201.

Añadimos las siguientes observaciones acerca del problema tratado en los artículos precedentes.

1) Puesto que hemos mostrado cómo resolver la ecuación $t^2 - Du^2 = m^2$ para todos los casos cuando m es el máximo común divisor de los tres números M, $2N$, P, tal que $N^2 - MP = D$, es útil especificar todos los números que pueden ser esos divisores, es decir, todos los valores de m para un valor dado de D. Sea $D = n^2 D'$ de modo que D' esté enteramente libre de factores cuadrados. Esto puede obtenerse poniendo n^2 como el cuadrado mayor que divide D y, si D no tiene un factor cuadrado, poniendo $n = 1$. Entonces:

Primero, si D' es de la forma $4k + 1$, cualquier divisor de $2n$ será un valor de m y viceversa. En efecto, si g es un divisor de $2n$, tendremos la forma $(g, n, \frac{n^2(1-D')}{g})$, cuyo determinante es D y en la cual el máximo común divisor de los números g, $2n$, $\frac{n^2(D'-1)}{g}$ será obviamente g (puesto que es claro que $\frac{n^2(D'-1)}{g^2} = \frac{4n^2}{g^2} \cdot \frac{(D'-1)}{4}$ es un entero). Si, por el otro lado, suponemos que g es un valor de m, es decir, el máximo común divisor de los números M, $2N$, P, y que $N^2 - MP = D$, manifiestamente $4D$ o $4n^2 D'$ será divisible por g^2. Se sigue que $2n$ es divisible por g. Pues, si g no dividiera a $2n$, g y $2n$ tendrían un máximo común divisor menor que g. Supóngase que fuera $= \delta$, y $2n = \delta n'$, $g = \delta g'$; $n'^2 D'$ será divisible por g'^2. Así, n' y g' al igual que n'^2 y g'^2 serían primos relativos y D' sería divisible por g'^2, en contra de la hipótesis según la cual D' está libre de factores cuadrados.

Segundo, si D' es de la forma $4k + 2$ o $4k + 3$, cualquier divisor de n será un valor de m e, inversamente, cualquier valor de m dividirá n. En efecto, si g es un divisor de n se tendrá una forma $(g, 0, \frac{-n^2 D'}{g})$ cuyo determinante es $= D$. Claramente el máximo común divisor de los números $g, 0, \frac{n^2 D'}{g}$ será g. Ahora, si suponemos que g es un valor de m, es decir, el máximo común divisor de los números $M, 2N, P$ y que $N^2 - MP = D$, de la misma forma que arriba, g dividirá $2n$ y $\frac{2n}{g}$ será un entero. Si este cociente es impar, el cuadrado $\frac{4n^2}{g^2}$ será $\equiv 1 \pmod 4$, y entonces $\frac{4n^2 D'}{g^2}$ sería $\equiv 2$, o $\equiv 3 \pmod 4$. Pero $\frac{4n^2 D'}{g^2} = \frac{4D}{g^2} = \frac{4N^2}{g^2} - \frac{4MP}{g^2} \equiv \frac{4N^2}{g^2} \pmod 4$ y entonces $\frac{4n^2}{g^2}$ sería $\equiv 2$ o $\equiv 3 \pmod 4$, Q.E.A, porque todo cuadrado debe ser congruente a cero o a la unidad según el módulo 4. Por lo tanto, el cociente $\frac{2n}{g}$ será necesariamente par, y así $\frac{n}{g}$ es un entero, es decir, g un divisor de n.

Entonces es claro que 1 es siempre un valor de m, es decir, que la ecuación $t^2 - Du^2 = 1$ es resoluble de la manera precedente para cualquier valor no cuadrado

positivo de D; 2 será un valor de m sólo si D es de la forma $4k$ o $4k+1$.

