207.

TEOREMA. *Dos formas reducidas* $(a, h, 0)$ *y* $(a', h, 0)$ *no idénticas no pueden ser propiamente equivalentes.*

Demostración. Si fueran propiamente equivalentes, la primera se transformaría en la segunda por una sustitución propia α, β, γ, δ y tendríamos las cuatro ecuaciones:

$$a\alpha^2 + 2h\alpha\gamma = a' \quad [1]$$

$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad [2]$$

$$a\beta^2 + 2h\beta\delta = 0 \quad [3]$$

$$\alpha\delta - \beta\gamma = 1 \quad [4]$$

Multiplicando la segunda ecuación por β, la tercera por α y restando, tenemos $-h(\alpha\delta - \beta\gamma)\beta = \beta h$ o, de [4], $-\beta h = \beta h$; de donde necesariamente β es $= 0$, por lo cual, usando [4], $\alpha\delta = 1$ y $\alpha = \pm 1$. Entonces de [1], $a \pm 2\gamma h = a'$, y esta ecuación no puede ser consistente a menos que $\gamma = 0$ (porque tanto a como a' por hipótesis están entre 0 y $2h - 1$), i.e. a menos que $a = a'$ o que las formas $(a, h, 0)$, $(a', h, 0)$ sean idénticas, lo que está en contra de la hipótesis .

Entonces los siguientes problemas, que ofrecían una mayor dificultad para los determinantes no cuadrados, pueden ser resueltos con muy poco esfuerzo.

I. *Dadas dos formas* F *y* F' *con el mismo determinante cuadrado investigar si son propiamente equivalentes o no.* Busquemos dos formas reducidas que sean propiamente equivalentes a las formas F y F' respectivamente. Si son idénticas, las formas dadas serán equivalentes; de otra manera, no lo serán.

II. *Dadas las mismas formas,* F *y* F'*, investigar si son impropiamente equivalentes o no.* Sea G la forma opuesta a una de las formas dadas, e.g. la forma F. Si G es propiamente equivalente a la forma F', F y F' serán propiamente equivalentes; de otra manera no lo serán.

208.

PROBLEMA. *Dadas dos formas propiamente equivalentes* F *y* F' *con determinante* h^2*, encontrar una transformación propia de una en la otra.*

Solución. Sea Φ una forma reducida propiamente equivalente a la forma F, que por hipótesis será también propiamente equivalente a la forma F'. Por el artículo 206 buscaremos una transformación propia α, β, γ, δ, de la forma F en Φ

y una transformación propia α', β', γ', δ' de la forma F' en Φ. Entonces Φ será transformada en F' por la transformación propia δ', $-\beta'$, $-\gamma'$, α' y entonces F en F' por la sustitución propia

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

Será útil desarrollar otra fórmula para la transformación de la forma F en F' para la cual no sea necesario conocer la forma reducida Φ. Supongamos que la forma

$$F = (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0)$$

Puesto que $\beta : \gamma$ es la razón con números menores igual a las razones $h - b : a$ o $c : -(h + b)$, es fácil ver que $\frac{h-b}{\beta} = \frac{a}{\delta}$ será un *entero*, que llamaremos f, y que $\frac{c}{\beta} = \frac{-h-b}{\delta}$ será también un entero, que llamaremos g. Tenemos, sin embargo:

$$A = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \quad \text{y por lo tanto} \quad \beta A = a\alpha^2\beta + 2b\alpha\beta\gamma + c\beta\gamma^2$$

o (sustituyendo $a\beta$ por $\delta(h - b)$ y c por βg)

$$\beta A = \alpha^2\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta^2\gamma^2 g$$

o sea (puesto que $b = -h - \delta g$)

$$\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$$

Similarmente

$$\begin{aligned} \delta A &= a\alpha^2\delta + 2b\alpha\gamma\delta + c\gamma^2\delta \\ &= \alpha^2\delta^2 f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma^2 h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f \end{aligned}$$

Por lo tanto

$$\alpha = \frac{\beta A - g}{2h}, \qquad \gamma = \frac{\delta A - f}{2h}$$

De exactamente la misma forma, poniendo

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \qquad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g'$$

tenemos

$$\alpha' = \frac{\beta' A - g'}{2h}, \qquad \gamma' = \frac{\delta' A - f'}{2h}$$

Si los valores $\alpha, \gamma, \alpha', \gamma'$ son sustituidos en la fórmula que acabamos de dar para la transformación de la forma F en F', obtenemos

$$\frac{\beta f' - \delta' g}{2h}, \quad \frac{\beta' g - \beta g'}{2h}, \quad \frac{\delta f' - \delta' f}{2h}, \quad \frac{\beta' f - \delta g'}{2h}$$

en donde A ha desaparecido completamente.

Si se dan formas impropiamente equivalentes F y F' y se busca una transformación impropia de una en la otra, sea G la forma opuesta a la forma F y sea α, β, γ, δ la transformación propia de la forma G en F'. Entonces, manifiestamente α, β, $-\gamma$, $-\delta$ será la transformación impropia de al forma F en F'.

Finalmente, si las formas dadas son propia e impropiamente equivalentes, este método nos puede dar dos transformaciones, una propia y la otra impropia.

209.

Ahora sólo resta mostrar cómo deducimos de una transformación todas las otras transformaciones similares. Esto depende de la solución de la ecuación indeterminada $t^2 - h^2 u^2 = m^2$, donde m es el máximo común divisor de los números a, $2b$, c y (a, b, c) es una de las formas equivalentes. Pero esta ecuación puede resolverse en sólo dos maneras, esto es, poniendo ya sea $t = m$, $u = 0$, o $t = -m$, $u = 0$. En efecto, supongamos que existe otra solución $t = T$, $u = U$, donde U no es $= 0$. Entonces, puesto que m^2 divide a $4h^2$, ciertamente obtendremos $\frac{4T^2}{m^2} = \frac{4h^2U^2}{m^2} + 4$ y tanto $\frac{4T^2}{m^2}$ como $\frac{4h^2U^2}{m^2}$ serán enteros cuadrados. Pero claramente el número 4 no puede ser la diferencia de dos enteros cuadrados, a no ser que el menor cuadrado sea 0, i.e., $U = 0$, en contra de la hipótesis. Por lo tanto, si la forma F se transforma en la forma F' por la sustitución α, β, γ, δ, no habrá otra transformación similar a ésta excepto $-\alpha$, $-\beta$, $-\gamma$, $-\delta$. Por lo tanto, si dos formas son sólo propiamente o sólo impropiamente equivalentes, habrá sólo *dos* transformaciones; pero si son propiamente e impropiamente equivalentes, habra *cuatro*, a saber, dos propias y dos impropias.

210.

Teorema. *Si dos formas reducidas* $(a, h, 0)$, $(a', h, 0)$ *son impropiamente equivalentes, resultará* $aa' \equiv m^2 \pmod{2mh}$, *donde* m *es el máximo común divisor*

de los números a, $2h$ o a', $2h$; y recíprocamente si a, $2h$ o a', $2h$ tienen el mismo máximo común divisor m y $aa' \equiv m^2 \pmod{2mh}$, las formas $(a, h, 0)$, $(a', h, 0)$ serán impropiamente equivalentes.

Demostración. I. Transfórmese la forma $(a, h, 0)$ en la forma $(a', h, 0)$ por la sustitución impropia α, β, γ, δ tal que tengamos cuatro ecuaciones

$$a\alpha^2 + 2h\alpha\gamma = a' \quad [1]$$

$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad [2]$$

$$a\beta^2 + 2h\beta\delta = 0 \quad [3]$$

$$\alpha\delta - \beta\gamma = -1 \quad [4]$$

Si multiplicamos [4] por h y restamos de [2], lo cual escribimos como $[2] - h[4]$, se sigue que

$$(a\alpha + 2h\gamma)\beta = 2h \quad [5]$$

Similarmente de $\gamma\delta[2] - \gamma^2[3] - (a + a\beta\gamma + h\gamma\delta)[4]$, al borrar los términos que se cancelan, tenemos

$$-a\alpha\gamma = a + 2h\gamma\delta \qquad \text{o} \qquad -(a\alpha + 2h\gamma)\delta = a \quad [6]$$

y finalmente de $a[1] \ldots a\alpha(a\alpha + 2h\gamma) = aa'$ o

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

o

$$(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)} \quad [7]$$

Ahora de [5] y [6] se sigue que $a\alpha + 2h\gamma$ divide a $2h$ y a a, de donde también a m, que es el máximo común divisor de a y $2h$; sin embargo manifiestamente m también divide a $a\alpha + 2h\gamma$; por lo tanto necesariamente $a\alpha + 2h\gamma$ será $= +m$ o $= -m$. Y se sigue inmediatamente de [7] que $m^2 \equiv aa' \pmod{2mh}$ *Q. E. P.*

II. Si a y $2h$, a' y $2h$ tienen el mismo máximo común divisor m y además $aa' \equiv m^2 \pmod{2mh}$, entonces $\frac{a}{m}, \frac{2h}{m}, \frac{a'}{m}, \frac{aa'-m^2}{2mh}$ serán enteros. Es fácil confirmar que la forma $(a, h, 0)$ será transformada en la forma $(a', h, 0)$ por la sustitución $\frac{-a'}{m}$, $\frac{-2h}{m}$, $\frac{aa'-m^2}{2mh}$, $\frac{a}{m}$, y que esta transformación es impropia. Por lo tanto las dos formas serán impropiamente equivalentes. *Q. E. S.*

De esto puede juzgarse inmediatamente si alguna forma reducida dada $(a, h, 0)$ es impropiamente equivalente a sí misma. Esto es, si m es el máximo común divisor de los números a y $2h$, deberemos tener $a^2 \equiv m^2 \pmod{2mh}$.

211.

Todas las formas reducidas de un determinante dado h^2 son obtenidas si en la forma indefinida $(A, h, 0)$ se sustituye A por todos los $2h$ números de 0 hasta $2h-1$ inclusive. Claramente todas las formas del determinante h^2 pueden ser distribuidas en este número de *clases* y tendrán las mismas propiedades mencionadas arriba (art. 175, 195) para las clases de formas con determinantes negativos y positivos no cuadrados. Entonces todas las formas con determinante 25 serán distribuidas en diez clases, que podrán distinguirse por las formas reducidas contenidas en cada una de ellas. Las formas reducidas serán: $(0,5,0)$, $(1,5,0)$, $(2,5,0)$, $(5,5,0)$, $(8,5,0)$, y $(9,5,0)$, cada uno de los cuales es impropiamente equivalente a sí misma; $(3,5,0)$ que es impropiamente equivalente a $(7,5,0)$, y $(4,5,0)$ que es impropiamente equivalente a $(6,5,0)$.

212.

PROBLEMA. *Encontrar todas las representaciones de un número dado M por una forma dada $ax^2+2bxy+cy^2$ con determinante h^2.*

La solución de este problema puede buscarse a partir de los principios del artículo 168 exactamente de la misma manera que enseñamos arriba (art. 180, 181, 205) para formas con determinantes negativos y positivos no cuadrados. Sería superfluo repetirla aquí, puesto que no ofrece dificultad alguna. Por otro lado, no estará fuera de lugar deducir la solución de otro principio que es propio para el caso presente.

Como en los artículos 206 y 208:

$$h-b : a = c : -(h+b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g$$

y se muestra sin dificultad que la forma dada es un producto de los factores $\delta x - \beta\gamma$ y $fx - gy$. Entonces es evidente que cualquier representación del número M por la forma dada debe proveer una resolución del número M en dos factores. Si, por lo tanto, todos los divisores del número M son d, d', d'', etc., (incluyendo también a 1 y M, y cada uno tomado *dos veces*, o sea positivamente y negativamente), es claro que todas las representaciones del número M serán obtenidas si se pone sucesivamente

que

$$\delta x - \beta y = d, \quad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \quad fx - gy = \frac{M}{d'} \text{ etc.}$$

Los valores de x e y se derivarán de aquí, y aquellas representaciones que producen valores fraccionales de x e y deberán ser descontadas. Pero, manifiestamente, de las dos primeras ecuaciones resulta

$$x = \frac{\beta M - gd^2}{(\beta f - \delta g)d} \qquad \text{e} \qquad y = \frac{\delta M - fd^2}{(\beta f - \delta g)d}$$

Estos valores serán siempre *determinados* porque $\beta f - \delta g = 2h$ y entonces el denominador con certeza no será $= 0$. Por lo demás, por el mismo principio podríamos haber resuelto los otros problemas respecto a la resolubilidad de cualquier forma con un determinante cuadrado en dos factores; pero preferimos usar un método análogo a aquél presentado arriba para formas con determinante no cuadrado.

