lo que sigue. Si pNq y qNp fueran verdaderos simultáneamente, tendríamos $-pRq$ y $-qRp$, y es fácil verificar que -1 es un número característico de la forma $(p, 0, q)$ que podría entonces (según la teoría de formas ternarias) ser representada por la forma $x^2 + y^2 + z^2$. Sea

$$pt^2 + qu^2 = (\alpha t + \beta u)^2 + (\alpha' t + \beta' u)^2 + (\alpha'' t + \beta'' u)^2$$

o

$$\alpha^2 + \alpha'^2 + \alpha''^2 = p, \qquad \beta^2 + \beta'^2 + \beta''^2 = q, \qquad \alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0$$

y tendremos de las ecuaciones 1 y 2 que todos los números α, α', α'', β, β' y β'' son impares; pero entonces la tercera ecuación no puede ser consistente. El caso II se puede resolver de una manera similar a ésta.

298.

PROBLEMA. *Dados tres números cualesquiera a, b y c diferentes de cero; encontrar las condiciones para la solubilidad de la ecuación*

$$ax^2 + by^2 + cz^2 = 0 \ldots (\omega)$$

Solución. Sean α^2, β^2 y γ^2 los máximos divisores cuadrados de bc, ac y ab respectivamente y sea $\alpha a = \beta\gamma A$, $\beta b = \alpha\gamma B$, $\gamma c = \alpha\beta C$. Entonces A, B y C serán enteros primos relativos entre sí; la ecuación (ω) será resoluble o no según

$$AX^2 + BY^2 + CZ^2 = 0 \ldots (\Omega)$$

admita o no una solución de acuerdo con las normas del artículo 294.

Demostración. Sean $bc = \mathfrak{A}\alpha^2$, $ac = \mathfrak{B}\beta^2, ab = \mathfrak{C}\gamma^2$. $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ serán enteros libres de factores cuadrados y $\mathfrak{A} = BC$, $\mathfrak{B} = AC$, $\mathfrak{C} = AB$; como resultado $\mathfrak{ABC} = (ABC)^2$ y así $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ es necesariamente un entero. Sea m el máximo común divisor de los números $\mathfrak{A}$ y $A\mathfrak{A}$. Entonces $\mathfrak{A} = gm$, $A\mathfrak{A} = hm$ y g será primo relativo a h y (puesto que $\mathfrak{A}$ está libre de factores cuadrados) a m. Ahora tenemos $h^2m = gA^2\mathfrak{A} = g\mathfrak{BC}$ así que g divide a h^2m, lo cual es obviamente imposible a menos que $g = \pm 1$. Así $\mathfrak{A} = \pm m$, $A = \pm h$ y por lo tanto son enteros y como consecuencia B y C también serán enteros. *Q. E. P.* Puesto que $\mathfrak{A} = BC$ no tiene factores cuadrados, B y C deben ser primos relativos; y similarmente, A será primo relativo a C y a B. *Q. E. S.* Finalmente si $X = P$, $Y = Q$, $Z = R$ satisfacen la ecuación (Ω), la ecuación (ω) será satisfecha por $x = \alpha P$, $y = \beta Q$, $z = \gamma R$; en cambio si (ω) es satisfecha por $x = p$, $y = q$, $z = r$, (Ω) será satisfecha por $X = \beta\gamma p$, $Y = \alpha\gamma q$, $Z = \alpha\beta r$ y así si una es resoluble lo será también la otra. *Q. E. T.*

Representaciones de cero por formas ternarias cualesquiera

299.

PROBLEMA. *Dada la forma ternaria*

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

determinar si cero es representable por esta forma (sin que todas las incógnitas sean = 0 simultáneamente).

