167.

TEOREMA. *Si las formas*

$$ax^2 + 2bxy + cy^2 \qquad (F)$$
$$a'x'^2 + 2b'x'y' + c'y'^2 \qquad (F')$$

son equivalentes, el determinante de ellas $= D$*, y la última se transforma en la primera al poner*

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y$$

y si además el número M *se representa por* F*, escribiendo* $x = m$*,* $y = n$*, y, por lo tanto, por* F' *haciendo*

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n'$$

de modo que m *sea primo a* n *y por tanto también* m' *a* n'*, entonces ambas representaciones pertenecerán o al mismo valor de la expresión* $\sqrt{D} \pmod{M}$ *o a valores opuestos según que la transformación de la forma* F' *en* F *sea propia o impropia.*

Demostración. Se determinarán los números μ y ν de manera que resulte $\mu m + \nu n = 1$ y póngase

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

(los cuales serán enteros pues $\alpha\delta - \beta\gamma = \pm 1$). Entonces tendremos

$$\mu' m' + \nu' n' = 1. \quad \text{(cf. final del artículo anterior)}$$

Además sea

$$\mu(bm + cn) - \nu(am + bn) = V, \quad \mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$$

y V y V' serán valores de la expresión $\sqrt{D} \pmod{M}$ a los cuales pertenecen la primera y la segunda representaciones. Si en V' para μ', ν', m', n' se sustituyen los valores de ellos, pero en V

$$\begin{aligned} &\text{para } a, && a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2 \\ &\text{para } b, && a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta \\ &\text{para } c, && a'\beta^2 + 2b'\beta\delta + c'\delta^2 \end{aligned}$$

se encontrará por cálculo que $V = V'(\alpha\delta - \beta\gamma)$.

Por esto tendremos o bien $V = V'$ o $V = -V'$ según que $\alpha\delta - \beta\gamma = +1$ o $= -1$, i.e., las representaciones pertenecerán al mismo valor de la expresión $\sqrt{D}$ (mod. M) o a los valores opuestos, según que la transformación de F' en F sea propia o impropia. *Q. E. D.*

Si de esta manera se tienen varias representaciones del número M por la forma (a, b, c) por medio de valores primos entre sí de las indeterminadas pertenecientes a valores *diferentes* de la expresión $\sqrt{D}$ (mod. M), entonces las representaciones correspondientes por la forma (a', b', c') pertenecerán a los mismos valores respectivos. Si no existe representación alguna del número M por ninguna forma perteneciente a un cierto valor del determinante, tampoco existirá ninguna otra perteneciente a este valor y equivalente a él.

168.

Teorema. *Si el número M se representa por la forma $ax^2 + 2bxy + cy^2$, asignando los valores m y n primos entre sí a x e y, y si el valor de la expresión $\sqrt{D}$* (mod. M)*, al cual pertenece esta representación, es N, entonces las formas (a, b, c) y $(M, N, \frac{N^2-D}{M})$ serán propiamente equivalentes.*

Demostración. Es claro que, por el artículo 155, pueden encontrarse números enteros μ y ν de modo que

$$m\mu + n\nu = 1, \quad \mu(bm + cn) - \nu(am + bn) = N.$$

Usando esto, la forma (a, b, c) se transforma mediante la sustitución $x = mx' - \nu y'$ e $y = nx' + \mu y'$, la cual claramente es propia, en una forma cuyo determinante es $= D(m\mu + n\nu)^2$, i.e., $= D$, o en una forma equivalente. Tal forma, si se pone $= (M', N', \frac{N'^2-D}{M'})$, será,

$$M' = am^2 + 2bmn + cn^2 = M, \quad N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N.$$

Por lo que la forma en la cual se transforma (a, b, c) por esta transformación será $(M, N, \frac{N^2-D}{M})$. *Q. E. D.*

Además, de las ecuaciones

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

se deduce

$$\mu = \frac{nN + ma + nb}{am^2 + 2bmn + cn^2} = \frac{nN + ma + nb}{M}, \quad \nu = \frac{mb + nc - mN}{M}$$

las cuales serán, por lo tanto, números enteros.

Además, hay que notar que esta proposición no vale si $M = 0$; pues el término $\frac{N^2 - D}{M}$ será indeterminado*).

169.

Si se tienen varias representaciones del número M por (a, b, c) pertenecientes al mismo valor N de la expresión $\sqrt{D} \pmod{M}$ (donde siempre suponemos que los valores de x e y son primos entre sí), también se deducirán varias transformaciones propias de la forma $(a, b, c) \ldots (F)$ en $(M, N, \frac{N^2 - D}{M}) \ldots (G)$. De hecho, si tal representación proviene de los valores $x = m'$ e $y = n'$, (F) también se transforma en (G) por la sustitución

$$x = m'x' + \frac{m'N - m'b - n'c}{M}y', \quad y = n'x' + \frac{n'N + m'a + n'b}{M}y'.$$

Viceversa, de cada transformación propia de la forma (F) en (G), se deriva una representación del número M por la forma (F) perteneciente al valor N. Si (F) se transforma en (G), al poner $x = mx' - \nu y'$ e $y = nx' + \mu y'$, entonces M se representa por (F) al poner $x = m$ e $y = n$, y puesto que aquí $m\mu + n\nu = 1$, el valor de la expresión $\sqrt{D} \pmod{M}$, al cual pertenece la representación, será $\mu(bm + cn) - \nu(am + bn)$, i.e., N. De varias transformaciones propias y diferentes resulta el mismo número de representaciones diversas pertenecientes a N†). De esto

*) De hecho, si deseamos extender la terminología a este caso, podemos decir que si N es el valor de la expresión $\sqrt{D} \pmod{M}$, o sea $N^2 \equiv D \pmod{M}$, significará que $N^2 - D$ es un múltiplo de M, y por lo tanto $= 0$.

†) Si se supone que la misma representación proviene de dos transformaciones propias diferentes, ellas tendrán que ser:

$$1)\, x = mx' - \nu y', \quad y = nx' + \mu y'; \qquad 2)\, x = mx' - \nu' y', \quad y = nx' + \mu' y'$$

Sin embargo, de las dos ecuaciones

$$m\mu + n\nu = m\mu' + n\nu', \quad \mu(mb + nc) - \nu(ma + nb) = \mu'(mb + nc) - \nu'(ma + nb)$$

se deduce fácilmente que o bien $M = 0$ o bien $\mu = \mu'$, $\nu = \nu'$. Pero ya hemos excluído a $M = 0$.

se concluye fácilmente que, si se tuvieran todas las transformaciones propias de la forma (F) en la (G), resultarán de éstas todas las representaciones de M por (F) pertenecientes al valor N. De donde, la cuestión de investigar las representaciones de un número dado por una forma dada (en la cual se dan valores primos entre sí a las indeterminadas) se reduce a la cuestión de investigar todas las transformaciones propias de esta forma en la forma equivalente dada.

Ahora, aplicando a ésta lo que aprendimos en el artículo 162, se colige con facilidad que si la representación de algún número M por la forma (F) perteneciente al valor N es ésta $x = \alpha$ e $y = \gamma$; la fórmula general que comprende todas las representaciones del mismo número por la forma (F) perteneciente al valor N será:

$$x = \frac{\alpha t - (\alpha b + \gamma c)u}{m}, \quad y = \frac{\gamma t + (\alpha a + \gamma b)u}{m}$$

donde m es el máximo común divisor de los números a, $2b$, c, y t y u representan todos los números que satisfacen la ecuación $t^2 - Du^2 = m^2$.

170.

Si la forma (a, b, c) es equivalente a alguna forma ambigua y por lo tanto equivalente a la forma $(M, N, \frac{N^2-D}{M})$, tanto propia como impropiamente, o propiamente equivalente a las formas $(M, N, \frac{N^2-D}{M})$ y $(M, -N, \frac{N^2-D}{M})$, se tendrán las representaciones del número M por la forma (F) perteneciente tanto al valor N como al valor $-N$. Y recíprocamente, si se tienen varias representaciones del número M por la misma forma (F) pertenecientes a valores *opuestos* N y $-N$ de la expresión $\sqrt{D}$ (mod. M), la forma (F) será equivalente a la forma (G) tanto propia como impropiamente y podrá encontrarse una forma ambigua a la cual sea equivalente (F).