Ejemplo. Buscaremos todas las representaciones del número 12 por la forma $3x^2 + 4xy - 7y^2$. Esto es resuelto en los factores $x - y$ y $3x + 7y$. Todos los divisores del número 12 son ± 1, 2, 3, 4, 6, 12. Poniendo $x - y = 1$ y $3x + 7y = 12$ obtenemos $x = \frac{19}{10}$ e $y = \frac{9}{10}$, lo que debe ser rechazado porque son fracciones. De la misma manera obtenemos valores inútiles de los divisores -1, ± 3, ± 4, ± 6, ± 12; pero del divisor $+2$ se obtienen los valores $x = 2$, $y = 0$ y del divisor -2, $x = -2$, $y = 0$. No existen, por lo tanto, otras representaciones excepto estas dos.

Este método no se puede usar si $M = 0$. En este caso, manifiestamente, todos los valores de x e y deben satisfacer ya sea la ecuación $\delta x - \beta y = 0$ o $fx - gy = 0$. Todas las soluciones de la primera ecuación están contenidas en la fórmula $x = \beta z$, $y = \delta z$, donde z es cualquier entero (mientras β y δ sean primos relativos, como supusimos); similarmente, si ponemos m como el máximo común divisor de los números f y g, todas las soluciones de la segunda ecuación estarán representadas por la fórmula $x = \frac{gz}{m}$, $y = \frac{hz}{m}$. Entonces estas dos fórmulas generales incluyen en este caso a todas las representaciones del número M.

En la discusión precedente todo lo concerniente a la equivalencia, al descubrimiento de todas las transformaciones de formas, y a la representación de números dados por formas dadas ha sido explicado satisfactoriamente. Solo resta, por consiguiente, mostrar cómo juzgar si una de dos formas dadas, que no pueden ser equivalentes porque tienen *determinantes no iguales*, está contenida en la otra o no, y, en este caso, encontrar las transformaciones de la una en la otra.

Formas contenidas en otras a las cuales no son equivalentes.

213.

En los artículos 157 y 158 arriba mostramos que, si la forma f con determinante D implica a la forma F con determinante E y es transformada en ella por la sustitución α, β, γ, δ, entonces $E = (\alpha\delta - \beta\gamma)^2 D$; y que si $\alpha\delta - \beta\gamma = \pm 1$, la forma f no sólo implica a la forma F sino que es equivalente a ella. Por consiguiente, si la forma f implica a F pero no es equivalente a ésta, el cociente $\frac{E}{D}$ es un entero mayor que 1. Este es el problema que por lo tanto deberá resolverse: *juzgar cuándo una forma dada f con determinante D implica a una forma dada F con determinante De^2* donde se supone que e es un número positivo mayor que 1. Para resolver esto, mostremos cómo asignar un número finito de formas contenidas en f, escogidas tal que si F está contenida en f, deba ser equivalente necesariamente a una de éstas.

I. Supongamos que todos los divisores positivos de un número e (incluyendo 1 y e) son m, m', m'' etc. y que $e = mn = m'n' = m''n''$ etc. Por brevedad, indicaremos por $(m; 0)$ la forma en la cual f es transformada por la sustitución propia m, 0, 0, n; por $(m; 1)$ la forma en la cual f es transformada por la sustitución propia m, 1, 0, n, etc.; y en general por $(m; k)$ la forma en la que f es cambiada por la sustitución propia m, k, 0, n. Similarmente, f será transformada por la transformación propia m', 0, 0, n' en $(m'; 0)$; por m', 0, 1, n' en $(m'; 1)$ etc.; por m'', 0, 0, n'' en $(m''; 0)$ etc.; etc. Todas estas formas estarán contenidas propiamente en f y el determinante de cada una será $= De^2$. Designaremos por Ω el conjunto de todas las formas $(m; 0)$, $(m; 1)$, $(m; 2)$, $\ldots (m; m-1)$, $(m'; 0)$, $(m'; 1)$, $\ldots (m'; m'-1)$, $(m''; 0)$, etc. Habrá $m + m' + m'' +$ etc. de ellas y es facil ver que todas serán diferentes la una de la otra.

Si, e.g., la forma f es $(2, 5, 7)$ y $e = 5$, Ω incluirá las siguientes formas $(1; 0)$, $(5; 0)$; $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$, y si son expandidas serán $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$.

II. Ahora, afirmo que si la forma F con determinante De^2 está propiamente contenida en la forma f, será necesariamente propiamente equivalente a una de las formas Ω. Supongamos que la forma f es transformada en F por la sustitución propia α, β, γ, δ; tendremos $\alpha\delta - \beta\gamma = e$. Sea n el máximo común divisor de los números γ, δ (que no pueden ser 0 al mismo tiempo) y sea $\frac{e}{n} = m$, lo que será, manifiestamente, un entero. Tómense g y h tal que $\gamma g + \delta h = n$, y finalmente sea k el residuo positivo mínimo del número $\alpha g + \beta h$ según el módulo m. Entonces la forma $(m; k)$, que está manifiestamente entre las formas Ω, será propiamente equivalente a la forma F y será

transformada en ella por la sustitución propia

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h,\quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g,\quad \frac{\gamma}{n},\quad \frac{\delta}{n}$$

Primeramente, es claro que estos cuatro números son enteros; *en segundo lugar*, es fácil confirmar que la sustitución es propia; *en tercer lugar*, es claro que la forma en la cual $(m;k)$ se transforma por esta sustitución es la misma en la que f*) se transforma por la sustitución

$$m(\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h)+k\frac{\gamma}{n},\quad m(\frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g)+\frac{k\delta}{n},\quad \gamma,\quad \delta$$

o puesto que $mn=e=\alpha\delta-\beta\gamma$ y entonces $\beta\gamma+mn=\alpha\delta$, $\alpha\delta-mn=\beta\gamma$, ésta es la sustitución

$$\frac{1}{n}(\alpha\gamma g+\alpha\delta h),\quad \frac{1}{n}(\beta\gamma g+\beta\delta h),\quad \gamma,\quad \delta$$

Pero $\gamma g+\delta h=n$, así que ésta es la sustitución α, β, γ, δ, i.e. por hipótesis ésta transforma f en F. Así $(m;k)$ y F serán propiamente equivalentes. *Q. E. D.*

De esto, por consiguiente, podemos siempre juzgar cuándo una forma dada f con determinante D implica propiamente a la forma F con determinante De^2. Si queremos encontrar cuándo f implica impropiamente a F, sólo necesitamos investigar cuándo la forma opuesta a F está contenida en f (art. 159).

214.

PROBLEMA. *Dadas dos formas, f con determinante D y F con determinante De^2, donde la primera implica propiamente a la segunda: encontrar todas las transformaciones propias de la forma f en F.*

Solución. Designando por Ω el mismo conjunto de formas como en el artículo precedente, extraiga de este conjunto todas las formas Φ, Φ', Φ'', etc. a las cuales F es propiamente equivalente. Cada una de estas formas proporcionará transformaciones propias de la forma f en F y cada una de ellas dará una transformación diferente, pero en total las proporcionarán todas (i.e., no habrá ninguna transformación propia de la forma f en F que no surja de una de las formas Φ, Φ', etc.). Puesto que el método es el mismo para todas las formas Φ, Φ', etc., hablamos de sólo una de ellas.

*) En efecto se transforma en $(m;K)$ por la sustitución m, K, 0, n. Vea artículo 159.

Supongamos que Φ es $(M;K)$ y $e = MN$ de manera que f se transforme en Φ por la sustitución propia M, K, 0, N. Además desígnense todas las transformaciones propias de la forma Φ en F en general por $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$. Entonces claramente f se transformará en Φ por la substitución propia $M\mathfrak{a} + K\mathfrak{c}$, $M\mathfrak{b} + K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$ y de esta manera cualquier transformación propia de la forma Φ en F dará una transformación propia de la forma f en F. Las otras formas Φ', Φ'', etc. se tratan del mismo modo, y cada transformación propia de una de éstas en F dará lugar a una transformación propia de la forma f en F.

Para mostrar que esta solución es completa en todo aspecto, se mostrará

I. *Que todas las transformaciones propias posibles de la forma f en F se obtienen de este modo.* Sea α, β, γ, δ cualquier transformación propia de la forma f en F y como en el artículo anterior, parte II, sea n el máximo común divisor de los números γ y δ; y sean los números m, g, h, k determinados tal como lo fueron allí. Entonces la forma $(m;k)$ estará entre las formas Φ, Φ', etc. y

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

será una de las transformaciones propias de esta forma en F; a partir de ésta, por la regla que acabamos de dar, se obtiene la transformación α, β, γ, δ; todo esto fue demostrado en el artículo precedente.

II. *Que todas las transformaciones obtenidas de esta manera son diferentes entre sí; esto es, ninguna de ellas se obtiene dos veces.* Es fácil ver que transformaciones diferentes de la misma forma Φ o Φ', etc. en F no pueden producir la misma transformación de f en F; se muestra de la siguiente manera que formas diferentes, por ejemplo Φ y Φ', no pueden producir la misma transformación. Supongamos que la transformación propia α, β, γ, δ de la forma f en F se obtiene *tanto de la transformación propia* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ *de la forma* Φ *en* F *como* de la transformación propia $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, $\mathfrak{d}'$ de la forma Φ' en F. Sean $\Phi = (M;K)$, $\Phi' = (M';K')$ y $e = MN = M'N'$. Habrá estas ecuaciones:

$$\alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' \quad [1]$$

$$\beta = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}' \quad [2]$$

$$\gamma = N\mathfrak{c} = N'\mathfrak{c}' \quad [3]$$

$$\delta = N\mathfrak{d} = N'\mathfrak{d}' \quad [4]$$

$$\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1 \quad [5]$$

De $\mathfrak{a}[4]-\mathfrak{b}[3]$ y usando ecuación [5] se sigue que $N = N'(\mathfrak{a}\mathfrak{d}'-\mathfrak{b}\mathfrak{c}')$, y de este modo N' divide a N; de manera análoga, de $\mathfrak{a}'[4]-\mathfrak{b}'[3]$ resulta $N' = N(\mathfrak{a}'\mathfrak{d}-\mathfrak{b}'\mathfrak{c})$ y N divide a N', de donde, dado que ambos N y N' se suponen positivos, tenemos necesariamente $N = N'$ y $M = M'$ y así de [3] y [4], $\mathfrak{c} = \mathfrak{c}'$ y $\mathfrak{d} = \mathfrak{d}'$. Además, de $\mathfrak{a}[2] - \mathfrak{b}[1]$,

$$K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$$

de aquí $K \equiv K'$ (mod. M), lo que no puede ser cierto a menos que $K = K'$, porque ambos K y K' se encuentran entre los límites 0 y $M - 1$. Por lo tanto las formas Φ y Φ' no son diferentes, contrariamente a la hipótesis.

Es claro que si D es negativo o un cuadrado positivo, este método nos dará todas las transformaciones propias de la forma f en F; y si D es positivo no cuadrado, pueden darse ciertas fórmulas generales que contendrán todas las transformaciones propias (su número es infinito).

Finalmente, si la forma F está impropiamente contenida en la forma f, todas las transformaciones impropias de la primera en la última pueden encontrarse fácilmente por el método dado. A saber, si α, β, γ, δ designan en general todas las transformaciones propias de la forma f en la forma opuesta a la forma F, todas las transformaciones impropias de la forma f en F serán representadas por α, $-\beta$, γ, $-\delta$.

Ejemplo. Se desean todas las transformaciones de la forma $(2, 5, 7)$ en $(275, 0, -1)$, la cual está contenida en ella tanto propia como impropiamente. En el artículo precedente dimos el conjunto de las formas Ω para este caso. Después de unos cálculos, se encuentra que tanto $(5; 1)$ como $(5; 4)$ son propiamente equivalentes a la forma $(275, 0, -1)$. Todas las transformaciónes propias de la forma $(5; 1)$, i.e., $(50, 35, 19)$ en $(275, 0, -1)$, se pueden hallar por nuestra teoría arriba dentro de la fórmula general

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u$$

donde t y u son representaciones indeterminadas de todos los enteros que satisfacen la ecuación $t^2 - 275u^2 = 1$; por lo tanto todas las transformaciones propias de la forma $(2, 5, 7)$ en $(275, 0, -1)$ estarán contenidas en la fórmula general

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u.$$

De manera análoga, todas las transformaciones propias de la forma $(5;4)$, i.e., $(50,65,79)$ en $(275,0,-1)$, están contenidas en la fórmula general

$$14t+275u, \quad t+14u, \quad -15t-275u, \quad -t-15u$$

y así todas las transformaciones propias de la forma $(2,5,7)$ en $(275,0,-1)$ estarán contenidas en

$$10t+275u, \quad t+10u, \quad -15t-275u, \quad -t-15u$$

Por lo tanto, estas dos fórmulas incluyen todas las transformaciones propias que buscamos*). De la misma manera se encuentra que todas las transformaciones impropias de la forma $(2,5,7)$ en $(275,0,-1)$ están contenidas en las dos fórmulas siguientes:

$$\text{(I)} \quad \ldots \quad 65t-1100u, \quad 4t-65u, \quad -15t+275u, \quad -t+15u$$

y

$$\text{(II)} \quad \ldots \quad 10t+275u, \quad -t-10u, \quad -15t-275u, \quad t+15u$$

Formas con determinante 0.