Solución. I. Cuando $a = 0$ los valores de x' y x'', se pueden tomar arbitrariamente y es claro de la ecuación

$$a'x'^2 + 2bx'x'' + a''x''^2 = -2x(b'x'' + b''x')$$

que x tomará un valor racional determinado; cuando obtenemos una fracción como valor de x, sólo debemos multiplicar los valores de x, x' y x'' por el denominador de la fracción para obtener enteros. Los únicos valores de x' y x'' que se deben excluir son aquéllos que hacen que $b'x'' + b''x' = 0$ a menos que también satisfagan $a'x'^2 + 2bx'x'' + a''x''^2 = 0$, en cuyo caso x es arbitrario. Así se pueden obtener todas las posibles soluciones. Pero el caso donde $b' = b'' = 0$ no se contempla aquí pues entonces x no participaría en la determinación de f; esto es, f es una forma binaria y la posible representación de cero por f debe decidirse a partir de la teoría de tales formas.

II. Cuando tenemos $a \neq 0$, la ecuación $f = 0$ será equivalente a

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = 0$$

al poner

$$b''^2 - aa' = A'', \qquad ab - b'b'' = B, \qquad b'^2 - aa'' = A'.$$

Ahora, cuando $A' = 0$ y $B \neq 0$ es claro que si tomamos $ax + b''x' + b'x''$ y x'' arbitrariamente, x y x' serán números racionales y cuando no son enteros se pueden hacer enteros mediante una multiplicación apropiada. Para un valor de x'', a saber $x'' = 0$, el valor de $ax + b''x' + b'x''$ no es arbitrario pero debe ser también $= 0$; pero el x' se puede tomar con completa libertad y producirá un valor de x racional. Cuando A'' y $B = 0$ simultáneamente, es claro que si A' es un cuadrado $= k^2$, la ecuación $f = 0$ se reduce a las siguientes dos ecuaciones lineales (donde una u otra debe tener lugar)

$$ax + b''x' + (b' + k)x'' = 0, \qquad ax + b''x' + (b' - k)x'' = 0$$

pero si (bajo la misma hipótesis) A' no es un cuadrado, la solución de la ecuación propuesta depende de las siguientes (ambas deben cumplirse) $x'' = 0$ y $ax + b''x' = 0$.

Será apenas necesario notar que el método de I es aplicable cuando a' o $a'' = 0$ y el método de II cuando $A' = 0$.

III. Cuando ni a ni $A'' = 0$, la ecuación $f = 0$ será equivalente a

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''^2 = 0$$

donde D es el determinante de la forma f y Da es el número $B^2 - A'A''$. Cuando $D = 0$ tendremos una solución como la del final del caso anterior; eso es, si A'' es un cuadrado $= k^2$, la ecuación propuesta se reduce a éstas:

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0, \qquad kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$$

pero si A'' no es un cuadrado, se debe tener

$$ax + b''x' + b'x'' = 0, \qquad A''x' - Bx'' = 0$$

Sin embargo, cuando D no es $= 0$ se nos reduce a la ecuación

$$A''t^2 - u^2 + Dav^2 = 0$$

una posibilidad que se puede decidir mediante el artículo anterior. Si esta ecuación no se puede resolver excepto para $t = 0$, $u = 0$ y $v = 0$, la ecuación propuesta no admite ninguna solución salvo $x = 0$, $x' = 0$ y $x'' = 0$; pero si tiene como solución cualquier otro conjunto de enteros t, u y v podemos mediante las ecuaciones

$$ax + b''x' + b'x'' = t, \qquad A''x' - Bx'' = u, \qquad x'' = v$$

obtener por lo menos valores racionales de x, x' y x''. Si éstas incluyen fracciones, podemos hacerlas enteros mediante una multiplicación apropiada.

Tan pronto se encuentra *una* solución de la ecuación $f = 0$ por enteros, el problema se reduce al caso I y todas las soluciones se pueden encontrar de la siguiente manera. Sean α, α' y α'' algunos valores de x, x' y x'' que satisfacen la ecuación $f = 0$. Supongamos que no tienen factores comunes. Ahora (por art. 40, 279) escoja enteros β, β', β'', γ, γ' y γ'' tales que