Estas generalidades sobre las representaciones son suficientes por ahora. Hablaremos más adelante sobre las representaciones en las cuales las indeterminadas tienen valores no primos entre sí. En lo que atañe a las otras propiedades, las formas cuyo determinante es negativo deben ser tratadas de modo totalmente diferente que las formas de determinante positivo; por lo tanto consideraremos ahora las dos por separado. Así, comenzamos con las más fáciles.

Sobre las formas de un determinante negativo.

171.

PROBLEMA. *Dada una forma cualquiera (a, b, a'), cuyo determinante nega-*

tivo $= -D$*, donde* D *es un número positivo, se debe encontrar una forma* (A, B, C) *propiamente equivalente a ésta, en la cual* A *no es mayor que* $\sqrt{\frac{4}{3}D}$*, ni mayor que* C*, ni menor que* $2B$*.*

Resolución. Suponemos que en la forma dada no valen a la vez las tres condiciones; de lo contrario no sería necesario buscar otra forma. Sea b' el menor residuo absoluto del número $-b$ según el módulo a'*), y $a'' = \frac{b'^2+D}{a'}$, el cual será un entero; ya que $b'^2 \equiv b^2$, $b'^2 + D \equiv b^2 + D \equiv aa' \equiv 0 \pmod{a'}$. Si $a'' < a'$, resulta de nuevo que b'' es el menor residuo absoluto de $-b'$, según el módulo a'', y $a''' = \frac{b''^2+D}{a''}$. Si de nuevo $a''' < a''$ sea de nuevo b''' el menor residuo absoluto de $-b''$ según el módulo a''', y sea $a'''' = \frac{b'''^2+D}{a'''}$. Esta operación continuará, hasta llegar en la progresión a', a'', a''', a'''' etc., a un término $a^{(m+1)}$, el cual no es menor que su antecedente $a^{(m)}$. Esto debe ocurrir finalmente, ya que se tendría una progresión infinita de números enteros decrecientes. Entonces la forma $(a^{(m)}, b^{(m)}, a^{(m+1)})$ satisfará todas las condiciones.

Demostración. I. En la progresión de formas (a, b, a'), (a', b', a''), (a'', b'', a''') etc., cada una es contigua a su antecedente; por lo cual la última será propiamente equivalente a la primera (artículos 159 y 160).

II. Como $b^{(m)}$ es el residuo menor absoluto de $-b^{(m-1)}$, según el módulo $a^{(m)}$, no será mayor que $\frac{1}{2}a^{(m)}$ (art. 4).

III. Ya que $a^{(m)}a^{(m+1)} = D + b^{(m)}b^{(m)}$ y $a^{(m+1)}$ no es $< a^{(m)}$, tampoco será $a^{(m)}a^{(m)} > D + b^{(m)}b^{(m)}$ y como $b^{(m)}$ no es $> \frac{1}{2}a^{(m)}$, tampoco será $> D + \frac{1}{4}a^{(m)}a^{(m)}$ y $\frac{3}{4}a^{(m)}a^{(m)}$ no será $> D$ y finalmente $a^{(m)}$ no $> \sqrt{\frac{4}{3}D}$.

Ejemplo. Dada la forma (304, 217, 155) cuyo determinante $= -31$, se encuentra la progresión de las formas:

$$(304, 217, 155), \quad (155, -62, 25), \quad (25, 12, 7), \quad (7, 2, 5), \quad (5, -2, 7)$$

La última es la buscada. Del mismo modo, para la forma $(121, 49, 20)$ cuyo determinante $= -19$, se encuentran las equivalentes $(20, -9, 5)$, $(5, -1, 4)$, $(4, 1, 5)$: por lo que $(4, 1, 5)$ será la forma buscada.

---

*) Conviene observar que, si el primer o el último término a ó a' de alguna forma dada (a, b, a') fuera $= 0$, su determinante sería un cuadrado positivo; por lo cual esto no puede ocurrir en este caso. Por la misma razón no pueden existir signos opuestos de los términos de ambos lados a y a' para la forma de un determinante negativo.

Llamaremos *formas reducidas* a tales formas (A, B, C) cuyo determinante es negativo y en las cuales A ni es mayor que $\sqrt{\frac{4}{3}D}$, ni mayor que C, ni menor que $2B$. Por lo que para cada forma de un determinante negativo podremos encontrar una forma reducida propiamente equivalente a ella.

172.

PROBLEMA. *Encontrar las condiciones bajo las cuales dos formas reducidas no idénticas* (a, b, c) *y* (a', b', c') *con el mismo determinante,* $-D$*, puedan ser propiamente equivalentes.*

Resolución. Supongamos, lo cual es posible, que a' no es $> a$, y que la forma $ax^2 + 2bxy + cy^2$ se transforma en $a'x'^2 + 2b'x'y' + c'y'^2$ por la sustitución propia $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Entonces se tendrán las siguientes ecuaciones

$$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a' \tag{1}$$

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b' \tag{2}$$

$$\alpha\delta - \beta\gamma = 1 \tag{3}$$

De la (1) resulta $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$; por lo cual aa' será positivo; y como $ac = D + b^2$, $a'c' = D + b'^2$, también serán positivos ac y $a'c'$; por lo tanto todos a, a', c, c' tendrán el mismo signo. Pero, ni a ni a' es $> \sqrt{\frac{4}{3}D}$ y, por tanto, tampoco aa' es $> \frac{4}{3}D$; por lo cual mucho menos puede ser $D\gamma^2 (= aa' - (a\alpha + b\gamma)^2)$ mayor que $\frac{4}{3}D$. De esto, γ será o $= 0$, o $= \pm 1$.

I. Si $\gamma = 0$, se deduce de la (3) que o bien son $\alpha = 1, \delta = 1$, o $\alpha = -1, \delta = -1$. En ambos casos, resulta de la (1) que $a' = a$, y de la (2) que $b' - b = \pm\beta a$. Pero, b no es $> \frac{1}{2}a$ ni $b' > \frac{1}{2}a'$ y tampoco $> \frac{1}{2}a$. Por consiguiente, la ecuación $b' - b = \pm\beta a$ no puede darse, a no ser que sea

o bien $b = b'$, de donde resultaría $c' = \frac{b'^2 + D}{a'} = \frac{b^2 + D}{a} = c$; por lo que las formas (a, b, c), (a', b', c') serían idénticas (contrariamente a la hipótesis),

o bien $b = -b' = \pm\frac{1}{2}a$. En este caso, también sería $c' = c$ y la forma (a', b', c') sería $(a, -b, c)$, i.e., la forma opuesta a (a, b, c). Al mismo tiempo, es evidente que estas formas serían ambiguas ya que $2b = \pm a$.

II. Si $\gamma = \pm 1$, de la (1) resulta $a\alpha^2 + c - a' = \pm 2b\alpha$. Pero c no es menor que a, y por lo tanto no menor que a'; de esto $a\alpha^2 + c - a'$, ó sea $2b\alpha$ no es menor que $a\alpha^2$. Por lo que, como $2b$ no es mayor que a, tampoco α será menor que α^2; de donde necesariamente $\alpha = 0$, ó $= \pm 1$.

1) Si $\alpha = 0$, de la (1) tenemos $a' = c$, y puesto que a ni es mayor que c, ni menor que a', será necesariamente $a' = a = c$. Además de la (3) tenemos que $\beta\gamma = -1$ de donde de la (2) $b + b' = \pm\delta c = \pm\delta a$. De modo semejante a como se dedujo de la (I) tendremos:

o bien $b = b'$, en tal caso las formas serían idénticas (contrariamente a la hipótesis),

o bien $b = -b'$, en tal caso las formas (a, b, c), (a', b', c') serían opuestas.