2) Si m es mayor que 2 pero es todavía un número idóneo, la solución de la ecuación $t^2 - Du^2 = m^2$ puede reducirse a la solución de una ecuación similar en la cual m es 1 o 2. Así, poniendo $D = n^2 D'$, si m divide a n, m^2 dividirá a D. Entonces si suponemos que los valores menores de p y q en la ecuación $p^2 - \frac{D}{m^2}q^2 = 1$ son $p = P$ y $q = Q$, los valores menores de t y u en la ecuación $t^2 - Du^2 = m^2$ serán $t = mP$ y $u = Q$. Pero si m no divide a n, al menos dividirá a $2n$ y será ciertamente par, y $4D/m^2$ será un entero. Entonces, si se encuentra que los valores menores de p y q en la ecuación $p^2 - \frac{4D}{m^2}q^2 = 4$ son $p = P$ y $q = Q$, los valores menores de t y u en la ecuación $t^2 - Du^2 = m^2$ serán $t = \frac{m}{2}P$ y $u = Q$. En cualquier caso, sin embargo, podrán deducirse no sólo los valores menores de t y u por el conocimiento de los valores menores de p y q, sino que, por este método podrán deducirse *todos* los valores del anterior de *todos* los valores del último.

3) Designemos por t^0, u^0; t', u'; t'', u'', etc. a todos los valores positivos de t y u, en la ecuación $t^2 - Du^2 = m^2$ (como en el artículo precedente). Si resulta que cualesquiera valores en la serie son congruentes a los primeros valores según un módulo dado r, por ejemplo si $t^\rho \equiv t^0$ (o $\equiv m$), $u^\rho \equiv u^0$ o $\equiv 0 \pmod{r}$, y si al mismo tiempo los valores siguientes son congruentes a los segundos valores, i.e.,

$$t^{\rho+1} \equiv t', \qquad u^{\rho+1} \equiv u' \pmod{r}$$

se tendrá también que

$$t^{\rho+2} \equiv t'', \quad u^{\rho+2} \equiv u''; \qquad t^{\rho+3} \equiv t''', \quad u^{\rho+3} \equiv u'''; \text{ etc.}$$

Esto puede deducirse facilmente porque cada serie t^0, t', t'', etc., u^0, u', u'', etc. es una serie recurrente; esto es así puesto que

$$t'' = \frac{2T}{m}t' - t^0, \qquad t^{\rho+2} = \frac{2T}{m}t^{\rho+1} - t^\rho$$

será

$$t'' \equiv t^{\rho-2}$$

y similarmente para el resto. Entonces se sigue que en general

$$t^{h+\rho} \equiv t^h, \qquad u^{h+\rho} \equiv u^h \pmod{r}$$

donde h es cualquier número; e incluso, más generalmente, si

$$\mu \equiv \nu \pmod{\rho}, \qquad \text{entonces} \quad t^\mu \equiv t^\nu, \quad u^\mu \equiv u^\nu \pmod{r}$$

4) Podemos siempre satisfacer las condiciones requeridas por la observación precedente; esto es, siempre puede encontrarse un índice ρ (para cualquier módulo dado r) para el cual sean

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u'$$

Para mostrar esto, observamos:

Primero, que la tercera condición siempre puede satisfacerse. Pues por los criterios dados en 1) es claro que la ecuación $p^2 - r^2Dq^2 = m^2$ es resoluble, y si se supone que los valores positivos menores de p y q (excepto m y 0) son P y Q, manifiestamente $t = P$ y $u = rQ$ estará entre los valores de t y u. Por lo tanto P y rQ estarán contenidos en las sucesiones t^0, t', etc., u^0, u', etc., y si $P = t^\lambda$ y $rQ = u^\lambda$ tendremos $u^\lambda \equiv 0 \equiv u^0 \pmod{r}$. Más aún, se ve que entre u^0 y u^λ no existirá ningún término que sea congruente a u^0 según el módulo r.