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1$$

y la forma f se transformará, por la sustitución

$$x = \alpha y + \beta y' + \gamma y'', \qquad x' = \alpha' y + \beta' y' + \gamma' y'', \qquad x'' = \alpha'' y + \beta'' y' + \gamma'' y'' \quad (S)$$

en la forma

$$g = cy^2 + c'y'^2 + c''y''^2 + 2dy'y'' + 2d'yy'' + 2d''yy'$$

Entonces se tendrá $c = 0$ y g será equivalente a f, de donde se concluye fácilmente que todas las soluciones por enteros de la ecuación $f = 0$ pueden obtenerse (por S) de todas las soluciones de $g = 0$. Y por I todas las soluciones de la ecuación $g = 0$ están contenidas en las fórmulas

$$y = -z(c'p^2 + 2dpq + c''q^2), \qquad y' = 2z(d''p^2 + d'pq), \qquad y'' = 2z(d''pq + d'q^2)$$

donde p y q son enteros cualesquiera , z un número cualquiera que puede ser una fracción siempre y cuando y, y' e y'' sean enteros. Si sustituimos estos valores de y, y' e y'' en (S), se tendrán todas las soluciones de la ecuación $f = 0$ por enteros. Así, por ejemplo, si

$$f = x^2 + x'^2 + x''^2 - 4x'x'' + 2xx'' + 8xx'$$

y una solución de la ecuación $f = 0$ es $x = 1$, $x' = -2$, $x'' = 1$; haciendo β, β', β'', γ, γ', $\gamma'' = 0$, 1, 0, 0, 0, 1 tenemos

$$g = y'^2 + y''^2 - 4y'y'' + 12yy''$$

Todas las soluciones de la ecuación $g = 0$ por enteros estarán contenidas en la fórmula

$$y = -z(p^2 - 4pq + q^2), \qquad y' = 12zpq, \qquad y'' = 12zq^2$$

y todas las soluciones de la ecuación $f = 0$ en las fórmulas

$$\begin{aligned} x &= -z(p^2 - 4pq + q^2) \\ x' &= 2z(p^2 + 2pq + q^2) \\ x'' &= -z(p^2 - 4pq - 11q^2) \end{aligned}$$

Solución general por racionales de ecuaciones de segundo grado en dos variables.

300.

A partir del problema del artículo anterior se obtiene inmediatamente la solución de la ecuación indeterminada

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

si se buscan sólo valores racionales. Ya la hemos resuelto para valores enteros (art. 216 y siguientes). Todo valor racional de x e y puede representarse por $\frac{t}{v}$ y $\frac{u}{v}$, donde t, u y v son enteros. Así pues, es claro que la solución de esta ecuación por números racionales es idéntica a la solución por enteros de la ecuación

$$at^2 + 2btu + cu^2 + 2dtv + 2euv + fv^2 = 0$$

y esto coincide con la ecuación tratada en el artículo anterior. Excluimos sólo aquellas soluciones donde $v = 0$; pero no puede ocurrir ninguna de este tipo cuando $b^2 - ac$ es un número no cuadrado. Así pues, e.g., toda solución por números racionales de la ecuación (resuelta de modo general por enteros en el art. 221)

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$$

estará contenida en la fórmula

$$x = \frac{p^2 - 4pq + q^2}{p^2 - 4pq - 11q^2}, \qquad y = -\frac{2p^2 + 4pq + 2q^2}{p^2 - 4pq - 11q^2}$$

donde p y q son enteros cualesquiera. Pero aquí hemos tratado brevemente estos dos problemas que están íntimamente conectados dejando por fuera muchas observaciones pertinentes para no hacernos demasiado prolijos. Tenemos otra solución del problema del artículo anterior basada en principios generales, sin embargo se tratará en otra ocasión puesto que requiere de un estudio más profundo de las formas ternarias.

Del número promedio de géneros.

301.

Regresemos ahora al estudio de las formas binarias de las cuales tenemos aún muchas propiedades notables que examinar. Primero le agregaremos algunas observaciones sobre el número de clases y géneros en un orden propiamente primitivo (positivo si el determinante es negativo) y para brevedad restringiremos nuestra investigación a éstas.