2) Si $\alpha = \pm 1$, resulta de la (1) que $\pm 2b = a + c - a'$. Por lo tanto como ni a ni $c < a'$, tampoco sería $2b < a$ ni $< c$. Pero, $2b$ ni es $> a$, ni $> c$, de donde necesariamente $\pm 2b = a = c$, y de la ecuación $\pm 2b = a + c - a'$ será también $= a'$. Por lo tanto de la (2) resulta que

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

o, puesto que $\alpha\delta - \beta\gamma = 1$,

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma)$$

por lo cual necesariamente como antes

o bien $b = b'$, de donde las formas (a, b, c) y (a', b', c') son idénticas (contrariamente a la hipótesis),

o bien $b = -b'$, y, por tanto, aquellas formas son opuestas. A la vez, en este caso las formas serían ambiguas; ya que $a = \pm 2b$.

De todo esto se concluye que las formas (a, b, c) y (a', b', c') no pueden ser propiamente equivalentes, a no ser que fueran opuestas, y al mismo tiempo *o bien* ambiguas *o bien* $a = c = a' = c'$. En estos casos, pudo verse fácilmente que las formas (a, b, c) y (a', b', c') son propiamente equivalentes. De hecho, si las formas son impropiamente opuestas y, además ambiguas, también tendrán que ser propiamente equivalentes. Si $a = c$, la forma $(\frac{D+(a-b)^2}{a}, a - b, a)$ será contigua a la forma (a, b, c) y por ende será equivalente; pero puesto que $D + b^2 = ac = a^2$ es $\frac{D+(a-b)^2}{a} = 2a - 2b$, la forma $(2a - 2b, a - b, a)$ es ambigua; por lo cual (a, b, c) también equivaldrá a su opuesta propiamente.

Igualmente, ahora puede deducirse fácilmente que cuando dos formas reducidas (a, b, c) y (a', b', c') son no opuestas pueden ser impropiamente equivalentes. En efecto serán impropiamente equivalentes si (a, b, c) y $(a', -b', c')$, las cuales no son idénticas, son propiamente equivalentes, y viceversa. Es evidente que la condición

bajo la cual aquéllas sean impropiamente equivalentes es que sean idénticas además de ser ambiguas o que $a = c$. Las formas reducidas que no son ni idénticas ni opuestas tampoco pueden ser propia ni impropiamente equivalentes.

173.

PROBLEMA. *Dadas dos formas F y F', con el mismo determinante negativo, se debe investigar si son equivalentes.*

Resolución. Búsquense dos formas reducidas f y f' propiamente equivalentes a las formas F y F' respectivamente. Si las formas f y f' son propiamente o impropiamente equivalentes, o equivalentes de ambos modos, entonces F y F' también lo son; pero si f y f' no son equivalentes de ninguna manera, tampoco lo son F y F'.

Del artículo anterior pueden presentarse cuatro casos:

1) Si f y f' no son ni idénticas ni opuestas, tampoco F y F' serían equivalentes de ningún modo.

2) Si f y f' son, *primero*, o idénticas u opuestas y, *segundo*, o ambiguas, o tienen sus términos extremos iguales, F y F' serían tanto propia como impropiamente equivalentes.

3) Si f y f' son idénticas, pero ni son ambiguas ni tienen términos extremos iguales, F y F' sólo serían propiamente equivalentes.

4) Si f y f' son opuestas, pero ni son ambiguas ni tienen términos extremos iguales, F y F' sólo serían impropiamente equivalentes.

Ejemplo. Para las formas $(41, 35, 30)$ y $(7, 18, 47)$ cuyo determinante $= -5$, se encuentran las formas reducidas no equivalentes $(1, 0, 5)$ y $(2, 1, 3)$; por lo que las formas originales de ningún modo serán equivalentes. A las formas $(23, 38, 63)$ y $(15, 20, 27)$ equivale la misma forma reducida $(2, 1, 3)$, y como ella es al mismo tiempo ambigua, las formas $(23, 38, 63)$ y $(15, 20, 27)$ serán equivalentes tanto propia como impropiamente. A las formas $(37, 53, 78)$ y $(53, 73, 102)$ equivalen las formas reducidas $(9, 2, 9)$ y $(9, -2, 9)$, y puesto que éstas son opuestas y sus términos extremos iguales, las formas dadas serán equivalentes propia e impropiamente a la forma opuesta.

174.

El número de formas reducidas que tienen un determinante dado $-D$ siempre es finito y relativamente pequeño en relación con el número D. Estas mismas

formas pueden encontrarse mediante dos métodos. Denotaremos las formas reducidas indefinidas del determinante $-D$ por (a, b, c) donde deben determinarse todos los valores de a, b, c.

Primer método. Tómense para a todos los números positivos y negativos no mayores que $\sqrt{\frac{4}{3}D}$, de los cuales $-D$ sea un residuo cuadrático, y para cada a se hace b sucesivamente igual a todos los valores de la expresión $\sqrt{-D} \pmod{a}$, no mayores que $\frac{1}{2}a$, tomados tanto positiva como negativamente; para cada uno de los valores determinados de a y b se pone $c = \frac{D+b^2}{a}$. Si resultan de este modo unas formas en las cuales $c < a$, éstas deberán rechazarse, pero las restantes son claramente reducidas.

Segundo método. Tómense para b todos los números positivos y negativos, no mayores que $\frac{1}{2}\sqrt{\frac{4}{3}D}$ o sea $\sqrt{\frac{1}{3}D}$. Para cada b, resuélvase $b^2 + D$ de todas las maneras como pueda hacerse en dos factores menores que $2b$ (también debe tomarse en cuenta la diversidad de los signos). Cuando los factores son diferentes, póngase el menor factor $= a$ y el otro $= c$. Como a no es $> \sqrt{\frac{4}{3}D}$, todas las formas originadas de esta manera serán claramente reducidas. Finalmente es claro que no puede existir ninguna forma reducida que no se encuentre por ambos métodos.

Ejemplo. Sea $D = 85$. Aquí el límite de los valores de a es $\sqrt{\frac{340}{3}}$, que está entre 10 y 11. Los números entre 1 y 10 (inclusive), de los cuales -85 es residuo cuadrático, son 1, 2, 5 y 10. De aquí se tienen doce formas:
$(1, 0, 85)$, $(2, 1, 43)$, $(2, -1, 43)$, $(5, 0, 17)$, $(10, 5, 11)$, $(10, -5, 11)$; $(-1, 0, -85)$,
$(-2, 1, -43)$, $(-2, -1, -43)$, $(-5, 0, -17)$, $(-10, 5, -11)$, $(-10, -5, -11)$.

Con el otro método, se tiene $\sqrt{\frac{85}{3}}$ para el límite de los valores de b, el cual está situado entre 5 y 6. Para $b = 0$, resultan las formas

$$(1, 0, -85), \quad (-1, 0, -85), \quad (5, 0, 17), \quad (-5, 0, -17),$$

para $b = \pm 1$ resultan $(2, \pm 1, 43)$ y $(-2, \pm 1, -43)$.
Para $b = \pm 2$ no existe ninguna, ya que 89 no puede resolverse en dos factores de los cuales sean ambos < 4. Lo mismo vale para ± 3 y ± 4. Finalmente para $b = \pm 5$ resultan

$$(10, \pm 5, 11) \quad \text{y} \quad (-10, \pm 5, -11).$$

175.

Si se rechaza una u otra de dos formas no idénticas pero propiamente equivalentes entre todas las formas reducidas de un determinante dado, las formas

restantes estarán provistas de esta propiedad notable: que cualquier forma del mismo determinante sería propiamente equivalente a una y sólo una de ellas (al contrario otras serían propiamente equivalentes entre sí). De donde, resulta claro que *todas las formas del mismo determinante pueden distribuirse en tantas clases como formas permanezcan*, a saber, se ponen en la misma clase todas las formas propiamente equivalentes a una forma reducida. Así para $D = 85$, permanecen las formas

$$(1, 0, 85), \quad (2, 1, 43), \quad (5, 0, 17), \quad (10, 5, 11)$$
$$(-1, 0, -85), \quad (-2, 1, -43), \quad (-5, 0, -17), \quad (-10, 5, -11).$$

Por lo que, todas las formas del determinante -85 podrán distribuirse en ocho clases según sean propiamente equivalentes o a la primera forma, o a la segunda etc. Desde luego, es claro que las formas colocadas en la misma clase serán propiamente equivalentes, y las formas de diferentes clases no pueden ser propiamente equivalentes. Pero más adelante desarrollaremos con mucho detalle este argumento concerniente a la clasificación de las formas. Aquí añadimos una sola observación. Mostramos antes que si el determinante de la forma (a, b, c) en negativo $= -D$, entonces a y c tendrán el mismo signo (porque $ac = b^2 + D$, y por lo tanto es positivo). Por la misma razón se percibe fácilmente que, si las formas (a, b, c) y (a', b', c') son equivalentes, todos los a, c, a', c' tendrán el mismo signo. De hecho, si la primera se transforma en la segunda por la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, será $a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$, de esto $aa' = (a\alpha + b\beta)^2 + D\gamma^2$ y por tanto ciertamente es no negativo. Puesto que ni a ni a' puede ser $= 0$, aa' será positivo y por eso los signos de a y a' serán los mismos. De esto es claro que las formas cuyos términos extremos son positivos están completamente separadas de aquéllas cuyos términos extremos son negativos. Sólo basta considerar estas formas reducidas, las que tienen sus términos extremos positivos; puesto que las restantes son iguales en número y provienen de ellas al asignar signos opuestos a los términos extremos. Lo mismo vale para las formas rechazadas o retenidas de las reducidas.