Segundo, si las otras tres condiciones se cumplen, es decir, si $u^{\lambda+1} \equiv u'$, $t^\lambda \equiv t^0$, $t^{\lambda+1} \equiv t'$, entonces se debe poner $\rho = \lambda$. Pero, si una u otra de estas condiciones no se cumple, podemos con certeza poner $\rho = 2\lambda$. En efecto, de la ecuación [1] y las fórmulas generales para t^e y u^e del artículo precedente se deduce

$$t^{2\lambda} = \frac{1}{m}(t^{2\lambda} + Du^{2\lambda}) = \frac{1}{m}(m^2 + 2Du^{2\lambda})$$

y entonces

$$\frac{t^{2\lambda} - t^0}{r} = \frac{2Du^{2\lambda}}{mr}$$

Esta cantidad será un entero porque por hipótesis r divide a u^λ y m^2 divide a $4D$ y, así, m divide a $2D$. Más aún $u^{2\lambda} = \frac{2}{m}t^\lambda u^\lambda$, y puesto que

$$4t^{2\lambda} = 4Du^{2\lambda} + 4m^2$$

es entonces divisible por m^2, $2t^\lambda$ será divisible por m y entonces $u^{2\lambda}$ por r o

$$u^{2\lambda} \equiv u^0 \pmod{r}$$

En el tercer lugar se encuentra

$$t^{2\lambda+1} = t' + \frac{2Du^{2\lambda+1}}{m}$$

y puesto que, por una razón similar, $\frac{2Du^{\lambda}}{mr}$ es un entero, se tendrá

$$t^{2\lambda+1} \equiv t' \pmod{r}$$

Finalmente se encuentra que

$$u^{2\lambda+1} = u' + \frac{2t^{\lambda+1}u^{\lambda}}{m}$$

y puesto que $2t^{\lambda+1}$ es divisible por m y u^{λ} por r, tenemos que

$$u^{2\lambda+1} \equiv u' \pmod{r}. \quad Q.\ E.\ D.$$

La utilidad de las últimas dos observaciones aparecerá en lo siguiente.

202.

Un caso particular del problema de resolver la ecuación $t^2 - Du^2 = 1$ ya ha sido tratado por geómetras del último siglo. El extremadamente agudo geómetra Fermat propuso el problema a los analistas ingleses, y Wallis atribuyó el descubrimiento de la solución a Brounker, y reportó éste en el capítulo 98 de su *Algebra*, *Opera T.* II, *p.* 418 y siguientes. Ozanam afirma que fue Fermat; y Euler, que trató de él en *Comm. Petr. VI p.* 175, *Comm. nov. XI, p.* 28 *), *Algebra P.* 2, *p.* 226, *Opusc. An. I, p.* 310, afirma que Pell fue el descubridor, y por esa razón se llama el problema de Pell por algunos autores. Todas estas soluciones coinciden esencialmente con lo que obtenemos si en el artículo 198 usamos la forma reducida con $a = 1$; pero nadie antes de Lagrange mostró que la operación necesariamente termina, es decir que el

*) En este comentario el algoritmo que consideramos en el artículo 27 se presenta con una notación similar. No lo reconocimos así en aquel momento.

problema es *realmente resoluble**). Consúltese *Mélanges de la Soc. de Turin, T.* 4, *p.* 19; y para una presentación más elegante *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. También hay una investigación de esta cuestión en el apéndice del *Algebra* de Euler, que hemos frecuentemente recomendado. Además nuestro método (partiendo de principios totalmente diferentes y no estando restringidos al caso de $m = 1$) nos da muchas formas de obtener una solución porque en el artículo 198 podemos empezar de cualquier forma reducida $(a, b, -a')$.

203.

PROBLEMA. *Si las formas* Φ *y* φ *son equivalentes, exhibir todas las transformaciones de una en la otra.*

Solución. Cuando estas formas son equivalentes de una sola manera (i.e., ya sea sólo propiamente o sólo impropiamente), por el artículo 196 se busca una transformación α, β, γ, δ de la forma φ en Φ, y es claro que todas las otras son similares a ésta. Pero cuando φ y Φ son equivalentes propia e impropiamente se buscan dos transformaciones disímiles (i.e., una propia, y la otra impropia) α, β, γ, δ; y α', β', γ', δ'; y cualquier otra transformación será similar a una de éstas. Si la forma φ es (a, b, c), su determinante es $= D$, m es el máximo común divisor de los números a, $2b$, c (como siempre fue el caso arriba), y t y u representan números indeterminados que satisfacen la ecuación $t^2 - Du^2 = m^2$, entonces en el primer caso todas las transformaciones de la forma φ en Φ estarán contenidas en la primera de las fórmulas, y en el último caso en la I o en la II.