El *número de géneros* en los cuales se distribuyen todas las formas (propiamente primitivas positivas) de determinante $\pm D$ positivo o negativo es siempre 1, 2, 4 ó una potencia mayor de 2 cuyo exponente depende de los factores de D y que se puede encontrar a priori mediante el argumento presentado anteriormente. Ahora, puesto que en una serie de números naturales los números primos están mezclados con números más o menos compuestos, sucede que para muchos determinantes sucesivos $\pm D$, $\pm(D+1)$, $\pm(D+2)$, etc. el número de géneros crece y decrece de manera desordenada. Sin embargo, si sumamos los números de géneros correspondientes a muchos determinantes sucesivos

$$\pm D, \quad \pm(D+1), \quad \ldots \pm(D+m)$$

y dividimos la suma por el número de determinantes, obtenemos el *número promedio de géneros*. Se puede considerarlo como si correspondiera al determinante central $\pm(D + \frac{1}{2}m)$ de la serie y establece una progresión muy regular. Supongamos no sólo que m es suficientemente grande sino también que D sea mucho mayor, de modo que la razón de los determinantes extremos D, $D+m$ no difiera mucho de la igualdad. La regularidad de esta progresión debe entenderse así: si D' es un número mucho mayor

que D, el número promedio de determinantes alrededor de D' será notablemente mayor que alrededor de D; y si D y D' no difieren por mucho, el número promedio de géneros alrededor de D y D' será aproximadamente igual. Pero el número promedio de géneros alrededor del determinante positivo $+D$ siempre será aproximadamente igual al número de géneros alrededor del correspondiente determinante negativo y entre mayor sea el valor de D, más cierto será lo anterior mientras que para valores pequeños el número de géneros correspondiente al determinante positivo será un poco mayor que el del determinante negativo. Estas observaciones quedarán ilustradas mejor por los siguientes ejemplos tomados de la tabla que clasifica a las formas binarias para más de 4000 determinantes. Entre los cien determinantes de 801 a 900 hay 7 que corresponden a un único género, 32, 52, 8, 1, que corresponden respectivamente a 2, 4, 8, 16 géneros. Hay en total 359 géneros y un número promedio de 3,59. Los cien determinantes negativos de -801 a -900 producen 360 géneros. Los siguientes ejemplos se toman con determinantes negativos. En la centena 16 (desde -1501 a -1600) el número promedio de géneros es 3,89; en la centena 25 es 4,03; en la centena 51 es 4,24; para los 600 determinantes desde -9401 a -10000 es 4,59. De estos ejemplos es claro que el número promedio de géneros crece mucho más lentamente que los determinantes mismos, pero se busca la ley que describe esta progresión. Mediante una discusión teórica bastante difícil, cuya explicación sería demasiado larga para presentar aquí, se encontró que el número promedio de géneros alrededor de $+D$ o $-D$ puede calcularse aproximadamente por la fórmula

$$\alpha \log D + \beta$$

donde α y β son cantidades constantes y de hecho

$$\alpha = \frac{4}{\pi^2} = 0{,}4052847346$$

(π es la mitad de la circunferencia de un círculo de radio unitario),

$$\beta = 2\alpha g + 3\alpha^2 h - \frac{1}{6} a \log 2 = 0{,}8830460462$$

donde g es el valor de la serie

$$1 - \log(1+1) + \frac{1}{2} - \log(1+\frac{1}{2}) + \frac{1}{3} - \log(1+\frac{1}{3}) + \text{ etc.} = 0{,}5772156649$$

(ver Euler, *Inst. Calc. Diff.* p. 444) y h es el valor de la serie

$$\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 + \text{ etc.}$$

que es aproximadamente = 0,9375482543. A partir de esta fórmula es claro que el número promedio de géneros aumenta en una progresión aritmética si los determinantes aumentan en una progresión geométrica. Los valores que nos proporciona esta fórmula para $D = 850\frac{1}{2},\ 1550\frac{1}{2},\ 2450\frac{1}{2},\ 5050\frac{1}{2},\ 9700\frac{1}{2}$ resultan ser 3,617; 3,86; 4,046; 4,339; 4,604; los cuales difieren poco de los valores presentados anteriormente. Entre mayor sea el determinante central y el número de determinantes a partir de los cuales se calcula el promedio, menor será la diferencia entre el valor real y el que se obtiene con la fórmula. Con la ayuda de esta fórmula, también se puede encontrar la suma aproximada del número de géneros que corresponden a determinantes sucesivos $\pm D$, $\pm(D+1)$, $\ldots \pm(D+m)$ sumando el número promedio correspondiente a cada uno sin importar que tan separados estén D y $D+m$. Esta suma será