176.

Tenemos aquí una tabla de formas para ciertos determinantes negativos, según las cuales todas las restantes del mismo determinante pueden separarse en clases. Según la observación del artículo anterior, listamos únicamente la mitad, a saber,

aquéllas cuyos términos extremos son positivos.

D	
1	$(1,0,1)$.
2	$(1,0,2)$.
3	$(1,0,3)$, $(2,1,2)$.
4	$(1,0,4)$, $(2,0,2)$.
5	$(1,0,5)$, $(2,1,3)$.
6	$(1,0,6)$, $(2,0,3)$.
7	$(1,0,7)$, $(2,1,4)$.
8	$(1,0,8)$, $(2,0,4)$, $(3,1,3)$.
9	$(1,0,9)$, $(2,1,5)$, $(3,0,3)$.
10	$(1,0,10)$, $(2,0,5)$.
11	$(1,0,11)$, $(2,1,6)$, $(3,1,4)$, $(3,-1,4)$.
12	$(1,0,12)$, $(2,0,6)$, $(3,0,4)$, $(4,2,4)$.

Sería superfluo continuar esta tabla, dado que enseñaremos luego un método mucho más adecuado para construirla.

Es evidente que cada forma del determinante -1 es propiamente equivalente a la forma x^2+y^2 si sus términos extremos son positivos, pero equivalente a $-x^2-y^2$ si son negativos. Cada forma del determinante -2 cuyos términos son positivos es equivalente a la forma x^2+2y^2, etc. Cada forma del determinante -11 cuyos términos extremos son positivos es equivalente a una de éstas x^2+11y^2, $2x^2+2xy+6y^2$, $3x^2+2xy+4y^2$, $3x^2-2xy+4y^2$, etc.

177.

Problema. *Se tiene una serie de formas de las cuales cada una es contigua a la parte posterior de la precedente y se desea una transformación propia de la primera en cualquier forma de la serie.*

Solución. Sean las formas $(a,b,a')=F$; $(a',b',a'')=F'$; $(a'',b'',a''')=F''$; $(a''',b''',a'''')=F'''$ etc. Se denotan $\frac{b+b'}{a'}$, $\frac{b'+b''}{a''}$, $\frac{b''+b'''}{a'''}$ etc., respectivamente por h', h'', h''' etc. Sean x, y; x', y'; x'', y'' etc., las indeterminadas de las formas F, F', F''

etc. Se supone que F se transmuta

$$\begin{aligned} &\text{en } F' \text{ poniendo } x = \alpha' x' + \beta' y', && y = \gamma' x' + \delta' y' \\ &F'' \ . \ . \ . \ . \ x = \alpha'' x'' + \beta'' y'', && y = \gamma'' x'' + \delta'' y'' \\ &F''' \ . \ . \ . \ . \ x = \alpha''' x''' + \beta''' y''', && y = \gamma''' x''' + \delta''' y''' \end{aligned}$$

etc.

Entonces, puesto que F se transforma en F' poniendo $x = -y', \quad y = x' + h' y'$
F' en F'' poniendo $x' = -y'', \ y' = x'' + h'' y''$
F'' en F''' poniendo $x'' = -y''', \ y'' = x''' + h''' y'''$
etc. (art. 160)

fácilmente se encuentra el algoritmo siguiente (art. 159):

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' - \alpha' & \gamma'' = \delta' & \delta'' = h''\delta' - \gamma' \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \alpha'' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \gamma'' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \alpha''' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \gamma''' \end{array}$$

etc.,

o sea

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta' & \delta'' = h''\delta' - 1 \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' \end{array}$$

etc.

Puede deducirse sin dificultad tanto de su formación como del art. 159 que todas estas transformaciones son propias.

Este algoritmo bien simple y preparado para los cálculos es análogo al algoritmo expuesto en el artículo 27, al cual también puede reducirse*). Además, esta solución no está restringida a las formas de un determinante negativo, si no a todos los casos donde ninguno de los números a', a'', a''', etc., $= 0$.

*) Será, en la notación del art. 27

$$\beta^n = \pm[-h'', h''', -h'''', \ldots \pm h^n]$$

donde los signos ambiguos puestos deben ser $--$; $-+$; $+-$; $++$ conforme a que n sea de la forma

178.

PROBLEMA. *Dadas dos formas propiamente equivalentes a F y f del mismo determinante negativo, encontrar alguna transformación propia de la una en la otra.*

Solución. Supongamos que la forma F es (A, B, A'), y que por el método del artículo 171 se ha encontrado la progresión de formas (A', B', A'') y (A'', B'', A''') etc. hasta la forma reducida (A^m, B^m, A^{m+1}). De manera similar supongamos que f es (a, b, a') y que por el mismo método se encuentra la serie (a', b', a'') y (a'', b'', a''') hasta la forma reducida (a^n, b^n, a^{n+1}). Entonces pueden tener lugar dos casos.

I. Si las formas (A^m, B^m, A^{m+1}) y (a^n, b^n, a^{n+1}) o son idénticas u opuestas y, a la vez, ambiguas, entonces, las formas (A^{m-1}, B^{m-1}, A^m) y $(a^n, -b^{n-1}, a^{n-1})$ serán contiguas (donde A^{m-1} denota el penúltimo término de la progresión A, A', A'', $\ldots A^m$, y de manera semejante B^{m-1}, a^{n-1}, b^{n-1}). Puesto que $A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ o sea } A^m}$, resulta $B^{m-1} - b^{n-1} \equiv b^n - B^m$ y, por tanto $\equiv 0$, si las formas (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) son idénticas, y $\equiv 2b^n$ y por tanto $\equiv 0$, si son opuestas y ambiguas. Por lo que, en las progresiones de las formas

$$\begin{gathered}(A, B, A'), \quad (A', B', A''), \quad \ldots (A^{m-1}, B^{m-1}, A^m), \\ (a^n, -b^{n-1}, a^{n-1}), \quad (a^{n-1}, -b^{n-2}, a^{n-2}), \quad \ldots (a', -b, a), \quad (a, b, a')\end{gathered}$$

cada forma será contigua a la precedente; y de esto, por el artículo anterior podrá encontrarse una transformación propia de la primera F en la segunda f.

II. Si las formas (A^m, B^m, A^{m+1}) y (a^n, b^n, a^{n+1}) no son idénticas, sino opuestas y, a la vez, $A^m = A^{m+1} = a^n = a^{n+1}$; entonces, la progresión de las formas

$$\begin{gathered}(A, B, A'), \quad (A', B', A''), \quad \ldots (A^m, B^m, A^{m+1}), \\ (a^n, -b^{n-1}, a^{n-1}), \quad (a^{n-1}, -b^{n-2}, a^{n-2}), \quad \ldots (a', -b, a), \quad (a, b, a')\end{gathered}$$

estarán provistas de la misma propiedad. Puesto que $A^{m+1} = a^n$, y $B^m - b^{n-1} = -(b^n + b^{n-1})$ será divisible por a^n. De donde, por el artículo anterior, se encontrará una transformación propia de la primera forma F en la segunda f.