$$\begin{array}{lll}
\text{I} \ . \ . \ . \ . & \frac{1}{m}\left(\alpha t - (\alpha b + \gamma c)u\right), & \frac{1}{m}\left(\beta t - (\beta b + \delta c)u\right) \\
& \frac{1}{m}\left(\gamma t + (\alpha a + \gamma b)u\right), & \frac{1}{m}\left(\delta t + (\beta a + \delta b)u\right) \\
\text{II} \ . \ . \ . \ . & \frac{1}{m}\left(\alpha' t - (\alpha' b + \gamma' c)u\right), & \frac{1}{m}\left(\beta' t - (\beta' b + \delta' c)u\right) \\
& \frac{1}{m}\left(\gamma' t + (\alpha' a + \gamma' b)u\right), & \frac{1}{m}\left(\delta' t + (\beta' a + \delta' b)u\right)
\end{array}$$

Ejemplo. Se desean todas las transformaciones de la forma $(129, 92, 65)$ en la forma $(42, 59, 81)$. Encontramos, en el artículo 195, que éstas son sólo impropiamente

*) Lo que Wallis, pp. 427–28, propuso para este objetivo no tiene peso. El paralogismo consiste en que, en la p. 428, línea 4, el presupone que, dada una cantidad p, pueden encontrarse enteros a y z tal que $\frac{z}{a}$ sea menor que p y que la diferencia sea menor que un número *asignado*. Esto es cierto cuando la diferencia *asignada* es una *cantidad dada* pero no cuando, como sucede en el presente caso, depende de a y z, y entonces es variable.

equivalentes y, en el artículo siguiente, que la transformación impropia de la primera en la última es -47, -56, 73, 87. Por lo tanto todas las transformaciones de la forma $(129, 92, 65)$ en $(42, 59, 81)$ serán expresadas por la fórmula

$$-(47t + 421u), \quad -(56t + 503u), \quad 73t + 653u, \quad 87t + 780u$$

donde t y u son todos los números que satisfacen la ecuación $t^2 - 79u^2 = 1$; y éstos están expresados por la fórmula

$$\pm t = \frac{1}{2}((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e)$$
$$\pm u = \frac{1}{2\sqrt{79}}((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e)$$

donde e representa a todos los enteros no negativos.

204.

Es claro que una fórmula general que represente a todas las transformaciones sería *más simple* si la transformación inicial de la cual se deduce la fórmula es más simple. Ahora, puesto que no importa desde cuál transformación empecemos, muy frecuentemente la fórmula general puede simplificarse si desde la primera fórmula encontrada deducimos una transformación menos compleja dando valores específicos a t y u, y usando esto para producir otra fórmula. Entonces, e.g., en la fórmula encontrada en el artículo precedente, al poner $t = 80$, $u = -9$, resulta una transformación que es más simple que la que encontramos. De esta forma obtenemos la transformación 29, 47, -37, -60 y la fórmula general $29t - 263u$, $47t - 424u$, $-37t + 337u$, $-60t + 543u$. Cuando, entonces, por medio de los preceptos precedentes la fórmula general es encontrada, podrá probarse si la transformación obtenida es más simple o no que aquélla de la que la fórmula fue deducida, dándole a t y u los valores específicos $\pm t'$, $\pm u'$; $\pm t''$, $\pm u''$, etc., y en este caso podrá derivarse una fórmula más simple de esa transformación. Pero qué constituye simpleza es todavía un principio arbitrario. Si fuera útil, podríamos encontrar una norma fija y asignar *límites* en las series t', u'; t'', u'', etc., más allá de las cuales las transformaciónes lleguen a ser contínuamente menos simples. Entonces no habría necesidad de buscar más y bastaría confinar nuestra búsqueda dentro de estos límites; no obstante, por brevedad suspendimos esta investigación porque muy frecuentemente mediante los métodos prescritos por nosotros surge la transformación más simple, ya sea inmediatamente o usando los valores $\pm t'$ y $\pm u'$ para t y u.

205.