$$= \alpha\,(\log D + \log(D+1) + \text{ etc.} + \log(D+m)) + \beta(m+1)$$

o con bastante exactitud

$$= \alpha\,((D+m)\log(D+m) - (D-1)\log(D-1)) + (\beta-\alpha)(m+1)$$

De esta manera la suma del número de géneros para los determinantes -1 a -100 resulta ser 234,4, mientras que su valor real es 233; similarmente desde -1 a -2000 la fórmula nos da 7116,6 mientras que el valor real es 7112; de -9001 a -10000 el valor real es 4595 y el aproximado por la fórmula 4594,9, una aproximación mejor de lo que se podría esperar.

Del número promedio de clases.

302.

En cuanto al *número de clases* (siempre asumimos que son propiamente primitivas positivas) los determinantes positivos se comportan de una manera completamente diferente a los determinantes negativos; por lo tanto los consideraremos separadamente. Concuerdan en el hecho de que para un determinante dado hay igual

número de clases en cada género, y por lo tanto el número de clases es igual al producto del número de géneros por el número de clases en cada uno.

Primero, con respecto a los determinantes negativos, el número de clases que corresponde a varios determinantes sucesivos $-D$, $-(D+1)$, $-(D+2)$, etc. genera una progresión que es tan irregular como el número de géneros. El número promedio de clases, sin embargo, (no hace falta una definición) aumenta de manera muy regular como se notará en los siguientes ejemplos. Los cien determinantes de -500 a -600 proporcionan 1729 clases y así el número promedio es 17,29. Similarmente en la centena #15 el número promedio de clases es 28,26; para la #24 y #25 se calcula 36,28; para la #61, #62 y #63 resulta 58,50; para las cinco centenas de #91 a #95 se encuentra 71,56; finalmente para las cinco de 96 a 100 se tiene 73,54. Estos ejemplos muestran que el número promedio de clases crece más lentamente que los determinantes pero mucho más rápidamente que el número promedio de géneros; con una leve atención se puede ver que crece casi exactamente en proporción a la raíz cuadrada del determinante central. De hecho hemos encontrado mediante una investigación teórica que el número promedio de clases cerca del determinante $-D$ se puede expresar aproximadamente como

$$\gamma\sqrt{D} - \delta$$

donde

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$$

donde e es la suma de la serie

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} + \text{ etc.}$$

$$\delta = 0{,}2026423673 = \frac{2}{\pi^2}$$

Los valores promedios obtenidos mediante la fórmula difieren poco de los valores tomados de la tabla de clasificaciones mencionada arriba. Con la ayuda de esta fórmula también se puede aproximar el número de clases (propiamente primitivas positivas) que corresponden a los determinantes sucesivos $-D$, $-(D+1)$, $-(D+2)$, $\ldots -(D+m-1)$, sin importar la separación de los extremos, sumando los números promedios correspondientes a estos determinantes, obtenidos según la fórmula. Se encuentra una suma

$$= \gamma\left(\sqrt{D} + \sqrt{D+1} + \text{ etc.} + \sqrt{D+m-1}\right) - \delta m$$

o aproximadamente

$$= \frac{2}{3}\gamma \left((D+m-\frac{1}{2})^{\frac{3}{2}} - (D-\frac{1}{2})^{\frac{3}{2}} \right) - \delta m$$

Así pues, e.g., por medio de la fórmula la suma de los cien determinantes -1 a -100 será 481,1, mientras que el valor real es 477; los mil determinantes entre -1 y -1000 según la tabla proporcionan 15533 clases, mientras que el valor que nos da la fórmula es 15551,4; en el segundo milenio según la tabla hay 28595 clases, y según la fórmula 28585,7. Similarmente el tercer milenio realmente tiene 37092 clases; la fórmula da 37074,3; el décimo milenio posee 72549 según la tabla y 72572 según la fórmula.