215.

Hasta ahora hemos excluido de todas las investigaciones las formas con determinante 0; ahora agreguemos algo acerca de estas formas para que nuestra teoría sea completa en todos los sentidos. Dado que se mostró en general que, si una forma con determinante D implica a una forma con determinante D', D' es un múltiplo de D, es inmediatamente claro que una forma cuyo determinante es igual a cero no puede implicar a otra forma a menos que su determinante también sea igual a cero. Así solamente dos problemas quedan por resolver, a saber: (1) *dadas dos formas f y F, donde F tiene determinante 0, juzgar si f implica a F o no, y,*

*) Más concisamente, todas las transformaciones propias se incluyen en la fórmula

$$10t+55u, \quad t+2u, \quad -15t-55u, \quad -t-3u$$

donde t y u son todos los enteros que satisfacen la ecuación $t^2-11u^2=1$.

en ese caso, exhibir todas las transformaciones involucradas; (2)*, encontrar todas las representaciones de un número dado por una forma dada con determinante 0.* El primer problema requiere de un método cuando el determinante de la forma f es también 0, otro cuando no es 0. Ahora explicamos todo esto.

I. Antes de todo observamos que cualquier forma $ax^2 + 2bxy + cy^2$ cuyo determinante es $b^2 - ac = 0$ puede ser expresada como $m(gx + hy)^2$ donde g y h son primos relativos y m un entero. Pues, sea m el máximo común divisor de a y c con el mismo signo que ellos (es fácil ver que ellos no pueden poseer signos opuestos), entonces $\frac{a}{m}$ y $\frac{c}{m}$ serán enteros primos relativos no negativos, y su producto será igual a $\frac{b^2}{m^2}$, i.e., un cuadrado, y así cada uno de ellos será también un cuadrado (art. 21). Sean $\frac{a}{m} = g^2$ y $\frac{c}{m} = h^2$ con g y h también primos relativos, y tenemos $g^2h^2 = \frac{b^2}{m^2}$ y $gh = \pm\frac{b}{m}$. Así es claro que

$$m(gx \pm hy)^2 \qquad \text{será} \qquad = ax^2 + 2bxy + cy^2$$

Sean ahora f y F dos formas dadas, cada una con determinante 0 y con

$$f = m(gx + hy)^2, \qquad F = M(GX + HY)^2$$

donde g y h, G y H son primos relativos. Afirmo ahora que si la forma f implica a la forma F, m es igual a M o al menos divide a M, y el cociente es un cuadrado; y, recíprocamente, si $\frac{M}{m}$ es un entero cuadrado, F está contenida en f. Pues si se asume que f se transforma en F, por la substitución

$$x = \alpha X + \beta Y, \qquad y = \gamma X + \delta Y$$

resultará

$$\frac{M}{m}(GX + HY)^2 = ((\alpha g + \gamma h)X + (\beta g + \delta h)Y)^2$$

y se sigue fácilmente que $\frac{M}{m}$ es un cuadrado. Igualándole a e^2, tenemos

$$e(GX + HY) = \pm\left((\alpha g + \gamma h)X + (\beta g + \delta h)Y\right), \quad \text{i.e.}$$
$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h$$

Por lo tanto si $\mathfrak{G}$ y $\mathfrak{H}$ se determinan de modo que $\mathfrak{G}G + \mathfrak{H}H = 1$ obtenemos

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h), \qquad \text{y por ende un } \textit{entero.} \quad \textit{Q. E. P.}$$

Si, recíprocamente, se supone que $\frac{M}{m}$ es un entero cuadrado igual a e^2, la forma f implicará a la forma F. Esto es, los enteros α, β, γ, δ pueden determinarse de modo que

$$\alpha g + \gamma h = \pm eG, \qquad \beta g + \delta h = \pm eH$$

Pues si se encuentran enteros $\mathfrak{g}$ y $\mathfrak{h}$ de modo que $\mathfrak{g}g + \mathfrak{h}h = 1$, podemos satisfacer estas ecuaciones poniendo:

$$\begin{aligned} \alpha &= \pm eG\mathfrak{g} + hz, \qquad & \gamma &= \pm eG\mathfrak{h} - gz \\ \beta &= \pm eH\mathfrak{g} + hz', \qquad & \delta &= \pm eH\mathfrak{h} - gz' \end{aligned}$$

donde z y z' pueden tomar valores enteros cualesquiera. Así F estará contenida en f. *Q. E. S.* Al mismo tiempo no es difícil ver que estas fórmulas dan todos los valores que α, β, γ, δ pueden asumir, i.e., todas las transformaciones de la forma f en F, a condición que z y z' asuman todos los valores enteros.

II. Propuestas las dos formas $f = ax^2 + 2bxy + cy^2$ cuyo determinante no es igual a 0, y $F = M(GX + HY)^2$ cuyo determinante es igual a 0 (aquí como antes G y H son primos entre si), afirmo *primero* que si f implica a F, el número M puede representarse por la forma f; *segundo*, si M puede representarse por f, F estará contenida en f; *tercero*, si en este caso todas las representaciones del número M por la forma f pueden ser exhibidas en términos generales por $x = \xi$ e $y = \nu$, todas las transformaciones de la forma f en F pueden exhibirse por $G\xi$, $H\xi$, $G\nu$, $H\nu$. Mostramos todo esto de la siguiente manera.

1^o Suponga que f se transforma en F por la substitución α, β, γ, δ y tómense números $\mathfrak{G}$, $\mathfrak{H}$ de modo que $\mathfrak{G}G + \mathfrak{H}H = 1$. Entonces si hacemos $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, el valor de la forma f se hará M y así M es representable por la forma f.

2^o Si se supone que $a\xi^2 + 2b\xi\nu + c\nu^2 = M$, por la substitución $G\xi$, $H\xi$, $G\nu$, $H\nu$ la forma f se transformará en F.

3^o En este caso la substitución $G\xi$, $H\xi$, $G\nu$, $H\nu$ presentará todas las transformaciones de la forma f en F si se supone que ξ y ν recorren todos los valores de x e y que hacen $f = M$; se muestra esto del siguiente modo. Sea α, β, γ, δ cualquier transformación de la forma f en F y sea como antes $\mathfrak{G}G + \mathfrak{H}H = 1$. Entonces entre los valores de x e y estarán también éstos:

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H}, \qquad y = \gamma\mathfrak{G} + \delta\mathfrak{H}$$

de los cuales se obtiene la substitución

$$G(\alpha\mathfrak{G}+\beta\mathfrak{H}), \qquad H(\alpha\mathfrak{G}+\beta\mathfrak{H}), \qquad G(\gamma\mathfrak{G}+\delta\mathfrak{H}), \qquad H(\gamma\mathfrak{G}+\delta\mathfrak{H})$$

o

$$\alpha+\mathfrak{H}(\beta G-\alpha H), \quad \beta+\mathfrak{G}(\alpha H-\beta G), \quad \gamma+\mathfrak{H}(\delta G-\gamma H), \qquad \delta+\mathfrak{H}(\gamma H-\gamma G).$$

Pero ya que

$$a(\alpha X+\beta Y)^2+2b(\alpha X+\beta Y)(\gamma X+\delta Y)+c(\gamma X+\delta Y)^2=M(GX+HY)^2$$

resultará

$$a(\alpha\delta-\beta\gamma)^2=M(\delta G-\gamma H)^2$$
$$c(\beta\gamma-\alpha\delta)^2=M(\beta G-\alpha H)^2$$

y así (ya que el determinante de la forma f multiplicado por $(\alpha\delta-\beta\gamma)^2$ es igual al determinante de la forma F, i.e., igual a 0, y así también $\alpha\delta-\beta\gamma=0$),

$$\delta G-\gamma H=0, \qquad \beta G-\alpha H=0$$

Por consiguiente la substitución en cuestión se reduce a α, β, γ, δ, y la fórmula que estamos considerando produce *todas* las transformaciones de la forma f en F.

III. Queda por mostrar cómo podemos exhibir todas las representaciones de un número dado por una forma dada con determinante 0. Sea esta forma $m(gx+hy)^2$, y es claro inmediatamente que el número debe ser divisible por m y que su cociente es un cuadrado. Si por lo tanto representamos al número dado por me^2, los valores de x e y que hacen $m(gx+hy)^2=me^2$ serán aquellos valores para los cuales $gx+hy$ sea igual a $+e$ o a $-e$. Así se tendrán todas las representaciones si se encuentran todas las soluciones enteras de las ecuaciones lineales $gx+hy=e$ y $gx+hy=-e$. Es claro que éstas son resolubles (si verdaderamente g y h son primos relativos como se supone). Esto es, si $\mathfrak{g}$ y $\mathfrak{h}$ son determinados de modo que $\mathfrak{g}g+\mathfrak{h}h=1$, la primera ecuación se satisfará poniendo $x=\mathfrak{g}e+hz$, $y=\mathfrak{h}e-gz$; la segunda tomando $x=-\mathfrak{g}e+hz$, $y=-\mathfrak{h}e-gz$ con z cualquier entero. Al mismo tiempo estas fórmulas darán *todos* los valores enteros de x e y si z representa en general a cualquier entero.

Solución general de toda ecuación indeterminada de segundo grado con dos incógnitas por numeros enteros.

Habiendo concluido exitosamente estas investigaciones, proseguimos.

216.

PROBLEMA. *Encontrar todas las soluciones enteras para la ecuación general**) indeterminada de segundo grado con dos incógnitas

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

(donde a, b, c, etc. son cualesquiera enteros dados).

Solución. En lugar de las incógnitas x e y introducimos otras

$$p = (b^2 - ac)x + be - cd \qquad \text{y} \qquad q = (b^2 - ac)y + bd - ae$$

que siempre serán enteros cuando x e y son enteros. Ahora resulta la ecuación

$$ap^2 + 2bpq + cq^2 + f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = 0$$

o si por brevedad escribimos

$$f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = -M$$

se da

$$ap^2 + 2bpq + cq^2 = M$$

Mostramos en la sección precedente cómo encontrar todas las soluciones de esta ecuación, i.e., todas las representaciones del número M por la forma (a, b, c). Ahora si para cada valor de p y q determinamos los valores correspondientes de x e y con la ayuda de las ecuaciones

$$x = \frac{p + cd - be}{b^2 - ac}, \qquad y = \frac{q + ae - bd}{b^2 - ac}$$

es fácil ver que todos estos valores satisfacen la ecuación dada y que no existen valores enteros de x e y que no se incluyen. Si por lo tanto eliminamos las fracciones entre todos los valores de x e y así obtenidos, todas las soluciones que deseamos permanecerán.

Con respecto a estas soluciones se observa lo siguiente.

---

*) Si se propusiera una ecuación en la cual el segundo, cuarto o quinto coeficiente no fuera par, su multiplicación por 2 produciría la forma que suponemos aquí.

1^o Si M no puede representarse por la forma $(a,\ b,\ c)$ o si no se obtienen valores *enteros* de x e y de ninguna representación, la ecuación no puede resolverse por enteros del todo.

2^o Cuando el determinante de la forma (a, b, c), i.e. el número $b^2 - ac$, es negativo o un cuadrado positivo y al mismo tiempo M no es igual a 0, el número de representaciones del número M será finito y así también el número de soluciones de la ecuación dada (si es que existe alguna) será finito.

3^o Cuando $b^2 - ac$ es positivo no cuadrado, o cuadrado con M igual a 0, el número M podrá representarse *en infinitamente distintas maneras* por la forma (a, b, c) si es que puede representarse de alguna manera. Pero dado que es imposible encontrar todas estas representaciones *individualmente* y examinar si ellas dan valores enteros o fraccionarios de x e y, es necesario establecer una regla bajo la cual podamos tener *certeza* de cuando ninguna representación en absoluto produce valores enteros de x e y (puesto que no importa cuántas representaciones se intenten, sin una regla tal nunca estaremos seguros). Y cuando algunas representaciones dan valores enteros de x e y y otras dan fracciones, debe determinarse cómo distinguir en general una de la otra.