$4k + 0$; 1; 2; 3; y

$$\delta^n = \pm[h', -h'', h''', \ldots \pm h^n]$$

donde los signos ambiguos deben ser $+-$; $++$; $--$; $-+$, según n sea de la forma $4k + 0$; 1; 2; 3. Pero dado que esto puede confirmarse fácilmente por sí mismo, la brevedad no permite exponerlo con amplitud.

Ejemplo. Para las formas $(23, 38, 63)$ y $(15, 20, 27)$ se tiene la progresión $(23, 38, 63)$, $(63, 25, 10)$, $(10, 5, 3)$, $(3, 1, 2)$, $(2, -7, 27)$, $(27, -20, 15)$, $(15, 20, 27)$ por lo cual

$$h' = 1, \quad h'' = 3, \quad h''' = 2, \quad h'''' = -3, \quad h''''' = -1, \quad h'''''' = 0$$

De esto se deduce que la transformación de la forma $23x^2 + 76xy + 63y^2$ en $15t^2 + 40tu + 27u^2$ es ésta: $x = -13t - 18u$, $y = 8t + 11u$.

De esta solución, se deduce sin dificultad la solución del problema: *Si las formas F y f son impropiamente equivalentes, hallar una transformación impropia de la forma F en f.* De hecho, sea $f = at^2 + 2btu + a'u^2$, entonces la forma opuesta $ap^2 - 2bpq + a'q^2$ será propiamente equivalente a la forma F. Búsquese una transformación propia de la forma F en $x = \alpha p + \beta q$ y $y = \gamma p + \delta q$, entonces es claro que F se transforma en f dadas $x = \alpha t - \beta u$, $y = \gamma t - \delta u$; por lo que esta transformación será impropia.

Si, por lo tanto, las formas F y f son equivalentes tanto propia como impropiamente, entonces podrá encontrarse tanto una transformación propia como una impropia.

179.

PROBLEMA. *Si las formas F y f son equivalentes, hallar todas las transformaciones de la forma F en f.*

Solución. Si las formas F y f son equivalentes de una sola manera, i.e., solamente propiamente o solamente impropiamente, por el artículo precedente búsquese alguna transformación de la forma F en f. Es claro que no pueden darse otras más que aquéllas semejantes a ésta. Si, por otro lado las formas F y f son equivalentes tanto propia como impropiamente, búsquense dos transformaciones: la una propia y la otra impropia. Sea la forma $F = (A, B, C)$, $B^2 - AC = -D$, y el máximo común divisor de los números A, $2B$, $C = m$. Entonces es claro del artículo 162 que, en el primer caso, todas las transformaciones de la forma F en f pueden deducirse de una transformación; y en el segundo, todas las propias de una propia y todas las impropias de una impropia, si se tuvieran todas las soluciones de la ecuación $t^2 + Du^2 = m^2$. Por lo tanto, encontradas éstas, el problema se habría resuelto.

Se tiene, sin embargo, $D = AC - B^2$, $4D = 4AC - 4B^2$; por lo cual $\frac{4D}{m^2} = 4(\frac{AC}{m^2}) - (\frac{2B}{m})^2$ será un entero. Ahora, si

1) $\frac{4D}{m^2} > 4$, será $D > m^2$; de donde en $t^2 + Du^2 = m^2$, u deberá ser $= 0$, y por tanto t no puede tener otros valores más que $+m$ y $-m$. De esto, si F y f son equivalentes de una sola manera, entonces no puede darse alguna transformación más que

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

la cual resulta poniendo $t = m$ (artículo 162), y otra

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'.$$

Si por el otro lado F y f son equivalentes tanto propia como impropiamente, y si se tiene alguna transformación propia

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

y una impropia

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

entonces no se presentará otra transformación propia salvo aquéllas (poniendo $t = m$) y éstas

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

(poniendo $t = -m$) y de modo semejante ninguna impropia salvo

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'; \quad y \quad x = -\alpha' x' - \beta' y', \quad y = -\gamma' x' - \delta' y'.$$

2) Si $\frac{4D}{m^2} = 4$, o sea $D = m^2$, la ecuación $t^2 + Du^2 = m^2$ admitirá cuatro soluciones: t, $u = m$, 0; $-m$, 0; 0, 1; 0, -1. De esto, si F y f son equivalentes de una sola manera y si tenemos alguna transformación

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

resultarán *cuatro* ecuaciones:

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \mp\frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y', \quad y = \pm\frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'$$

Por otro lado, si F y f son equivalentes de dos maneras, o sea, si además de esta transformación dada se tiene otra no semejante a esta misma, ella también

proporcionará cuatro no semejantes a ella de tal manera que se tengan *ocho* transformaciones. Además, en este caso puede demostrarse que F y f siempre son equivalentes de dos maneras. Como $D = m^2 = AC - B^2$, m también dividirá a B. El determinante de la forma $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ será $= -1$, por lo que será equivalente a la forma $(1, 0, 1)$ o a $(-1, 0, -1)$. Sin embargo, se percibe que, mediante la misma transformación por la cual se transforma $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ en $(\pm 1, 0, \pm 1)$, se transformará la forma (A, B, C) en una ambigua $(\pm m, 0, \pm m)$. Por lo que, la forma (A, B, C), equivalente a una ambigua, equivaldrá tanto propia como impropiamente a cualquier forma a la cual sea equivalente.

3) Si $\frac{4D}{m^2} = 3$, o sea $4D = 3m^2$, entonces m será par y el total de soluciones de la ecuación $t^2 + Du^2 = m^2$ será seis:

$$t,\, u \quad = m,\, 0; \quad -m,\, 0; \quad \frac{1}{2}m,\, 1; \quad \frac{-1}{2}m,\, -1; \quad \frac{1}{2}m,\, -1; \quad \frac{-1}{2}m,\, 1.$$

Por consiguiente, si se tienen dos transformaciones no semejantes de la forma F en f,

$$\begin{array}{ll} x = \alpha x' + \beta y' & y \,=\, \gamma x' + \delta y' \\ x = \alpha' x' + \beta' y' & y = \gamma' x' + \delta' y' \end{array}$$

se tendrán doce transformaciones, a saber, seis semejantes a la primera

$$\begin{array}{l} x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y' \\ x = \pm(\frac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m})x' \pm (\frac{1}{2}\beta - \frac{\beta B + \delta C}{m})y' \\ y = \pm(\frac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m})x' \pm (\frac{1}{2}\delta + \frac{\beta A + \delta B}{m})y' \\ x = \pm(\frac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m})x' \pm (\frac{1}{2}\beta + \frac{\beta B + \delta C}{m})y' \\ y = \pm(\frac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m})x' \pm (\frac{1}{2}\delta - \frac{\beta A + \delta B}{m})y' \end{array}$$

y seis semejantes a la segunda, que se originan de éstas al sustituir α, β, γ, δ por α', β', γ', δ'.

Para demostrar que en este caso F y f siempre son equivalentes de ambas maneras, consideremos lo siguiente. El determinante de la forma $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ será $= \frac{-4D}{m^2} = -3$, y por tanto esta forma es equivalente (art. 176) o a la forma $(\pm 1, 0, \pm 3)$, o a la forma $(\pm 2, \pm 1, \pm 2)$. De donde se sabe que la forma (A, B, C) es equivalente

o a la forma $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ o a la forma $(\pm m, \frac{1}{2}m, \pm m)$*), las cuales son ambas ambiguas, y, por tanto, de ambas maneras equivalente a una de ellas.

4) Si se supone $\frac{4D}{m^2} = 2$, sería $(\frac{2B}{m})^2 = 4\frac{AC}{m^2} - 2$, y, por tanto, $\equiv 2 \pmod 4$. Pero, como ningún cuadrado puede ser $\equiv 2 \pmod 4$, este caso no puede darse aquí.

5) Suponiendo que $\frac{4D}{m^2} = 1$, sería $(\frac{2B}{m})^2 = 4\frac{AC}{m^2} - 1 \equiv -1 \pmod 4$. Pero como esto es imposible, este caso tampoco puede ocurrir aquí.

Además, como D no puede ser ni $= 0$ ni negativo, no pueden darse otros casos diferentes más que los enumerados.

180.