303.

La tabla de determinantes negativos ordenados según varias clasificaciones ofrece muchas otras observaciones notables. Para determinantes de la forma $-(8n+3)$ el número de clases (tanto el número total como el número de clases contenido en cada género propiamente primitivo) es siempre divisible por tres, con la única excepción del determinante -3, como se puede concluir del artículo 256, VI. Para aquellos determinantes cuyas formas están contenidas en un solo género, el número de clases es siempre impar, puesto que para estos determinantes hay una única clase ambigua, la principal, las restantes clases siempre están opuestas en parejas y el número de ellas es por lo tanto par, lo cual hace impar el número total de clases. Esta última propiedad es también válida para determinantes positivos. Además, la serie de determinantes que corresponden a una clasificación dada (i.e. un número dado de géneros y de clases) parece siempre finita e ilustramos esta observación notable con los siguientes ejemplos. (El numeral romano indica el número de géneros propiamente primitivos positivos, el numeral arábigo el número de clases en cada género, luego sigue la serie de determinantes que corresponde a esta clasificación. Por razones de brevedad omitimos el signo negativo.)

I. $1 \ldots 1, 2, 3, 4, 7$

I. $3 \ldots 11, 19, 23, 27, 31, 43, 67, 163$

I. $5 \ldots 47, 79, 103, 127$

I. $7 \ldots 71, 151, 223, 343, 463, 487$

II. $1 \ldots 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58$

II. $2 \ldots 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193$

IV. $1 \ldots 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253$

VIII. $1 \ldots 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760$

XVI. $1 \ldots 840, 1320, 1365, 1848$

Similarmente, se encuentran 20 determinantes (el mayor $= -1423$) que corresponden a la clasificación I. 9; 4 (el mayor $= -1303$) que corresponden a la clasificación I. 11 etc; a las clasificaciones II. 3, II. 4, II. 5, IV. 2, corresponden no más de 48, 31, 44 y 69 determinantes respectivamente, donde los mayores son -652, -862, -1318 y -1012. Puesto que la tabla de la cual obtuvimos estos valores se ha extendido mucho más allá que el mayor determinante que aparece aquí*) y puesto que no proporciona ningún otro que pertenezca a estas clases, no hay duda de que las series anteriores terminan, y por analogía es permitido extender la conclusión a cualquier otra clasificación. Por ejemplo, puesto que en todo el décimo milenio de determinantes, no hay ninguno que corresponde a menos de 24 clases, es muy probable que las clasificaciones I. 23, I. 21, etc. II. 11, II. 10, etc. IV. 5, IV. 4, IV. 3; VIII. 2 están todas completas antes de llegar al número -9000 o que por lo menos tienen muy pocos determinantes mayores que -10000. Sin embargo, probar *rigurosamente* estas observaciones parece ser muy difícil. Es también notable que todo determinante cuyas formas se distribuyen entre 32 o más géneros tiene por lo menos dos clases en cada género y, por lo tanto, que las clasificaciones XXXII. 1, LXIV. 1 etc. no existen del todo (el determinante menor entre éstos es -9240 y corresponde a la clasificación XXXII. 2); y parece ser muy probable que cuando crece el número de géneros más clasificaciones desaparecen. En este aspecto los 65 determinantes mencionados anteriormente, aquéllos de las clasificaciones I. 1, II. 1, IV. 1, VIII. 1, XVI. 1, son bastante excepcionales, y es fácil ver que sólo ellos gozan de dos propiedades notables: todas las clases de las formas que pertenecen a ellos son ambiguas y todas las formas contenidas en el mismo género son a la vez propia e impropiamente equivalentes. El ilustre Euler en *Nouv. Mém. de l'Ac. de Berlin*, 1776, *p.* 338 ya ha determinado estos 65 números (bajo un aspecto ligeramente diferente que mencionaremos luego, y con un criterio que es fácil de demostrar).

*) Mientras esto estaba en impresión calculamos la tabla hasta -3000 *completamente* y también para todo el décimo milenio, para muchas centenas separadas y para muchos determinantes individuales cuidadosamente seleccionados.