4^o Cuando $b^2 - ac = 0$, los valores de x e y no pueden determinarse del todo por las fórmulas precedentes; por lo tanto para este caso necesitaremos recurrir a un *método especial*.

217.

Para el caso donde $b^2 - ac$ es un número positivo no cuadrado, mostramos arriba que todas las representaciones del número M por la forma $ap^2 + 2bpq + cq^2$ (si es que existe alguna) pueden exhibirse por una o por varias fórmulas como la siguiente:

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

donde $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ son enteros dados, m es el máximo común divisor de los números a, $2b$ y c, finalmente t y u son en general todos los enteros que satisfacen la ecuación $t^2 - (b^2 - ac)u^2 = m^2$. Como todos los valores de t y u pueden tomarse tanto positiva como negativamente, para cada una de estas formas podemos substituir otras *cuatro*:

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$
$$p = \frac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t - \mathfrak{D}u)$$
$$p = \frac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u)$$
$$p = -\frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = -\frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

de modo que el número de fórmulas es ahora cuatro veces lo que era antes, y t y u ya no son todos los números que satisfacen la ecuación $t^2 - (b^2 - ac)a^2 = m^2$ sino solamente los valores positivos. Por lo tanto cada una de estas formas será considerada separadamente, y debe investigarse cuáles valores de t y u dan valores enteros de x e y.

De la fórmula

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \qquad [1]$$

los valores de x e y serán éstos:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(b^2 - ac)}, \qquad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(b^2 - ac)}$$

Demostramos antes que todos los valores (positivos) de t forman una serie recurrente t^0, t', t'', etc. y similarmente, que los valores correspondientes de u también forman una serie recurrente u^0, u', u'', etc.; y que además puede asignarse un número ρ tal que según cualquier módulo dado tengamos

$$t^\rho \equiv t^0,\ t^{\rho+1} \equiv t',\ t^{\rho+2} \equiv t'' \text{ etc.}, \quad u^\rho \equiv u^0,\ u^{\rho+1} \equiv u',\ \text{etc.}$$

Tomaremos para este módulo el número $m(b^2 - ac)$ y por brevedad designaremos por x^0 e y^0 los valores de x e y que se obtienen haciendo $t = t^0$, $u = u^0$; de la misma manera x' e y' designarán los valores que se obtienen haciendo $t = t'$ y $u = u'$, etc. Entonces no es difícil notar que si x^h e y^h son enteros y ρ apropiadamente escogido, $x^{h+\rho}$ e $y^{h+\rho}$, $x^{h+2\rho}$ e $y^{h+2\rho}$ y, en general, $x^{h+k\rho}$ e $y^{h+k\rho}$ también serán enteros; y recíprocamente, si x^h o y^h es una fracción, $x^{h+k\rho}$ o $y^{h+k\rho}$ será también una fracción. Se concluye que si uno revisa los valores de x e y correspondientes a los índices 0, 1, 2, $\ldots \rho - 1$ y encuentra que no hay uno de ellos para el cual *tanto x como y* sea

entero, entonces no existen en absoluto índices, para los cuales ambos x e y posean valores enteros, y así de la fórmula [1] no se pueden deducir valores enteros de x e y. Pero si existen algunos índices, digamos μ, μ', μ'', etc., para los cuales x e y poseen valores enteros, entonces todos los valores de x e y que pueden obtenerse a partir de la fórmula [1] serán aquéllos cuyos índices estén contenidos en una de las fórmulas $\mu + k\rho$, $\mu' + k\rho$, $\mu'' + k\rho$, etc., donde k es cualquier entero positivo incluyendo al cero.

Las otras fórmulas que contienen los valores de p y q pueden tratarse exactamente de la misma manera. Si se diera el caso que de ninguna de éstas se obtienen valores enteros de x e y, entonces la ecuación propuesta no puede ser resuelta por enteros. Pero cuando ésta puede ser resuelta, todas las soluciones enteras se pueden mostrar por medio de las reglas precedentes.

218.

Cuando $b^2 - ac$ es un cuadrado y M es igual a cero, todos los valores de p y q están incluidos en dos fórmulas de la forma $p = \mathfrak{A}z$, $q = \mathfrak{B}z$ o $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, donde z indica de modo indefinido a cualquier entero, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ son enteros dados, y el primero y el segundo no han de poseer un divisor común, ni tampoco el tercero y el cuarto (art. 212). Todos los valores enteros de x e y que surgen de la primera fórmula estarán contenidos en la fórmula [1]:

$$x = \frac{\mathfrak{A}z + cd - be}{b^2 - ac}, \qquad y = \frac{\mathfrak{B}z + ae - bd}{b^2 - ac}$$

y todos los otros que surjan de la segunda fórmula estarán contenidos en [2]:

$$x = \frac{\mathfrak{A}'z + cd - be}{b^2 - ac}, \qquad y = \frac{\mathfrak{B}'z + ae - bd}{b^2 - ac}$$

Pero dado que cada fórmula puede producir valores fraccionarios (a menos que $b^2 - ac = 1$), es necesario separar de los otros, en cada fórmula, aquellos valores de z que hacen a ambos x e y enteros. Sin embargo, es suficiente considerar la primera fórmula solamente, dado que exactamente el mismo método puede usarse para la otra.

Como $\mathfrak{A}$ y $\mathfrak{B}$ son primos relativos, se pueden determinar dos números $\mathfrak{a}$ y $\mathfrak{b}$ tales que $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$. De esto se obtiene

$$(\mathfrak{a}x + \mathfrak{b}y)(b^2 - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$$

De esto es inmediatamente claro que todos los valores de z que producen valores enteros de x e y deben ser congruentes al número $\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$ según el módulo b^2-ac, o deben estar contenidos en la fórmula $(b^2-ac)z'+\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$ donde z' designa cualquier entero. Entonces en lugar de la fórmula [1] obtenemos fácilmente la siguiente:

$$x = \mathfrak{A}z' + \mathfrak{b}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{b^2-ac}$$
$$y = \mathfrak{B}z' - \mathfrak{a}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{b^2-ac}$$

Queda de manifiesto que ésta da valores enteros para x e y ambos para todos los valores de z' o para ninguno. Lo primero será cierto cuando $\mathfrak{A}(bd-ae)$ y $\mathfrak{B}(be-cd)$ sean congruentes según el módulo b^2-ac, el último cuando ellos no sean congruentes. Podemos tratar la fórmula [2] exactamente de la misma manera y separar las soluciones enteras (si existe alguna) del resto.

219.

Cuando $b^2-ac=0$, la forma $ax^2+2bxy+cy^2$ puede expresarse como $m(\alpha x+\beta y)^2$ donde m, α, β son enteros (art. 215). Si se pone $\alpha x+\beta y=z$, la ecuación se convertirá en:

$$mz^2+2dx+2ey+f=0$$

De esto y del hecho que $z=\alpha x+\beta y$ deducimos que

$$x=\frac{\beta mz^2+2ez+\beta f}{2\alpha e-2\beta d}, \qquad y=\frac{\alpha mz^2+2dz+\alpha f}{2\beta d-2\alpha e}$$

Ahora es claro que si no fuera $\alpha e=\beta d$ (consideraremos este caso por separado de inmediato), los valores de x e y obtenidos a medida que z toma cualquier valor en estas fórmulas, satisfarán la ecuación dada; por lo tanto, sólo queda por demostrar cómo determinar los valores de z que darán valores enteros de x e y.

Dado que $\alpha x+\beta y=z$, puede escogerse sólo valores *enteros* para z. Además es claro que si cualquier valor de z da valores enteros tanto para x como para y, todos los valores congruentes con z según el módulo $2\alpha e-2\beta d$ producirán de la

misma manera valores enteros. Por esto si se substituyen en z todos los enteros de 0 a $2\alpha e - 2\beta d - 1$ (cuando $\alpha e - \beta d$ es positivo) o inclusive a $2\beta d - 2\alpha e - 1$ (cuando $\alpha e - \beta d$ es negativo), y si para ninguno de estos valores se hacen x e y enteros, entonces ningún valor de z producirá valores enteros para x e y, y la ecuación dada no podrá resolverse por enteros. Pero si x e y poseen valores enteros para alguno de esos valores de z, digamos ζ, ζ', ζ'', etc., (ellos también pueden hallarse resolviendo la congruencia de segundo grado de acuerdo con los principios de la sección IV), se encuentran *todas* las soluciones poniendo $z = (2\alpha e - 2\beta d)\nu + \zeta$, $z = (2\alpha e - 2\beta d)\nu + \zeta'$, etc., con ν tomando todos los valores enteros.

220.

Es conveniente indagar un método especial para el caso que hemos excluído, donde $\alpha e = \beta d$. Supongamos que α y β son primos entre sí, lo cual es posible por el artículo 215.I; así $\frac{d}{\alpha} = \frac{e}{\beta}$ será un entero (art. 19), que llamamos h. Entonces, la ecuación dada tomará esta forma:

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf = 0$$

y claramente ésta no puede resolverse racionalmente, a menos que $h^2 - mf$ sea un cuadrado. Sea $h^2 - mf = k^2$, y la ecuación dada será equivalente a las siguientes dos:

$$m\alpha x + m\beta y + h + k = 0, \qquad m\alpha x + m\beta y + h - k = 0$$

i.e., cualquier solución de la ecuación dada satisfará una u otra de estas ecuaciones y viceversa. Obviamente la primera ecuación no puede resolverse por enteros a menos que $h + k$ sea divisible por m, y, similarmente, la segunda ecuación no admitirá solución por enteros a no ser que $h - k$ sea divisible por m. Estas condiciones son suficientes para resolver todas las ecuaciones (porque nosotros asumimos que α y β son primos entre sí) y puede encontrarse todas las soluciones usando reglas bien conocidas.

221.

Ilustramos con un ejemplo el caso del artículo 217 (pues éste es el más difícil). Sea $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$ la ecuación dada. Por la introducción de otros indeterminados $p = 15x - 9$ y $q = 15y + 6$, se deriva la ecuación $p^2 + 8py + q^2 = -540$.

Todas las soluciones por enteros de esta ecuación se encuentran por consiguiente contenidas en las siguientes cuatro fórmulas:

$$\begin{aligned} p &= 6t, & q &= -24t - 90u \\ p &= 6t, & q &= -24t + 90u \\ p &= -6t, & q &= 24t - 90u \\ p &= -6t, & q &= 24t + 90u \end{aligned}$$

donde t y u denotan todos los enteros positivos que satisfacen la ecuación $t^2 - 15u^2 = 1$, y ellos se expresan por la fórmula:

$$\begin{aligned} t &= \frac{1}{2}\left((4+\sqrt{15})^n + (4-\sqrt{15})^n\right) \\ u &= \frac{1}{2\sqrt{15}}\left((4+\sqrt{15})^n - (4-\sqrt{15})^n\right) \end{aligned}$$

donde n designa a todos los enteros positivos (incluido el cero). Por esto todos los valores de x e y estarán contenidos en estas fórmulas

$$\begin{aligned} x &= \frac{1}{5}(2t+3), & y &= -\frac{1}{5}(8t+30u+2) \\ x &= \frac{1}{5}(2t+3), & y &= -\frac{1}{5}(8t-30u+2) \\ x &= \frac{1}{5}(-2t+3), & y &= \frac{1}{5}(8t-30u-2) \\ x &= \frac{1}{5}(-2t+3), & y &= \frac{1}{5}(8t+30u-2) \end{aligned}$$

Si aplicamos correctamente lo que hemos dicho arriba, descubrimos que para producir enteros debemos usar en la primera y segunda fórmulas valores de t y u que vienen de tomar n *par*; en la tercera y cuarta de tomar n *impar*. Las soluciones más simples son: $x = 1, -1, -1$ e $y = -2, 0, 12$ respectivamente.

Por otra parte, observamos que la solución del problema en los artículos precedentes puede a menudo acortarse por varios artificios especialmente ideados para excluir soluciones inútiles, i.e., fracciones; pero debemos omitir esta discusión a fin de no prolongar nuestra discusión más allá de los límites.

Anotaciones Históricas.

222.

Dado que mucho de lo que hemos explicado también ha sido tratado por otros geómetras, no podemos pasar sobre sus trabajos en silencio. El ilustre Lagrange emprendió investigaciones generales concernientes a la *equivalencia de las formas* en *Nouv. Mém. de l'Ac. de Berlin*, 1773, *p.* 263 y 1775, *p.* 323 y siguientes, donde él mostró, que para un determinante dado, puede encontrarse un número finito de formas tales que cada forma de ese determinante sea equivalente a una de éstas, y así que todas las formas de un determinante dado pueden distribuirse en clases. Más tarde el distinguido Legendre descubrió, en gran parte por inducción, muchas propiedades elegantes de esta clasificación, cuyas demostraciones presentaremos más abajo. Hasta aquí nadie ha usado la distinción entre equivalencia propia e impropia, pero este es un instrumento muy efectivo para investigaciones más sutiles.