PROBLEMA. *Hallar todas las representaciones del número dado M por la forma $ax^2 + 2bxy + cy^2 \ldots F$, del determinante negativo $-D$, en la cual x e y tengan valores primos entre sí.*

Solución. Por el artículo 154, notamos que M no puede representarse tal como se necesita, a menos que $-D$ sea residuo cuadrático de M. Así, primero búsquense todos los valores diferentes (i.e. incongruentes) de la expresión $\sqrt{-D} \pmod M$; sean estos valores $N, -N, N', -N', N'', -N''$ etc. Para simplificar los cálculos, se pueden determinar todos los N, N', etc., de tal manera que no sean $> \frac{1}{2}M$. Puesto que cualquier representación debe pertenecer a alguno de estos valores, consideraremos cada uno separadamente.

Si las formas F, $(M, N, \frac{D+N^2}{M})$ no son propiamente equivalentes, no puede existir ninguna representación de M perteneciente al valor N (artículo 168). Si al contrario existen, buscaremos una transformación propia de la forma F en

$$Mx'^2 + 2Nx'y' + \frac{D+N^2}{M}y'^2$$

la cual sea

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

y $x = \alpha$, $y = \gamma$ será una representación del número M por F perteneciente al valor N. Sea el máximo común divisor de los números A, $2B$, $C = m$, entonces distinguiremos tres casos (artículo anterior):

*) Puede demostrarse que la forma (A, B, C) necesariamente equivaldrá a la segunda; pero esto no es necesario aquí.

1) Si $\frac{4D}{m^2} > 4$ no se darán representaciones pertenecientes a N salvo estas *dos* $x = \alpha$, $y = \gamma$ y $x = -\alpha$, $y = -\gamma$ (artículos 169 y 179).

2) Si $\frac{4D}{m^2} = 4$ se tendrán *cuatro* representaciones

$$x = \pm\alpha, \quad y = \pm\gamma; \qquad x = \mp\frac{\alpha B + \gamma C}{m}, \quad y = \pm\frac{\alpha A + \gamma B}{m}$$

3) Si $\frac{4D}{m^2} = 3$ se tendrán *seis* representaciones

$$\begin{array}{ll} x = \pm\alpha & y = \pm\gamma \\ x = \pm(\frac{1}{2}\alpha - \frac{\alpha B+\gamma C}{m}) & y = \pm(\frac{1}{2}\gamma + \frac{\alpha A+\gamma B}{m}) \\ x = \pm(\frac{1}{2}\alpha + \frac{\alpha B+\gamma C}{m}) & y = \pm(\frac{1}{2}\gamma - \frac{\alpha A+\gamma B}{m}) \end{array}$$

De la misma manera se deben buscar las representaciones pertenecientes a los valores $-N$, N', $-N'$ etc.

181.

La investigación de las representaciones del número M por la forma F, en la cual x e y tienen valores no primos entre sí, puede reducirse fácilmente al caso ya considerado. Suponga que se hace tal representación al poner $x = \mu e$ e $y = \mu f$ de manera que μ sea el máximo común divisor de μe y μf, o sea, e y f son primos entre sí. Entonces tendremos que $M = \mu^2(Ae^2 + 2Bef + Cf^2)$ y, por lo tanto, será divisible por μ^2. Sin embargo, la sustitución $x = e$, $y = f$ será una representación del número $\frac{M}{\mu^2}$ por la forma F, en la cual x e y tienen valores primos entre sí. Si M no es divisible por ningún cuadrado (salvo 1), por ejemplo, si es un número primo, no se darán tales representaciones de M. Sin embargo, si M involucra divisores cuadrados, sean éstas μ^2, ν^2, π^2 etc. Se buscan primero todas las representaciones del número $\frac{M}{\mu^2}$ por la forma (A, B, C), en las cuales x e y tienen valores primos entre sí. Tales valores, si se multiplican por μ, suministrarán todas las representaciones de M en las cuales el máximo común divisor de los números x e y es μ. De modo semejante, todas las representaciones de $\frac{M}{\nu^2}$, en las cuales los valores de x e y son primos entre sí, producirán todas las representaciones de M en las que el máximo común divisor de los valores x e y es ν etc.

Por lo tanto, es claro que por las reglas precedentes pueden encontrarse todas las representaciones de un número dado por una forma dada de un determinante negativo.

Aplicaciones especiales a la descomposición de los números en dos cuadrados, en un cuadrado simple y uno doble, en un cuadrado simple y uno triple .

182.

Pasamos a ciertos casos especiales tanto por su elegancia notable como por el incesante trabajo empleado en ellos por el ilustre Euler, por lo que están provistos de una belleza casi clásica.

I. Ningún número puede representarse por la forma $x^2 + y^2$, de modo que x sea primo a y (o sea descompuesto en dos cuadrados primos entre sí) a no ser que -1 sea un residuo cuadrático de él. Sin embargo, tales números tomados positivamente sí pueden serlo. Sea M un número tal, y todos los valores de la expresión $\sqrt{-1} \pmod{M}$ éstos: N, $-N$, N', $-N'$, N'', $-N''$ etc., entonces, por el artículo 176 la forma $(M, N, \frac{N^2+1}{M})$ será propiamente equivalente a la forma $(1, 0, 1)$. Sea $x = \alpha y' + \beta y'$, $y = \gamma x' + \delta y'$ una transformación propia de la segunda en la primera, y las representaciones del número M por la forma $x^2 + y^2$ pertenecientes a N estas cuatro*): $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\gamma$, $y = \pm\alpha$.

Puesto que la forma $(1, 0, 1)$ es ambigua, de hecho será propiamente equivalente a la forma $(M, -N, \frac{N^2+1}{M})$, y por ende aquélla se transmutará en ésta, poniendo $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. De esto se derivan cuatro representaciones de M pertenecientes a $-N$, $x = \pm\alpha$, $y = \mp\gamma$; $x = \pm\gamma$, $y = \pm\alpha$. Así pues, existen ocho representaciones de M, la mitad de los cuales pertenece a N, la otra mitad a $-N$; pero todas éstas representan sólo *una* descomposición del número M en dos cuadrados, $M = \alpha^2 + \gamma^2$, si sólo consideramos a los cuadrados mismos, pero no al orden de las raíces ni a sus signos.

Por tanto, si no existen otros valores de la expresión $\sqrt{-1} \pmod{M}$, salvo N y $-N$, lo cual e.g. resulta cuando M es un número primo, M podrá resolverse en dos cuadrados primos entre sí de una sola manera. Puesto que -1 es un residuo cuadrático de cualquier número primo de la forma $4n + 1$ (art. 108), entonces es evidente que un número primo no puede descomponerse en dos cuadrados no primos entre sí. Así tendremos el teorema:

Cualquier número primo de la forma $4n + 1$ *puede descomponerse como suma de dos cuadrados, y de una sola manera.*

$$1 = 0 + 1, \quad 5 = 1 + 4, \quad 13 = 4 + 9, \quad 17 = 1 + 16, \quad 29 = 4 + 25, \quad 37 = 1 + 36,$$

*) Es claro que este caso está contenido en (2) del artículo 180.

$$41 = 16 + 25, \quad 53 = 4 + 49, \quad 61 = 25 + 36, \quad 73 = 9 + 64, \quad 89 = 25 + 64,$$
$$97 = 16 + 81 \text{ etc.}$$

Este teorema elegantísimo ya fue conocido por Fermat, pero fue demostrado primero por el ilustre Euler, *Comm. nov. Petr.*, V, 1754 y 1755, p. 3. En el cuarto volumen existe una disertación perteneciente al mismo argumento (p. 3) pero entonces aún no había encontrado una solución completa, véase especialmente artículo 27.

Por lo tanto, si algún número de la forma $4n + 1$ puede resolverse en dos cuadrados o bien en varias maneras, o bien de ninguna manera, entonces no será primo.

Al contrario, si la expresión $\sqrt{-1}$ (mod. M) tiene otros valores, además de N y $-N$, se presentarán todavía otras representaciones de M, pertenecientes a éstos. Así pues, en este caso M podrá resolverse de varias maneras en dos cuadrados; e.g. $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Las restantes representaciones, en las cuales x e y tienen valores no primos entre sí, pueden encontrarse con facilidad por nuestro método general. Sólo observamos que, si algún número que involucra factores de la forma $4n + 3$ no puede liberarse de éstos por ninguna división por un cuadrado (esto sucederá si uno o varios de tales factores tienen *un exponente impar*), entonces dicho número tampoco puede resolverse de manera alguna en dos cuadrados*).