PROBLEMA. *Encontrar todas las representaciones de un número dado M por una fórmula dada $ax^2 + 2bxy + cy^2$ cuyo determinante no cuadrado positivo es $= D$.*

Solución. Primero observamos que la investigación de representaciones por valores de x e y que no son primos relativos se puede reducir al caso (art. 181) de formas con determinante negativo donde se buscaron las representaciones por valores relativamente primos de las incógnitas. No hay necesidad de repetir aquí el argumento. Ahora, para representar M por valores primos relativos de x e y se requiere que D sea un residuo cuadrático de M, y si todos los valores de la expresión $\sqrt{D}$ (mod. M) son N, $-N$, N', $-N'$, N'', $-N''$, etc. (podemos escogerlos tal que ninguno sea $> \frac{1}{2}M$), entonces cualquier representación del número M por la forma dada pertenecerá a uno de estos valores. Antes de todo, se debe buscar estos valores y después investigar las representaciones que pertenecen a cada uno de ellos. No habrá ninguna representación que pertenezca al valor de N a no ser que las formas (a, b, c) y $(M, N, \frac{N^2-D}{M})$ sean propiamente equivalentes; si lo son, se busca una transformación propia α, β, γ, δ de la primera en la segunda. Entonces tendremos una representación del número M por la forma (a, b, c) perteneciente al valor N, poniendo $x = \alpha$ e $y = \gamma$, y todas las representaciones pertenecientes a este valor estarán expresadas por la fórmula

$$x = \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u), \qquad y = \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u)$$

donde m es el máximo común divisor de los números a, $2b$, c y t, u representan en general a todos los números que satisfacen la ecuación $t^2 - Du^2 = m^2$. Pero, manifiestamente esta fórmula general será más simple si la transformación α, β, γ, δ de la que fue deducida es más simple. Entonces será útil encontrar, según el artículo precedente, la transformación más simple de la forma (a, b, c) en $(M, N, \frac{N^2-D}{M})$ y deducir la fórmula de ésta. Exactamente de la misma manera podemos producir fórmulas generales para representaciones pertenecientes a los valores restantes $-N$, N', $-N'$ etc. (si efectivamente existe alguno).

Ejemplo. Se buscan todas las representaciones del número 585 por la fórmula $42x^2 + 62xy + 21y^2$. En relación con las representaciones por valores de x e y que no son primos relativos, es inmediatamente evidente que no puede haber otros de este tipo excepto aquéllos en los cuales el máximo común divisor de x e y sea 3, porque 585 es divisible sólo por un cuadrado, 9. Cuando encontramos, entonces, todas las representaciones del número $\frac{585}{9}$, i.e. 65 por la forma $42x'^2 + 62x'y' + 21y'^2$ con x' e y' primos relativos, podemos derivar todas las representaciones del número 585 por

la forma $42x^2 + 62xy + 21y^2$ no siendo x e y primos relativos, poniendo $x = 3x'$ e $y = 3y'$. Los valores de la expresión $\sqrt{79}$ (mod. 65) son ± 12 y ± 27. Se encuentra que la representación del número 65 perteneciente al valor -12 es $x' = 2$ e $y' = -1$. Por lo tanto todas las representaciones de 65 pertenecientes a este valor estarán expresadas por la fórmula $x' = 2t - 41u$, $y' = -t + 53u$ y *de esto* todas las representaciones de 585 por la fórmula $x = 6t - 123u$, $y = -3t + 159u$. De manera similar encontramos que la fórmula general para todas las representaciones del número 65 pertenecientes al valor 12 es $x' = 22t - 199u$, $y' = -23t + 211u$; y la fórmula para todas las representaciones del número 585 derivadas de esto será $x = 66t - 597u$, $y = -69t + 633u$. Pero, no existe una representación del número 65 perteneciente a los valores $+27$ y -27. Para encontrar representaciones del número 585 por valores x e y primos entre sí, debemos primero calcular los valores de la expresión $\sqrt{79}$ (mod. 585), los cuales son ± 77, ± 103, ± 157, ± 248. No existe ninguna representación perteneciente a los valores ± 77, ± 103 y ± 248, pero la representación $x = 3$, $y = 1$ pertenece al valor -157, y podemos deducir la fórmula general para todas las representaciones pertenecientes a este valor: $x = 3t - 114u$, $y = t + 157u$. Similarmente encontramos la representación $x = 83$, $y = -87$ perteneciente a $+157$, y la fórmula en la que todas las respresentaciones similares están contenidas es $x = 83t - 746u$, $y = -87t + 789u$. Tenemos entonces cuatro fórmulas generales en las que están contenidas todas las representaciones del número 585 por la forma $42x^2 + 62xy + 21y^2$:

$$\begin{aligned} x &= 6t - 123u \qquad & y &= -3t + 159u \\ x &= 66t - 597u \qquad & y &= -69t + 633u \\ x &= 3t - 114u \qquad & y &= t + 157u \\ x &= 83t - 746u \qquad & y &= -87t + 789u \end{aligned}$$

donde t y u representan en general todos los enteros que satisfacen la ecuación $t^2 - 79u^2 = 1$.

Por brevedad no nos detendremos en aplicaciones especiales del análisis precedente sobre formas con determinante no cuadrado positivo. Cualquiera podrá tener su propia lucha con éstas imitando el método de los artículos 176 y 182. Nos vamos a apresurar inmediatamente a considerar formas con determinante cuadrado positivo, que es el único caso que falta.

Formas de determinante cuadrado.

206.

PROBLEMA. *Dada la forma* (a, b, c) *con el determinante cuadrado* h^2*, donde* h *es la raíz positiva, encontrar una forma* (A, B, C) *que sea propiamente equivalente a ella, en la que* A *esté entre los límites* 0 *y* $2h - 1$ *inclusive,* B *sea* $= h$*,* $C = 0$*.*

Solución. I. Puesto que $h^2 = b^2 - ac$, tenemos $(h - b) : a = c : -(h + b)$. Sea $\beta : \delta$ igual a esta razón de modo que β sea primo a δ, y determínense α y γ tal que $\alpha\delta - \beta\gamma = 1$, lo cual puede hacerse. Por la sustitución α, β, γ, δ, la forma (a, b, c) será transformada en (a', b', c'), la cual será propiamente equivalente. Entonces se tendrá

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ &= (h - b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h + b)\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \\ &= (h - b)\beta\delta + 2b\beta\delta - (h + b)\beta\delta = 0 \end{aligned}$$

Más aún, si a' está entre los límites 0 y $2h - 1$, la forma (a', b', c') satisfará todas las condiciones.

II. Pero si a' está fuera de los límites 0 y $2h - 1$, sea A el residuo positivo mínimo de a' relativo al módulo $2h$ que manifiestamente estará entre esos límites y sea $A - a' = 2hk$. Entonces la forma (a', b', c'), i.e. $(a', h, 0)$ será transformada por la sustitución 1, 0, k, 1 en la forma $(A, h, 0)$ que será propiamente equivalente a las formas (a', b', c') y (a, b, c) y satisfará todas las condiciones. Por otra parte es claro que la forma (a, b, c) será transformada en la forma $(A, h, 0)$ por la sustitución $\alpha + \beta k$, β, $\gamma + \delta k$, δ.

Ejemplo. Considere la forma (27,15,8) cuyo determinante es $= 9$. Aquí $h = 3$ y $4 : -9$ es la razón con los términos menores que es igual a las razones $-12 : 27 = 8 : -18$. Por lo tanto, con $\beta = 4$, $\gamma = -9$, $\alpha = -1$, $\gamma = 2$, la forma (a', b', c') se convierte en $(-1, 3, 0)$, que va a la forma $(5, 3, 0)$ por la sustitución 1, 0, 1, 1. Esta es entonces la forma buscada, y la forma dada se transforma en ella por la sustitución propia 3, 4, -7, -9.

A tales formas (A, B, C), en las que $C = 0$, $B = h$, y A está entre los límites 0 y $2h - 1$, las llamaremos *formas reducidas*, que deben distinguirse de las formas reducidas que tienen un determinante negativo o no cuadrado positivo.