Lagrange fue el primero en resolver completamente el famoso problema del artículo 216 y siguientes, *Hist. de l'Ac. de Berlin*, 1767, *p.* 165 y 1768 *p.* 181 y siguientes. También existe una solución (pero menos completa) en el suplemento al *Algebra* de Euler, el cual hemos nombrado regularmente. El mismo Euler atacó este problema en *Comm. Petr., T.* VI, *p.* 175, *Comm. Nov., T.* IX, *p.* 3; *Ibid., T.* 18, *p.* 185 y siguientes, pero él siempre restringió su investigación a derivar otras soluciones de una que él asumía ya conocida; además, sus métodos pueden dar *todas* las soluciones en solamente unos cuantos casos (véase Lagrange *Hist. de l'Ac. de Berlin*, 1767, *p.* 237). Ya que el último de estos tres comentarios es de fecha más reciente que la solución de Lagrange, que trata el problema con toda generalidad y no deja nada que desear en este aspecto, parece que Euler no sabía entonces de esa solución (el Vol. 18 de los *Commentarii* corresponde al año 1773 y fue publicado en 1774). Por lo demás, nuestra solución (al igual que todas las cosas discutidas en esta sección) es construida sobre principios totalmente diferentes.

Lo que Diofanto, Fermat, etc., entre otros, han tratado en relación con este tema pertenece solamente a casos especiales; por esto, ya que arriba hemos mencionado lo más digno de notar, no lo discutiremos separadamente.

Lo que ha sido dicho hasta aquí acerca de las formas de segundo grado debe ser considerado solamente como los primeros principios de esta teoría. El campo dejado para investigación posterior parece muy vasto, y en lo que sigue notaremos cualquier cosa que parezca especialmente digna de atención. Pero esta línea del argumento es tan fértil que deberemos pasar sobre muchos otros resultados que hemos descubierto, y sin duda muchos más permanecerán ocultos, esperando una

más amplia investigación. Finalmente, conviene notar que formas con determinante 0 están excluidas de los límites de nuestra investigación, a menos que específicamente mencionemos lo contrario.

Distribución de formas de un determinante dado en clases.

223.

Ya hemos mostrado (arts. 175, 195, 211) que, dado cualquier entero D (positivo o negativo) se puede asignar un número finito de formas F, F', F'', etc. con determinante D, tal que cada forma de determinante D sea propiamente equivalente a una, y sólo una, de éstas. Así todas las formas con determinante D (su número es infinito) pueden *clasificarse* según estas formas para componer una primera clase del conjunto de todas las formas propiamente equivalentes a la forma F; una segunda clase de formas que son propiamente equivalentes a la forma F', etc.

Una forma puede seleccionarse de cada una de las clases de formas con determinante dado D, y ésta será considerada como la *forma representante* de toda la clase. De por sí es enteramente arbitrario cuál forma es tomada de una clase dada, pero se debe preferir siempre la que parezca ser *más simple que las demás*. La simplicidad de una forma (a, b, c) ciertamente debe ser juzgada por el tamaño de los números a, b, c, y así la forma (a', b', c') se dice menos simple que (a, b, c) si $a' > a$, $b' > b$, $c' > c$. Pero esto no nos concede una determinación completa porque estaría ligeramente indefinido si e.g., escogemos $(17, 0, -45)$ o $(5, 0, -153)$ como la forma más simple. Sin embargo, muy a menudo sería ventajoso observar las siguientes normas.

I. Cuando el determinante D es negativo, se toman las formas reducidas en cada clase como las formas representantes; cuando dos formas en la misma clase son formas reducidas (ellas serán opuestas, art. 172), se toma aquélla cuyo término medio sea positivo.

II. Cuando el determinante D es positivo no cuadrado, se calcula el período de toda forma reducida contenida en la clase. Existirán o bien dos formas ambiguas o ninguna (art. 187).

1) En el primer caso sean (A, B, C) y (A', B', C') las formas ambiguas; y sean M y M' los residuos mínimos de los números B y B' según los módulos A y A' respectivamente (que se pueden tomar positivamente a menos que sean iguales a cero); finalmente, sean $\frac{D-M^2}{A} = N$, $\frac{D-M'^2}{A'} = N'$. Habiendo hecho esto, de las formas $(A, M, -N)$ y $(A', M', -N')$, tómese como forma representante aquélla que parezca ser la más simple. Para juzgar esto, la forma cuyo término medio es igual a

cero es la preferida; cuando el término medio es cero o es distinto de cero en ambas, la forma que posee el menor primer término se prefiere sobre la otra, y cuando los primeros términos sean iguales en tamaño pero con signos opuestos, aquélla con el signo positivo será la preferida.

2) Cuando no hay formas ambiguas en todo el período, se elige la forma cuyo primer término sea menor, sin importar el signo. Si ocurren dos formas en el mismo período, una con signo positivo y la otra con el mismo término con signo negativo, se deberá tomar la de signo positivo. Sea (A, B, C) la forma escogida y como en el caso anterior deducimos otra forma $(A, M, -N)$ a partir de ésta (esto es, tomando M como el menor residuo absoluto de B relativo al módulo A, y haciendo $N = \frac{D-M^2}{A}$); ésta será la forma representante.

Si sucediera que el mismo menor primer término A fuera común a varias formas del período, trátense todas estas formas de la manera que ya hemos delineado, y de las formas resultantes escójase como la forma representante aquélla que posea el menor término medio.

Así, e.g., para $D = 305$ uno de los períodos es: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, del cual se escoje la forma $(7, 16, -7)$, y entonces se deduce la forma representante $(7, 2, -43)$.

III. Cuando el determinante es un cuadrado positivo igual a k^2, se busca una forma reducida $(A, k, 0)$ en la clase bajo consideración y, si $A < k$ o $= k$, ésta es tomada como forma representante. Pero si $A > k$, tómese en su lugar la forma $(A - 2k, k, 0)$. El primer término será negativo, pero menor que k.

Ejemplo. De esta manera todas las formas del determinante -235 se distribuirán en dieciseis clases con los siguientes representantes: $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$ y otras ocho que son diferentes de las anteriores solamente en que poseen términos exteriores con signos opuestos: (-1, 0, -235), $(-2, 1, -118)$, etc.

Las formas con determinante 79 caen en seis clases con los siguientes representantes: $(1, 0, -79)$, $(3, 1, -26)$, $(3, -1, -26)$, $(-1, 0, 79)$, $(-3, 1, 26)$, $(-3, -1, 26)$.

224.

Mediante esta clasificación, formas que son propiamente equivalentes pueden separarse completamente de todas las demás. Dos formas con el mismo determinante serán propiamente equivalentes si ellas pertenecen a la misma clase; cualquier número

que sea representable por una de ellas será también representable por la otra; y si un número cualquiera M puede representarse por la primera forma de tal manera que los valores indeterminados sean primos entre sí, el mismo número podrá ser representado por la otra forma de la misma manera y, claro está, de manera que cada representación pertenezca al mismo valor de la expresión $\sqrt{D}$ (mod. M). Si, no obstante, dos formas pertenecen a diferentes clases, ellas no serán propiamente equivalentes; y si un número dado es representado por una de las formas, nada puede decirse con respecto a si éste es representable por la otra. Por otro lado, si el número M puede ser representado por una de éstas de tal manera que los valores de los indeterminados sean primos entre sí, podemos estar seguros inmediatamente que no existe representación similar del mismo número por otra forma que pertenezca al mismo valor de la expresión $\sqrt{D}$ (mod. M) (véanse arts. 167, 168).

Puede suceder, sin embargo, que dos formas F y F' que provienen de clases diferentes, K y K', sean impropiamente equivalentes, en este caso *toda* forma de una de las clases será impropiamente equivalente a *todas* las formas de la otra clase. Toda forma de K poseerá una forma opuesta en K' y las clases se llamarán *opuestas*. Así, en el primer ejemplo del artículo precedente, la tercera clase de formas con determinante -235 es opuesta a la cuarta, la sétima a la octava; en el segundo ejemplo, la segunda clase es opuesta a la tercera y la quinta a la sexta. Por esto, dadas dos formas cualesquiera de dos clases opuestas, cualquier número M que pueda representarse por una, también puede ser representado por la otra. Si en una esto sucede por valores primos entre sí de las indeterminadas, esto podrá suceder también en la otra pero de tal manera que estas dos representaciones correspondan a valores opuestos de la expresión $\sqrt{D}$ (mod. M). Además, las reglas dadas arriba para la elección de formas representantes están fundadas de modo que clases opuestas siempre dan origen a formas representantes opuestas.

Finalmente, existen clases que son *opuestas a sí mismas*. A saber, si alguna forma y su opuesta están contenidas en la misma clase, es fácil ver que todas las formas de esta clase son tanto propia como impropiamente equivalentes a alguna otra y que ellas tendrán todas sus opuestas en la clase. Cualquier clase tendrá esta propiedad si contiene una forma ambigua y, recíprocamente, una forma ambigua se encuentra en cualquier clase que es opuesta a sí misma (art. 163, 165). Por esto le llamaremos *clase ambigua*. Así, entre las clases con determinante -235 se encuentran ocho clases ambiguas. Sus formas representantes son $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$; entre las clases de formas con determinante 79 se encuentran dos con representantes: $(1, 0, -79)$

y $(-1, 0, 79)$. Pero si las formas representadas han sido determinadas de acuerdo con nuestras reglas, las clases ambiguas se pueden determinar a partir de ellas sin ningún problema. Esto es, para un determinante positivo no cuadrado una clase ambigua ciertamente corresponde a una forma representante ambigua (art. 194); para un determinante negativo la forma representante de una clase ambigua será ella misma ambigua o bien sus términos exteriores serán iguales (art. 172); finalmente, para un determinante positivo cuadrado, por el artículo 210 es fácil deducir si la forma representante es impropiamente equivalente a sí misma y así si la clase a la cual representa es ambigua.

225.

Nosotros demostramos arriba (art. 175) que para una forma (a, b, c) con determinante negativo los términos exteriores deben poseer el mismo signo y que éste será el mismo signo que el de los términos exteriores de cualquier otra forma equivalente a ésta. Si a y c son positivos, podremos llamar *positiva* a la forma (a, b, c), y diremos que la clase entera en la cual (a, b, c) está contenida, y la cual está compuesta sólo por formas positivas, es una *clase positiva*. Al contrario (a, b, c) será una *forma negativa* contenida en una *clase negativa* si a y c son negativos. Un número negativo no puede representarse por una forma positiva, ni un número positivo lo puede ser por una forma negativa. Si (a, b, c) es la forma representante de una clase positiva, $(-a, b, -c)$ será la forma representante de una clase negativa. Así se sigue que el número de clases positivas es igual al número de clases negativas, y tan pronto como conozcamos una conoceremos la otra. Por lo tanto, al investigar formas con determinante negativo es muy a menudo suficiente considerar clases positivas, ya que sus propiedades pueden ser fácilmente transferidas a clases negativas.

Pero esta distinción se cumple sólo para formas con determinante negativo; números positivos y negativos pueden representarse igualmente por formas con determinante positivo, así no es raro encontrar en este caso las dos formas (a, b, c) y $(-a, b, -c)$ en la misma clase.

Distribución de clases en órdenes.

226.

Llamamos *primitiva* a la forma (a, b, c) si los números a, b, c no poseen divisores en común; en otro caso la llamaremos *derivada* y, claro está, si el máximo

común divisor de a, b, c es igual a m, la forma (a, b, c) será la forma *derivada de la forma primitiva* $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$. A partir de esta definición es obvio que cualquier forma cuyo determinante no es divisible por ningún cuadrado (excepto 1) es necesariamente primitiva. Además, por el artículo 161, si tenemos una forma primitiva en una clase arbitraria dada de formas con determinante D, todas las formas de esa clase serán primitivas; en este caso se dice que la clase misma es *primitiva*. Y es claro que, si cualquier forma F con determinante D se deriva de una forma primitiva f con determinante $\frac{D}{m^2}$, y si las clases en las cuales las formas F y f respectivamente están contenidas son K y k, todas las formas de la clase K serán formas derivadas de la clase primitiva k; en este caso diremos que la clase K es asimismo *derivada de la clase primitiva* k.