II. Ningún número del cual -2 es un no residuo podrá representarse por la forma $x^2 + 2y^2$, de tal modo que x sea primo a y, pero todos los restantes sí podrán. Sea -2 un residuo del número M, y N algún valor de la expresión $\sqrt{-2}$ (mod. M). Entonces, por art. 176 las formas $(1,\ 0,\ 2)$ y $(M, N, \frac{N^2+2}{M})$ serán propiamente equivalentes. La primera se transforma en la segunda poniendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, y $x = \alpha$, $y = \gamma$ será una representación del número M perteneciente a

*) Si el número $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$ de manera que a, b, c sean números primos diferentes de la forma $4n + 1$ y si S es el producto de todos los factores primos de M de la forma $4n + 3$ (a tal forma cualquier número positivo puede reducirse, haciendo $\mu = 0$ cuando M es impar, y $S = 1$, cuando M no involucra factores de la forma $4n + 3$), entonces M *de ninguna manera* podrá resolverse en dos cuadrados si S no es un cuadrado, pero si S es un cuadrado, se presentarán $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. descomposiciones de M cuando alguno de los números α, β, γ, etc. es impar, pero $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. $+ \frac{1}{2}$ cuando todos α, β, γ, etc. son pares (puesto que se examinan solamente los cuadrados). Los que son versados en el cálculo de combinaciones podrán llevar a cabo la demostración de este teorema (en el que, como para otros *casos particulares*, no podemos detenernos) sin dificultad a partir de nuestra teoría general. Vea artículo 105.

N. Además de ésta, tendremos $x = -\alpha$ e $y = -\gamma$, y no existen otras pertenecientes a N (artículo 180).

De modo semejante, se percibe que las representaciones $x = \pm\alpha$, $y = \mp\gamma$ pertenecen al valor $-N$. Sin embargo estas cuatro representaciones presentan únicamente una descomposición de M en un cuadrado y el doble de un cuadrado, y si más allá de N y $-N$ no se dan otros valores de la expresión $\sqrt{-2}$ (mod. M), tampoco existirán otras descomposiciones. De esto, con la ayuda de las proposiciones del artículo 116, se deduce fácilmente este teorema:

Cualquier número primo de la forma $8n+1$ *u* $8n+3$ *puede descomponerse en un cuadrado y un cuadrado duplicado de una sola manera.*

$$1 = 1 + 0, \quad 3 = 1 + 2, \quad 11 = 9 + 2, \quad 17 = 9 + 8, \quad 19 = 1 + 18, \quad 41 = 9 + 32,$$
$$43 = 25 + 18, \quad 59 = 9 + 50, \quad 67 = 49 + 18, \quad 73 = 1 + 72, \quad 83 = 81 + 2,$$
$$89 = 81 + 8, \quad 97 = 25 + 72 \quad \text{etc.}$$

Fermat también conocía este teorema, como varios semejantes; pero el ilustre Lagrange dio la primera demostración, *Suite des recherches d'Arithmétique,* Nouv. Mém. de l'Ac. de Berlín, 1775, p. 323. Ya el ilustre Euler había llevado a cabo mucho con relación al mismo argumento, *Specimen de usu observationum in mathesi pura,* Comm. nov. Petr., VI, p. 185. Pero nunca encontró una demostración completa del teorema. Compárese también la disertación en el Tomo VIII (para los años 1760 y 1761) *Supplementum quorundam theorematum arithmeticorum*, al final.

III. Se demuestra por un método semejante que, cada número del cual -3 es un residuo cuadrático, puede representarse o por la forma $x^2 + 3y^2$ o por $2x^2 + 2xy + 2y^2$, de manera que el valor de x sea primo al valor de y. Por lo tanto, puesto que -3 es un residuo de todos los números primos de la forma $3n+1$ (art. 119), y ya que únicamente números *pares* pueden representarse por la forma $2x^2+2xy+2y^2$. Tal como arriba se tiene este teorema:

Cualquier número primo de la forma $3n+1$ *puede descomponerse como suma de un cuadrado y un cuadrado triplicado y sólo de una manera.*

$$1 = 1 + 0, \quad 7 = 4 + 3, \quad 13 = 1 + 12, \quad 19 = 16 + 3, \quad 31 = 4 + 27, \quad 37 = 25 + 12,$$
$$43 = 16 + 27, \quad 61 = 49 + 12, \quad 67 = 64 + 3, \quad 73 = 25 + 48 \quad \text{etc.}$$

El ilustre Euler presentó la primera demostración de este teorema en el comentario citado, *Comm. nov. Petr.,* VIII, p. 105.

De modo semejante podremos adelantar y mostrar que todo número primo de la forma $20n+1$, o $20n+3$, o $20n+7$, o $20n+9$ (de los cuales -5 es un residuo) puede representarse por una de las dos formas x^2+5y^2, $2x^2+2xy+3y^2$, y los números primos de la forma $20n+1$ y $20n+9$ pueden representarse por la primera forma, los números primos de la forma $20n+3$, $20n+7$ por la segunda, y además los dobles de los primos de la forma $20n+1$, $20n+9$ por la forma $2x^2+2xy+3y^2$ y los dobles de los primos de la forma $20n+3$, $20n+7$ por la forma x^2+5y^2. Pero esta proposición y otras infinitas particulares podrán derivarse de las precedentes y de lo que se discuta más adelante. Pasamos ahora a las *formas de un determinante positivo.* Dado que la naturaleza de ellas es completamente diferente cuando el determinante es un cuadrado que cuando no es un cuadrado, excluiremos primero las formas de un determinante cuadrado y luego las consideraremos por separado.

Sobre las formas de un determinante positivo no cuadrado.

183.

PROBLEMA. *Dada cualquier forma (a, b, a'), cuyo determinante positivo y no cuadrado es $= D$, se debe encontrar una forma (A, B, C) propiamente equivalente a ella, en la cual B sea positivo y $< \sqrt{D}$ y donde A, si es positivo o $-A$, si A es negativo, estará situada entre $\sqrt{D} + B$ y $\sqrt{D} - B$.*

Resolución. Suponemos que en la forma propuesta las dos condiciones aún no tienen lugar; de lo contrario no sería necesario buscar otra forma. Además, observamos que en una forma de un determinante *no cuadrado*, el primer término o el último no puede ser $= 0$ (artículo 171, nota de pie). Sea $b' \equiv -b \pmod{a'}$ de modo que esté situado entre los límites $\sqrt{D}$ y $\sqrt{D} \mp a'$ (tomando el signo superior cuando a' es positivo, el inferior cuando es negativo), lo cual es posible por un razonamiento como el del art. 3. Sea $\frac{b'^2-D}{a'} = a''$, que será un entero ya que $b'^2 - D \equiv b^2 - D \equiv aa' \equiv 0 \pmod{a'}$. Ahora, si $a'' < a'$, se tomará $b'' \equiv -b' \pmod{a''}$ y situado entre $\sqrt{D}$ y $\sqrt{D} \mp a''$ (según a'' sea positivo o negativo) y $\frac{b''^2-D}{a''} = a'''$. Si de nuevo $a''' < a''$, sea otra vez $b''' \equiv -b'' \pmod{a'''}$ y situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'''$ y $\frac{b'''^2-D}{a'''} = a''''$. Se continuará este procedimiento para formar la progresión a', a'', a''', a'''' etc. hasta un término a^{m+1} no menor que el precedente a^m. Esto finalmente debe suceder, pues de lo contrario se tendrá una progresión infinita de números enteros continuamente decrecientes. Entonces, dadas $a^m = A$, $b^m = B$ y $a^{m+1} = C$, la forma (A, B, C) satisfará todas las condiciones.

Demostración. I. Puesto que en la progresión de formas (a, b, a'), (a', b', a''), (a'', b'', a''') etc. cualquiera es contigua a la precedente, la última (A, B, C) será propiamente equivalente a la primera (a, b, a').

II. Puesto que B está situado entre $\sqrt{D}$ y $\sqrt{D} \mp A$ (tomando siempre el signo superior cuando A es positivo, el inferior cuando A es negativo), es claro que, si se pone $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$, estos p y q serán positivos. Se confirma fácilmente que $q^2 + 2pq + 2p\sqrt{D} = D + A^2 - B^2$; por lo que $D + A^2 - B^2$ será un número positivo, el cual pondremos $= r$. De esto, puesto que $D = B^2 - AC$ resulta $r = A^2 - AC$ y por tanto $A^2 - AC$ será un número positivo. Pero, ya que por hipótesis A no es mayor que C, es claro que esto no puede suceder a menos que AC sea negativo, y por lo tanto los signos de A y C deben ser opuestos. De esto, $B^2 = D + AC < D$ y por tanto $B < \sqrt{D}$.

III. Además, ya que $-AC = D - B^2$, tendremos $AC < D$, y de esto (puesto que A no es $> C$) $A < \sqrt{D}$. Por lo que, $\sqrt{D} \mp A$ será positivo, y por tanto también lo será B, el cual está situado entre los límites $\sqrt{D}$ y $\sqrt{D} \mp A$.

IV. De esto, con más razón $\sqrt{D} + B \mp A$ es positivo, y dado que $\sqrt{D} - B \mp A = -q$, es negativo, $\pm A$ estará situado entre $\sqrt{D} + B$ y $\sqrt{D} - B$. *Q. E. D.*

Ejemplo. Propuesta la forma $(67, 97, 140)$ cuyo determinante es $= 29$, se encontrará aquí la progresión de las formas $(67, 97, 140)$, $(140, -97, 67)$, $(67, -37, 20)$, $(20, -3, -1)$ y $(-1, 5, 4)$. La última es la buscada.

Llamaremos *formas reducidas* a tales formas (A, B, C) de un determinante positivo no cuadrado D, en las cuales A, tomado positivamente, está situado entre $\sqrt{D} + B$ y $\sqrt{D} - B$, siendo B positivo y $< \sqrt{D}$. Así pues las formas reducidas de un determinante positivo no cuadrado difieren de las formas reducidas de un determinante negativo. Pero debido a la gran analogía entre éstas y aquéllas, no quisimos introducir diferentes denominaciones.

184.

Si se pudiera reconocer la equivalencia de dos formas *reducidas* de determinante positivo con la misma facilidad que en el caso de aquéllas de determinante negativo (art. 172) se reconocería sin dificultad la equivalencia de dos formas *cualesquiera* de determinante positivo. Pero aquí el asunto es muy diferente, y puede suceder que muchas formas reducidas sean equivalentes entre sí. Antes de dedicarnos a este problema, será necesario inquirir más detalladamente en la naturaleza de las

formas reducidas (de un determinante positivo no cuadrado, lo cual siempre está supuesto).

1) Si (a, b, c) es una forma reducida, a y c tendrán signos opuestos. Ya que puesto el determinante de la forma $= D$, será $ac = b^2 - D$, y por lo tanto, puesto que $b < \sqrt{D}$, será negativo.

2) El número c tomado positivamente estará situado, tal como a, entre $\sqrt{D}+b$ y $\sqrt{D} - b$. Puesto que $-c = \frac{D-b^2}{a}$; entonces c, abstraído del signo, estará situado entre $\frac{D-b^2}{\sqrt{D}+b}$ y $\frac{D-b^2}{\sqrt{D}-b}$, i.e., entre $\sqrt{D} - b$ y $\sqrt{D} + b$.

3) De esto es evidente que (c, b, a) también será una forma reducida.

4) Tanto a como c serán $< 2\sqrt{D}$. En efecto, ambos son $< \sqrt{D} + b$, y así con más razón $< 2\sqrt{D}$.

5) El número b estará situado entre $\sqrt{D}$ y $\sqrt{D} \mp a$ (tomando el signo superior cuando a es positivo, el inferior cuando es negativo). Puesto que $\pm a$ cae entre $\sqrt{D}+b$ y $\sqrt{D} - b$, entonces $\pm a - (\sqrt{D} - b)$, o sea $b - (\sqrt{D} \mp a)$ será positivo; sin embargo $b - \sqrt{D}$ es negativo, debido a que b estará situado entre $\sqrt{D}$ y $\sqrt{D} \mp a$. Del mismo modo se demuestra que b cae entre $\sqrt{D}$ y $\sqrt{D} \mp c$ (según c sea positivo o negativo).

6) *Cada forma reducida* (a, b, c) *es contigua por una u otra parte a una reducida y no a varias.*

Sea $a' = c$, $b' \equiv -b \pmod{a'}$ tal que esté situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'$*), $c' = \frac{b'^2-D}{a'}$, y la forma (a', b', c') estará contigua a la forma (a, b, c) por su última parte. A la vez, es evidente que si existe alguna forma reducida contigua a la forma (a, b, c) por la última parte, ella misma no puede ser diferente a (a', b', c'). Sin embargo, demostramos que ésta se ha reducido así:

A) Si se pone

$$\sqrt{D} + b \mp a' = p, \qquad \pm a' - (\sqrt{D} - b) = q, \qquad \sqrt{D} - b = r$$

entonces por (2) arriba y la definición de forma reducida, p, q y r serán positivos. Además, póngase

$$b' - (\sqrt{D} \mp a') = q', \qquad \sqrt{D} - b' = r'$$

*) Donde los signos son ambiguos, siempre vale el superior cuando a' es positivo, el inferior cuando a' es negativo.

y q' y r' serán positivos, puesto que b' está situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'$. Finalmente, sea $b + b' = \pm ma'$ entonces m será un entero. Es claro que será $p + q' = b + b'$, y por tanto $b + b'$, o sea $\pm ma'$ es positivo, y por eso también lo es m; de donde resulta que $m - 1$ no será negativo. Además, tenemos

$$r + q' \pm ma' = 2b' \pm a', \qquad \text{o sea} \quad 2b' = r + q' \pm (m-1)a'$$

de donde $2b'$ y b' serán necesariamente positivos. Y puesto que $b' + r' = \sqrt{D}$, tendremos $b' < \sqrt{D}$.

B) Además tenemos

$$r \pm ma' = \sqrt{D} + b', \qquad \text{o sea} \quad r \pm (m-1)a' = \sqrt{D} + b' \mp a'$$

por lo cual $\sqrt{D} + b' \mp a'$ será positivo. Puesto que $\pm a' - (\sqrt{D} - b') = q'$, y por lo tanto positivo, $\pm a'$ estará situado entre $\sqrt{D} + b'$ y $\sqrt{D} - b'$. Por esto, (a', b', c') será una forma reducida.

Del mismo modo se demuestra que si tenemos $'c = a$, $'b \equiv -b \pmod{'c}$ con $'b$ situado entre $\sqrt{D}$ y $\sqrt{D} \pm 'c$, y si $'a = \frac{'b^2 - D}{'c}$, entonces la forma $('a, 'b, 'c)$ será reducida. Evidentemente, esta forma también es contigua a la forma (a, b, c) por la primera parte, y salvo $('a, 'b, 'c)$, otra forma reducida no podrá estar provista de esta propiedad.

Ejemplo. La forma reducida $(-14, 3, 13)$ es contigua por la parte última a la reducida $(5, 11, -14)$ cuyo determinante es $= 191$, y por la parte primera es contigua a $(-22, 9, 5)$.

7) Si la forma reducida (a', b', c') es contigua a la forma reducida (a, b, c) por la parte última, la forma (c', b', a') será contigua por la parte primera a la forma reducida (c, b, a). Si la forma $('a, 'b, 'c)$ es contigua por la parte primera a la reducida (a, b, c), la reducida $('c, 'b, 'a)$ será contigua a la reducida (c, b, a) por la parte última. También las formas $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b', -c')$ serán reducidas, y la segunda contigua a la primera, la tercera a la segunda por la parte última, o sea la primera a la segunda y la segunda a la tercera por la parte primera. De modo semejante, esto vale para las tres formas $(-c', b', -a')$, $(-c, b, -a)$ y $(-'c, 'b, -'a)$. Esto es tan obvio que no es necesario explicarlo.