Si (a, b, c) es una forma primitiva y a y c no son ambos pares (i.e. o uno es impar o bien ambos son impares), entonces evidentemente no sólo a, b y c sino también a, $2b$ y c no poseen divisores comunes. En este caso la forma (a, b, c) se dice *propiamente primitiva* o simplemente una *forma propia*. Pero si (a, b, c) es una forma primitiva y los números a y c son ambos pares, obviamente los números a, $2b$ y c tendrán el divisor común 2 (este será también el máximo divisor) y (a, b, c) se llamará una *forma impropiamente primitiva* o simplemente una *forma impropia**). En este caso b será necesariamente impar (en otro caso (a, b, c) no sería una forma primitiva); por lo tanto tendremos $b^2 \equiv 1 \pmod 4$ y, como ac es divisible por 4, el determinante $b^2 - ac \equiv 1 \pmod 4$. Por lo que formas impropias corresponderán solamente a determinantes de la forma $4n + 1$ si son positivos o de la forma $-(4n+3)$ si son negativos. A partir del artículo 161 es obvio que si encontramos una forma propiamente primitiva en una clase dada, todas las formas de esta clase serán propiamente primitivas y que una clase que incluya una forma impropiamente primitiva estará compuesta solamente por formas impropiamente primitivas. Por ende, en el primer caso la clase se llamará *propiamente primitiva* o simplemente *propia*; y en el último caso *impropiamente primitiva* o *impropia*. Así, p. ej., entre las clases positivas de formas con determinante -235 existen seis propias con formas representantes $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$ y $(13, -5, 20)$ y el mismo número de negativas; y se encuentran dos clases impropias en cada una. Todas las clases de formas con determinante 79 (dado que ellas son de la forma $4n+3$) son propias.

---

*) Hemos escogido aquí los términos *propiamente* e *impropiamente* porque no hay otros más convenientes. Deseamos prevenir al lector de no buscar alguna conexión entre este caso y el del artículo 157 porque no existe ninguna. Pero ciertamente no se debería temer la ambigüedad.

Si la forma (a, b, c) se deriva de la forma primitiva $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$ esta última puede ser o propiamente o bien impropiamente primitiva. En el primer caso m será también el máximo común divisor de los números a, $2b$, c; en el último el máximo común divisor será $2m$. A partir de esto podemos hacer una clara distinción entre una *forma derivada de una forma propiamente primitiva* y una *forma derivada de una forma impropiamente primitiva*; y además (ya que por el art. 161 todas las formas de una misma clase son las mismas en ese sentido) entre una *clase derivada de una clase propiamente primitiva* y una *clase derivada de una clase impropiamente primitiva*.

Por medio de estas distinciones hemos obtenido el primer principio fundamental sobre el cual podemos construir la noción de distribución de todas las clases de formas con un determinante dado en varios *órdenes*. Dadas dos representaciones (a, b, c) y (a', b', c'), las agruparemos en el *mismo orden* siempre que los números a, b y c tengan el mismo máximo común divisor que a', b' y c', y, a, $2b$ y c posean el mismo máximo común divisor que a', $2b'$ y c'; si una u otra de esas condiciones falla, las clases serán asignadas a *órdenes diferentes*. Es claro de inmediato que todas las clases propiamente primitivas constituirán un orden; y todas las clases impropiamente primitivas otro. Si m^2 es un cuadrado que divide al determinante D, las clases derivadas de las clases propiamente primitivas del determinante $\frac{D}{m^2}$ formarán un orden especial, y las clases derivadas de clases impropiamente primitivas del determinante $\frac{D}{m^2}$ formarán otro, etc. Si D es divisible por un no cuadrado (excepto 1), no habrá órdenes de clases derivadas, y así habrá o solamente un orden (cuando $D \equiv 2$ o 3 según módulo 4) que es un orden de clases propiamente primitivas, o dos órdenes (cuando $D \equiv 1 \pmod 4$), esto es, un orden de clases propiamente primitivas y un orden de clases impropiamente primitivas. No es difícil establecer la siguiente regla general con la ayuda de los principios del cálculo de combinaciones. Suponemos que $D = D' 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \dots$ donde D' denota un factor no cuadrado y a, b, c, etc. son diferentes números primos impares (cualquier número puede reducirse a esta forma tomando $\mu = 0$ cuando D no es divisible por 4; y cuando D no es divisible por un cuadrado impar tomamos α, β, γ, etc. iguales a 0 o, lo que es la misma cosa, omitimos los factores $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$, etc.); así habrá o

$$(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

órdenes cuando $D' \equiv 2$ ó $3 \pmod 4$; o

$$(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

órdenes cuando $D' \equiv 1 \pmod 4$. Pero no demostraremos esta regla, dado que no es difícil ni es necesaria aquí.

Ejemplo. 1. Para $D = 45 = 5 \cdot 3^2$ tenemos seis clases con representantes $(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $(6, 3, -6)$. Estas se distribuyen en cuatro órdenes. El orden I incluye dos clases propias cuyas representantes son $(1, 0, 45)$ y $(-1, 0, 45)$; el orden II contendrá dos clases impropias cuyas representantes son $(2, 1, -22)$ y $(-2, 1, 22)$; el orden III contendrá una clase derivada de la clase propia del determinante 5, con representante $(3, 0, -15)$; el orden IV estará conformado por una clase derivada de una clase impropia del determinante 5 con representante $(6, 3, -6)$.

Ejemplo. 2. Las clases positivas del determinante $-99 = -11 \cdot 3^2$ se distribuirá en cuatro órdenes: el orden I incluirá las siguientes clases propiamente primitivas:*) $(1, 0, 99)$, $(4, 1, 25)$, $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; el orden II contendrá las clases impropias $(2, 1, 50)$, $(10, 1, 10)$; el orden III contendrá las clases derivadas de las clases propias del determinante -11, a saber $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; el orden IV, la clase derivada de las clases impropias del determinante -11, i.e., $(6, 3, 18)$. Clases negativas de este determinante pueden distribuirse en órdenes de exactamente la misma manera.

Observaremos que *clases opuestas son siempre asignadas al mismo orden.*

227.

De todos estos diferentes órdenes el orden de las clases propiamente primitivas merece especial atención. Para cada clase derivada obtenemos su origen de ciertas clases primitivas (con un determinante mínimo) y, considerando éstas, las propiedades de las clases se harán claras de inmediato. Mostraremos después que cualquier clase impropiamente primitiva se asocia o con una clase propiamente primitiva o con tres (con el mismo determinante). Además, para determinantes negativos, se puede omitir la consideración de clases negativas, dado que ellas siempre corresponderán a ciertas clases positivas. A fin de entender más plenamente la naturaleza de las clases propiamente primitivas, debemos primero explicar una cierta diferencia esencial según la cual el orden completo de clases propias puede subdividirse en varios *géneros.* Dado que todavía no hemos alcanzado este muy importante tema, lo trataremos desde el principio.

*) Usando, por brevedad, las formas representantes en lugar de sus clases.

La partición de órdenes en géneros.

228.

TEOREMA. *Existe una infinidad de números no divisibles por un número primo p dado, que pueden representarse por una forma propiamente primitiva.*

Demostración. Si la forma $F = ax^2 + 2bxy + cy^2$, es claro que p no puede ser divisor de los tres números a, $2b$, c. Ahora si a no es divisible por p, es claro que si elegimos un número no divisible por p para x , y para y un número que sea divisible por p, el valor de la forma F no será divisible por p; cuando c no es divisible por p ocurrirá lo mismo si damos a x un valor divisible por p y a y un valor que no sea divisible por p; finalmente, cuando ambos a y c son divisibles por p, y $2b$ no lo es, la forma F tendrá un valor no divisible por p si damos a ambos x y y valores que no sean divisibles por p. *Q. E. D.*

Es obvio que el teorema también es válido para formas que sean *impropiamente primitivas* mientras que no se tenga $p = 2$.

Dado que muchas condiciones de este tipo se pueden dar simultáneamente, tal como que el mismo número es divisible por ciertos números primos pero no por otros (véase art. 32), es fácil notar que los números x e y se pueden determinar de infinitas maneras, resultando que la forma primitiva $ax^2 + 2bxy + cy^2$ adquiera un valor que no es divisible por cualquier cantidad de números primos, excluyendo, sin embargo, el número 2 cuando la forma sea impropiamente primitiva. Así podemos proponer el teorema más generalmente: *Siempre se puede representar por medio de cualquier forma primitiva una infinidad de números que sean primos relativos a un número dado (el cual es impar cuando la forma es impropiamente primitiva).*

229.

TEOREMA. *Sea F una forma primitiva con determinante D y p un número primo que divide a D: entonces los números no divisibles por p que pueden representarse por la forma F son todos residuos cuadráticos de p o todos no residuos.*

Demostración. Sea $F = (a, b, c)$, y sean m y m' dos números cualesquiera no divisibles por p que pueden ser representados por la forma F; o sea

$$m = ag^2 + 2bgh + ch^2, \quad m' = ag'^2 + 2bg'h' + ch'^2$$

Entonces tendremos

$$mm' = [agg' + b(gh' + hg') + chh']^2 - D[gh' - hg']^2$$

y mm' será congruente a un cuadrado según el módulo D y así también según p; i.e., mm' será un residuo cuadrático de p. Se sigue por lo tanto que ambos m y m' son residuos cuadráticos de p, o que ambos no lo son. *Q. E. D.*

De la misma manera podemos demostrar que cuando el determinante D es divisible por 4, todos los números primos representables por F son o congruentes a 1 o congruentes a 3 (mod. 4). Esto es, el producto de dos de esos números siempre será un residuo cuadrático de 4 y por ende congruente a 1 (mod. 4); así ambos deben ser congruentes a 1 o ambos a 3.

Finalmente, cuando D es divisible por 8, el producto de dos números impares cualesquiera que pueden representarse por F será un residuo cuadrático de 8 y por tanto congruente a 1 (mod. 8). Así, en este caso los números impares representables por F serán todos congruentes a 1, o todos congruentes a 3, o todos congruentes a 5, o todos congruentes a 7 (mod. 8).

De este modo, p. ej., ya que el número 10 que es un no residuo de 7 se puede representar por la forma $(10, 3, 17)$, todos los números no divisibles por 7 que se pueden representar por esa forma serán no residuos de 7. Como -3 es representable por la forma $(-3, 1, 49)$ y es congruente a 1 (mod. 4), todos los números impares representables por esta forma serán congruentes a 1 (mod. 4).

Si fuese necesario para nuestros propósitos, podríamos demostrar fácilmente que los números representables por la forma F no guardan tal relación con números primos que no dividan a D. Ambos residuos y no residuos de un número primo que no divide a D se pueden representar igualmente por la forma F. Por el contrario, con respecto a los números 4 y 8 existe una cierta analogía, en otros casos también, que no podemos atrasar.

I. *Cuando el determinante D de la forma primitiva F es congruente a* 3 (mod. 4)*, todos los números impares representables por la forma F serán congruentes a* 1 *o todos congruentes a* 3 (mod. 4). En efecto, si m y m' son dos números representables por F, el producto mm' podrá reducirse a la forma $p^2 - Dq^2$ tal y como hicimos arriba. Cuando cada uno de los números m y m' es impar, uno de los números p o q es necesariamente par, y el otro impar, y por ende uno de los cuadrados p^2 o q^2 será congruente a 0 y el otro a 1 (mod. 4). Así $p^2 - Dq^2$ debe ser ciertamente congruente a 1 (mod. 4), y ambos m y m' deben ser congruentes a 1 o a 3 (mod. 4). Luego, p. ej., ningún número impar, más que aquéllos de la forma $4n + 1$, puede representarse por la forma $(10, 3, 17)$.

II. *Cuando el determinante D de la forma primitiva F es congruente a* 2 (mod. 8)*: todos los números impares representables por la forma F serán o*

congruentes en parte a 1 *y en parte a* 7*, o bien en parte a* 3 *y en parte a* 5 (mod. 8). En efecto, supongamos que m y m' son dos números impares representables por F cuyo producto mm' puede reducirse a la forma $p^2 - Dq^2$. Por lo que cuando ambos m y m' son impares, p debe ser impar (porque D es par) y así $p^2 \equiv 1 \pmod 8$; q^2 por lo tanto será congruente a 0, 1 o 4 y Dq^2 a 0 o a 2. Así $mm' = p^2 - Dq^2$ será congruente a 1 o a 7 (mod. 8); por eso, si m es congruente a 1 o a 7, m' será también congruente a 1 o a 7; y si m es congruente a 3 o a 5, m' será también congruente a 3 o a 5. Por ejemplo, todos los números impares representables por la forma $(3, 1, 5)$ son congruentes a 3 o a 5 (mod. 8), y ningún número de la forma $8n + 1$ u $8n + 7$ puede representarse por esta forma.

III. *Cuando el determinante D de una forma primitiva F es congruente a* 6 (mod. 8)*: los números impares que pueden representarse por esta forma son o todos congruentes a* 1 *y a* 3*, o todos congruentes a* 5 *y a* 7 (mod. 8). El lector puede desarrollar el argumento sin ningún problema. Es exactamente como el argumento anterior (II). Así, p. ej., para la forma $(5, 1, 7)$, solamente aquellos números impares que son congruentes a 5 o a 7 (mod. 8) pueden representarse.

230.

Por lo tanto todos los números que pueden representarse por una forma primitiva F dada con determinante D guardarán una estrecha relación con cada uno de los divisores primos de D (por el cual ellos no son divisibles). Y números impares que pueden representarse por la forma F guardarán también una estrecha relación con los números 4 y 8 en ciertos casos: a saber, con 4 siempre que D sea congruente a 0 o a 3 (mod. 4) y con 8 siempre que D sea congruente a 0, a 2 o a 6 (mod. 8)*). Llamaremos a este tipo de relación con cada uno de estos números el *carácter* o el *carácter particular* de la forma F, y expresaremos éste de la siguiente manera. Cuando solamente residuos cuadráticos de un número primo p pueden representarse por la forma F, asignaremos a ella el carácter Rp, en caso contrario asignaremos el carácter Np; similarmente escribiremos 1, 4 cuando ningún otro número puede representarse por la forma F excepto aquéllos que son congruentes a 1 (mod. 4). Es claro de inmediato cuáles caracteres se denotan por 3, 4; 1, 8; 3, 8; 5, 8 y 7, 8. Finalmente, si tenemos formas a través de las cuales solamente pueden representarse aquellos números impares que son congruentes a 1 o a 7 (mod. 8), les asignaremos a

*) Si el determinante es divisible por 8 se ignorará su relación con el número 4 pues en este caso ya se encuentra contenida en la relación con 8.

ellos el carácter 1 *y* 7, 8. Es obvio de inmediato que representamos por los caracteres 3 *y* 5, 8; 1 *y* 3, 8 ; 5 *y* 7, 8.

Los diferentes caracteres de una forma primitiva dada (a, b, c) con determinante D siempre se pueden conocer a partir de al menos uno de los números a o c (partiendo de que ambos son representables por tal forma). En efecto, siempre y cuando p sea un divisor primo de D, ciertamente uno de los números a o c, no será divisible por p; pues si ambos fueran divisibles por p, p dividiría también a b^2 $(= D+ac)$ y por lo tanto también a b; i.e. la forma (a, b, c) no sería primitiva. Similarmente, en aquellos casos en que la forma (a, b, c) posee una relación fija con el número 4 o el 8, al menos uno de los números a o c será impar, y podrá conocerse la relación de ese número. Así, p. ej., el carácter de la forma $(7, 0, 23)$ con respecto al número 23 puede inferirse a partir del número 7 como $N23$, y el carácter de la misma forma con respecto al número 7 puede deducirse a partir del número 23, a saber $R7$; finalmente, el carácter de esta forma con respecto al número 4, a saber 3, 4, puede hallarse a partir del número 7 o a partir del número 23.

Dado que todos los números que pueden representarse por una forma F contenida en una clase K son también representables por cualquier otra forma de la clase, queda manifiesto que los diferentes caracteres de la forma F se aplicarán a todas las demás formas de esta clase y por ende podemos considerar estos caracteres como representativos de toda la clase. Los caracteres individuales de una clase primitiva dada pueden entonces conocerse a partir de sus formas representantes. Clases opuestas poseerán siempre los mismos caracteres.

231.

El conjunto de *todos* los caracteres particulares de una clase o forma dada constituyen el carácter completo de esta forma o clase. Así, p. ej., el carácter completo de la forma $(10, 3, 17)$ o de la clase completa que ella representa será 1, 4; $N7$; $N23$. De manera análoga el carácter completo de la forma $(7, 1, -17)$ será 7, 8; $R3$; $N5$. Omitimos el carácter particular 3, 4 en este caso porque esta se halla contenida en el carácter 7, 8. A partir de estos resultados derivaremos una subdivisión del orden completo de clases propiamente primitivas (positivas cuando el determinante es negativo) de un determinante dado en muchos diferentes *géneros*, colocando todas las clases que poseen el mismo carácter completo en el mismo género, y en diferentes géneros aquéllos que poseen diferentes caracteres completos. Asignaremos a cada género aquéllos caracteres completos que poseen las clases contenidas en ellos. Así,

p. ej., para el determinante -161 tenemos 16 clases positivas propiamente primitivas que están distribuidas en 4 géneros de la siguiente manera:

Carácter	Formas representantes de las clases
1, 4; $R7$; $R23$	$(1,0,161)$, $(2,1,81)$, $(9,1,18)$, $(9,-1,18)$
1, 4; $N7$; $N23$	$(5,2,33)$, $(5,-2,33)$, $(10,3,17)$, $(10,-3,17)$
3, 4; $R7$; $N23$	$(7,0,23)$, $(11,2,15)$, $(11,-2,15)$, $(14,7,15)$
3, 4; $N7$; $R23$	$(3,1,54)$, $(3,-1,54)$, $(6,1,27)$, $(6,-1,27)$.

Se puede decir unas cuantas palabras con respecto a la cantidad de diferentes caracteres completos que son posibles *a priori*.

I. Cuando el determinante D es divisible por 8, con respecto al número 8 cuatro caracteres particulares son posibles; el número 4 no aportará ningún carácter en especial (véase el artículo precedente). Además, con respecto a cada divisor primo impar de D existirán dos caracteres; por lo tanto, si hay m de esos divisores, existirán en total 2^{m+2} diferentes caracteres completos (siendo $m = 0$ siempre que D sea potencia de 2).

II. Cuando el determinante D no es divisible por 8 pero sí es divisible por 4 y por m números primos impares, habrá en total 2^{m+1} caracteres completos diferentes.

III. Cuando el determinante es par y no divisible por 4, este será congruente a 2 o a 6 (mod. 8). En el primer caso existirán dos caracteres particulares con respecto al número 8, a saber 1 *y* 7, 8 y 3 *y* 5, 8; y el mismo número en el último caso. Por lo tanto, tomando el número de divisores primos impares de D igual a m, habrá en total 2^{m+1} caracteres completos diferentes.

IV. Cuando D es impar, será congruente a 1 o a 3 (mod. 4). En el segundo caso existirán dos diferentes caracteres con respecto al número 4, pero en el primer caso esta relación no formará parte del carácter completo. Así si definimos m como antes, en el primer caso existirán 2^m diferentes caracteres completos, en el último caso 2^{m+1}.

Pero hay que señalar bien que no se sigue *a priori* que siempre existirán tantos géneros como diferentes posibles caracteres. En nuestro ejemplo el número de clases o géneros es solamente la mitad de la cantidad posible. No existen clases positivas para los caracteres 1, 4; $R7$; $N23$ o 1, 4; $N7$; $R23$ o 3, 4; $R7$; $R23$ o 3, 4; $N7$; $N23$. Trataremos este importante tema plenamente más abajo.

A partir de ahora llamaremos a la forma $(1,0,-D)$, que es indudablemente la más simple de las formas con determinante D, la *forma principal*; y llamaremos a la clase completa en la cual ésta se encuentra la *clase principal*; y finalmente el género

completo en el cual se encuentra la clase principal se llamará *el género principal*. Por lo tanto, hay que distinguir claramente entre la forma principal, una forma de la clase principal, y una forma del género principal; y entre la clase principal y una clase del género principal. Siempre usaremos esta terminología, aún cuando quizás para un determinante en particular no exista otra clase más que la clase principal o ningún otro género más que el género principal. Esto sucede muy a menudo, p. ej., cuando D es un número primo positivo de la forma $4n + 1$.

232.

Aún cuando todo lo que se ha explicado sobre los caracteres de las formas fue con el propósito de encontrar una subdivisión para todo el orden de *clases positivas propiamente primitivas*, nada nos impide ir más lejos. Podemos aplicar las mismas reglas a formas y clases negativas o impropriamente primitivas, y bajo el mismo principio podemos subdividir en géneros tanto un orden positivo impropiamente primitivo, como un orden negativo propiamente primitivo, como un orden negativo impropiamente primitivo. Así pues, por ejemplo, después de que se ha subdividido el orden propiamente primitivo de formas de determinante 145 en los dos siguientes géneros:

$R5$, $R29$	$(1, 0, -145)$, $(5, 0, -29)$
$N5$, $N29$	$(3, 1, -48)$, $(3 - 1, -48)$

el orden impropiamente primitivo puede también ser subdividido en dos géneros:

$R5$, $R29$	$(4, 1, -36)$, $(4, -1, -36)$
$N5$, $N29$	$(2, 1, -72)$, $(10, 5, -12)$

o, tal como las clases positivas de las formas de determinante -129 se distribuyen en cuatro géneros:

1, 4; $R3$; $R43$	$(1, 0, 129)$, $(10, 1, 13)$, $(10, -1, 13)$
1, 4; $N3$; $N43$	$(2, 1, 65)$, $(5, 1, 26)$, $(5, -1, 26)$
3, 4; $R3$; $N43$	$(3, 0, 43)$, $(7, 2, 19)$, $(7, -2, 19)$
3, 4; $N3$; $R43$	$(6, 3, 23)$, $(11, 5, 14)$, $(11, -5, 14)$

las clases negativas también se pueden distribuir en cuatro órdenes:

3, 4; $N3$; $N43$	$(-1,0,-129)$, $(-10,1,-13)$, $(-10,-1,-13)$
3, 4; $R3$; $R43$	$(-2,1,-65)$, $(-5,1,-26)$, $(-5,-1,-26)$
1, 4; $N3$; $R43$	$(-3,0,-43)$, $(-7,2,-19)$, $(-7,-2,-19)$
1, 4; $R3$; $N43$	$(-6,3,-23)$, $(-11,5,-14)$, $(-11,-5,-14)$

Sin embargo, puesto que el sistema de clases negativas es siempre muy similar al sistema de clases positivas, resulta superfluo construirlo por aparte. Mostraremos luego cómo reducir un orden impropiamente primitivo a uno propiamente primitivo.

Finalmente, en cuanto a la subdivisión de órdenes obtenidos a partir de otros, no son necesarias reglas nuevas. Es así puesto que cualquiera de estos órdenes tiene origen en algún orden primitivo (con un determinante menor), y las clases de uno pueden relacionarse de manera natural con las clases del otro, y entonces es claro que la subdivisión de una de estas formas puede obtenerse a partir de la subdivisión de un orden primitivo.

233.

Si la forma (primitiva) $F = (a,b,c)$ es tal que se puede encontrar dos enteros g y h, tales que $g^2 \equiv a$, $gh \equiv b$, $h^2 \equiv c$ con respecto a un módulo dado m, diremos que la forma es un residuo cuadrático del número m, y que $gx + hy$ es un valor de la expresión $\sqrt{ax^2 + 2bxy + cy^2} \pmod{m}$ o simplemente que (g,h) es un valor de la expresión $\sqrt{(a,b,c)}$ o $\sqrt{F} \pmod{m}$. De manera más general, si el multiplicador M, primo relativo al módulo m es tal que tenemos

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m}$$

diremos que $M \cdot (a,b,c)$ o MF es un residuo cuadrático de m y que (g,h) es el valor de la expresión $\sqrt{M(a,b,c)}$ o $\sqrt{MF} \pmod{m}$. Por ejemplo, la forma $(3,1,54)$ es un residuo cuadrático de 23 y $(7,10)$ un valor de la expresión $\sqrt{(3,1,54)} \pmod{23}$; similarmente $(2,-4)$ es un valor de la expresión $\sqrt{5(10,3,17)} \pmod{23}$. El uso de estas definiciones se demostrará después. Anotaremos las siguientes proposiciones:

I. Si $M(a,b,c)$ es un residuo cuadrático del número m, m será un divisor del determinante de la forma (a,b,c). Pues si (g,h) es un valor de la expresión $\sqrt{M(a,b,c)} \pmod{m}$ es decir, si

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m}$$

tendremos $b^2M^2 - acM^2 \equiv 0$ o sea $(b^2 - ac)M^2$ es divisible por m. Pero, puesto que hemos supuesto que M y m son primos relativos, $b^2 - ac$ será divisible por m.

II. Si $M(a, b, c)$ es un residuo cuadrático de m, donde m es un número primo o una potencia p^μ de un número primo, el carácter particular de la forma (a, b, c) con respecto al número p será Rp o Np según M sea un residuo o no residuo de p. Esto se sigue inmediatamente del hecho de que ambos aM y cM son residuos de m o p, y que al menos uno de los números a y c no es divisible por p (art. 230).

Similarmente, si (con todo lo demás igual) $m = 4$, entonces 1, 4 ó 3, 4 será un carácter particular de la forma (a, b, c) según $M \equiv 1$ ó $M \equiv 3$; y si $m = 8$ o una potencia mayor del número 2, entonces, 1, 8; 3, 8; 5, 8; 7, 8 serán caracteres particulares de la forma (a, b, c) según $M \equiv 1;\ 3;\ 5;\ 7 \pmod 8$ respectivamente.

III. En cambio, suponga que m es un número primo o una potencia p^μ de un número primo impar y que es divisor del determinante $b^2 - ac$. Si M es un residuo o no de p según el carácter de la forma (a, b, c) respecto a p sea Rp o Np respectivamente, entonces $M(a, b, c)$ será un residuo cuadrático de m. Pues cuando a no es divisible por p, aM será un residuo de p y así también de m; por lo tanto, si g es un valor de la expresión $\sqrt{aM} \pmod m$, h un valor de la expresión $\frac{bg}{a} \pmod m$, tendremos $g^2 \equiv aM$, $ah \equiv bg$. Entonces

$$agh \equiv bg^2 \equiv abM \qquad \text{y} \quad gh \equiv bM$$

y finalmente

$$ah^2 \equiv bgh \equiv b^2M \equiv b^2M - (b^2 - ac)M \equiv acM$$

Así $h^2 \equiv cM$; i.e. (g, h) es un valor de la expresión $\sqrt{M(a, b, c)}$. Cuando a es divisible por m es de seguro que c no lo será. Entonces obviamente obtendremos el mismo resultado si h asume un valor de la expresión $\sqrt{cM} \pmod m$ y g un valor de la expresión $\frac{bh}{c} \pmod m$.

De manera similar se puede mostrar que si $m = 4$ y es divisor de $b^2 - ac$, y si el número M se toma $\equiv 1$ ó $\equiv 3$ según 1, 4 ó 3, 4 sea un carácter particular de la forma (a, b, c), entonces, $M(a, b, c)$ será un residuo cuadrático de m. Además, si $m = 8$ ó una potencia mayor de 2 y divisor de $b^2 - ac$, y si $M \equiv 1;\ 3;\ 5;\ 7 \pmod 8$ según el carácter particular de la forma (a, b, c) respecto al número 8; entonces $M(a, b, c)$ será un residuo cuadrático de m.

IV. Si el determinante de la forma (a, b, c) es $= D$ y $M(a, b, c)$ es un residuo cuadrático de D, a partir del número M pueden conocerse inmediatamente todos los caracteres particulares de la forma (a, b, c) respecto a cada uno de los divisores

primos impares de D y respecto al número 4 u 8 (si dividen a D). Entonces, por ejemplo, puesto que $3(20, 10, 27)$ es un residuo cuadrático de 440, es decir, que $(150, 9)$ es un valor de la expresión $\sqrt{3(20, 10, 27)}$ respecto al módulo 440 y $3N5$, $3R11$, los caracteres de la forma $(20, 10, 27)$ son 3, 8; $N5$; $R11$. Los caracteres particulares con respecto a los números 4 y 8, siempre que no sean divisores del determinante, son los únicos que no tienen una conexión necesaria con el número M.

V. En cambio, si el número M es primo relativo a D y contiene todos los caracteres particulares de la forma (a, b, c) (excepto por aquéllos respecto a los números 4 y 8 cuando no son divisores de D), entonces $M(a, b, c)$ será un residuo cuadrático de D. Pues, a partir de III es claro que si D se reduce a la forma $\pm A^\alpha B^\beta C^\gamma \ldots$ donde A, B, C, etc. son números primos distintos, $M(a, b, c)$ será un residuo cuadrático de cada uno de los A^α, B^β, C^γ, etc. Ahora supongamos que el valor de la expresión $\sqrt{M(a, b, c)}$ respecto al módulo A^α es $(\mathfrak{A}, \mathfrak{A}')$; respecto al módulo B^β es $(\mathfrak{B}, \mathfrak{B}')$; respecto al módulo C^γ es $(\mathfrak{C}, \mathfrak{C}')$ etc. Si los números g y h se determinan tales que $g \equiv \mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc; $h \equiv \mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ etc. respecto a los módulos A^α, B^β, C^γ, etc. respectivamente (art. 32): es fácil ver que tendremos $g^2 \equiv aM$, $gh \equiv bM$, $h^2 \equiv cM$ respecto a cada uno de los módulos A^α, B^β, C^γ, etc. y, por lo tanto, también respecto al módulo D, que es su producto.

VI. Por esta razón números como M se llamarán *números característicos* de la forma (a, b, c). Muchos de estos números pueden encontrarse fácilmente mediante los métodos de V, una vez que se conocen todos los caracteres particulares de la forma. Los más sencillos se encontrarán por tanteo. Claramente, si M es un número característico de una forma primitiva de determinante D dado, todos los números congruentes a M respecto al módulo D serán números característicos de la misma forma. También es claro que formas de la misma clase o de diferentes clases del mismo género tienen los mismos números característicos. Como consecuencia, cualquier número característico de una forma dada también se puede asignar a toda la clase y a todo el género. Finalmente, 1 es siempre un número característico de cualquier forma, clase o género principal; es decir, toda forma de un género principal es un residuo de su determinante.

VII. Si (g, h) es un valor de la expresión $\sqrt{M(a, b, c)}$ (mod. m) y $g' \equiv g$ y $h' \equiv h$ (mod. m), entonces (g', h') también será un valor de la misma expresión. Tales valores se denominarán *equivalentes*. Sin embargo, si (g, h) y (g', h') son valores de la expresión $\sqrt{M(a, b, c)}$, pero no se cumple que $g' \equiv g$, $h' \equiv h$ (mod. m), se denominarán *diferentes*. Es claro que siempre que (g, h) sea un valor de una expresión como la anterior, $(-g, -h)$ también será un valor, y estos valores

siempre serán diferentes excepto cuando $m = 2$. También es fácil mostrar que una expresión $\sqrt{M(a,b,c)}$ (mod. m) no puede tener más que dos valores diferentes opuestos cuando m es un número primo impar, una potencia de un número primo impar ó $= 4$; sin embargo, cuando $m = 8$ ó una potencia mayor de 2, habrá cuatro en total. Entonces, a partir de VI vemos fácilmente que si el determinante D de la forma (a,b,c) es $= \pm 2^{\mu} A^{\alpha} B^{\beta} \ldots$ donde A, B, etc. son n números primos impares diferentes en total, y M es un número característico de la forma; entonces habrá, en total, 2^n ó 2^{n+1} ó 2^{n+2} valores diferentes de la expresión $\sqrt{M(a,b,c)}$ (mod. D) según μ sea < 2 ó $= 2$ ó > 2. Entonces, por ejemplo, hay 16 valores de la expresión $\sqrt{7(12,6,-17)}$ (mod. 240), a saber $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Para abreviar, y puesto que no es particularmente importante para lo que sigue, omitiremos una demostración más detallada.

VIII. Finalmente observamos que si el determinante de dos formas equivalentes (a,b,c) y (a',b',c') es D, el número característico es M y la primera se puede transformar en la segunda mediante la sustitución α, β, γ, δ; entonces, a partir de cualquier valor (g,h) de la expresión $\sqrt{M(a,b,c)}$ se obtiene un valor (g',h') de la expresión $\sqrt{M(a',b',c')}$, a saber $(\alpha g + \gamma h, \beta g + \delta h)$. El lector puede demostrar esto fácilmente.

Sobre la composición de formas.

234.

Ahora que hemos explicado la distribución de formas entre clases, géneros y órdenes, y las propiedades generales que resultan de estas distinciones, pasaremos a otro tema muy importante, la *composición* de formas. Hasta el momento, nadie ha considerado este punto. Antes de iniciar la discusión enunciaremos el siguiente lema para no interrumpir, más adelante, la continuidad de nuestra demostración.

LEMA: *Suponga que tenemos cuatro series de enteros.*

$$a,\ a',\ a'',\ \ldots a^n; \quad b,\ b',\ b'',\ \ldots b^n; \quad c,\ c',\ c'',\ \ldots c^n; \quad d,\ d',\ d'',\ \ldots d^n$$

donde cada serie tiene el mismo número $(n+1)$ *de términos y están ordenados tal que*

$$cd' - dc', \quad cd'' - dc'' \text{ etc.}, \quad c'd'' - d'c'' \text{ etc., etc.}$$

son respectivamente

$$= k(ab' - ba'), \quad k(ab'' - ba'') \text{ etc.}, \quad k(a'b'' - b'a'') \text{ etc., etc.}$$

o en general

$$c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$$

*Aquí k es un entero dado; λ y μ son dos enteros distintos cualesquiera entre 0 y n inclusive, con μ el mayor de los dos**). Además, no debe haber un divisor común entre todos los $a^\lambda b^\mu - b^\lambda a^\mu$. Bajo estas condiciones, se pueden encontrar cuatro enteros α, β, γ y δ tales que

$$\begin{aligned} \alpha a + \beta b = c, \quad \alpha a' + \beta b' = c', \quad \alpha a'' + \beta b'' = c'' \text{ etc.} \\ \gamma a + \delta b = d, \quad \gamma a' + \delta b' = d', \quad \gamma a'' + \delta b'' = d'' \text{ etc.} \end{aligned}$$

o en general

$$\alpha a^\nu + \beta b^\nu = c^\nu, \quad \gamma a^\nu + \delta b^\nu = d^\nu$$

y tenemos

$$\alpha\delta - \beta\gamma = k$$

Puesto que por hipótesis los números $ab' - ba'$, $ab'' - ba''$, etc. $a'b'' - b'a''$ etc. (el número de ellos será $= \frac{1}{2}(n+1)n$) no tienen un divisor común, podemos encontrar la misma cantidad de enteros (diferentes) tal que si multiplicamos el primer conjunto por el segundo respectivamente, la suma de los productos será $= 1$ (art. 40). Designaremos estos multiplicadores por $(0,1)$, $(0,2)$ etc., $(1,2)$ etc. o en general el multiplicador de $a^\lambda b^\mu - b^\lambda a^\mu$ por (λ, μ) y

$$\sum(\lambda,\ \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1$$

(Mediante la letra $\sum$ indicamos la suma de todos los valores de la expresión cuando le damos sucesivamente a λ y a μ, todos los valores diferentes entre 0 y n y tal que $\mu > \lambda$). Ahora si se pone

$$\begin{aligned} \sum(\lambda,\mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha, \quad \sum(\lambda,\mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta \\ \sum(\lambda,\mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma, \quad \sum(\lambda,\mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta \end{aligned}$$

estos números α, β, γ y δ tienen las propiedades deseadas.

---

*) Tomando a como a^0, b como b^0 etc. Pero es claro que la misma ecuación es válida cuando $\lambda = \mu$ ó $\lambda > \mu$.

Demostración. I. Si ν es cualquier entero entre 0 y n, tenemos

$$\begin{aligned}\alpha a^\nu + \beta b^\nu &= \sum (\lambda,\mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu)\\ &= \frac{1}{k}\sum (\lambda,\mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu)\\ &= \frac{1}{k}c^\nu \sum (\lambda,\mu)(c^\lambda d^\mu - d^\lambda c^\mu)\\ &= c^\nu \sum (\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu\end{aligned}$$

Y mediante un cálculo similar se demuestra

$$\gamma a^\nu + \delta b^\nu = d^\nu. \quad Q.\ E.\ P.$$

II. Entonces, puesto que

$$c^\lambda = \alpha a^\lambda + \beta b^\lambda, \qquad c^\mu = \alpha a^\mu + \beta b^\mu$$

se tiene

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$$

y similarmente

$$\begin{aligned}a^\lambda c^\mu - c^\lambda a^\mu &= \beta(a^\lambda b^\mu - b^\lambda a^\mu)\\ d^\lambda b^\mu - b^\lambda d^\mu &= \gamma(a^\lambda b^\mu - b^\lambda a^\mu)\\ a^\lambda d^\mu - d^\lambda a^\mu &= \delta(a^\lambda b^\mu - b^\lambda a^\mu)\end{aligned}$$

A partir de estas fórmulas pueden obtenerse los valores de α, β, γ y δ mucho más fácilmente, siempre y cuando λ y μ sean escogidos tales que $a^\lambda b^\mu - b^\lambda a^\mu$ no sea 0. Esto de seguro se puede lograr, ya que por hipótesis no hay un divisor común de todos los $a^\lambda b^\mu - b^\lambda a^\mu$ y por lo tanto todos no pueden ser 0. A partir de estas mismas ecuaciones, si multiplicamos la primera por la cuarta, la segunda por la tercera y restamos, obtenemos

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$$

y necesariamente entonces

$$\alpha\delta - \beta\gamma = k. \quad Q.\ E.\ S.$$