247.

De la solución del problema precedente, es manifiesto que si g es una forma primitiva del mismo orden y género que f, y g' es una forma primitiva del mismo orden y género que f': entonces la forma compuesta por g y g' será del mismo género que la forma compuesta por f y f'. Así se ve lo que significa un *género compuesto* por dos (o incluso varios) géneros. Además, si f y f' tienen el mismo determinante, f es una forma del género principal, y F está compuesta por f y f': entonces F será del mismo género que f'; de ahí que el género principal puede siempre ser omitido en la composición de otros géneros del mismo determinante. Es así como, siendo otras cosas iguales, si f no está en el género principal y f' es una forma primitiva, F ciertamente estará en un género que no es f'. Finalmente, si f y f' son formas propiamente primitivas del mismo género, F estará en el género principal; si, de hecho f y f' son ambas propiamente primitivas con el mismo determinante pero en distintos géneros, F no puede pertenecer al género principal. Y si una forma propiamente primitiva se compone *consigo misma*, la forma resultante, la cual también será propiamente primitiva con el mismo determinante, necesariamente pertenecerá al género principal.

248.

Problema. *Dadas dos formas cualesquiera, f y f' de las cuales F está compuesta: determinar el género de la forma F a partir de aquéllos de las formas f y f'.*

Solución. Sean $f = (a, b, c)$, $f' = (a', b', c')$ y $F = (A, B, C)$; de seguido, desígnase por $\mathfrak{m}$ el máximo común divisor de los números a, b, c y por $\mathfrak{m}'$ el maximo común divisor de los números a', b', c', de modo que las formas f y f' sean derivadas de las formas primitivas $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$ y $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$, las que designaremos por $\mathfrak{f}$ y $\mathfrak{f}'$ respectivamente. Ahora si al menos una de las formas $\mathfrak{f}$ o $\mathfrak{f}'$ es propiamente primitiva, el máximo común divisor de los números A, B, C será $\mathfrak{m}\mathfrak{m}'$, y por ende F será derivado de la forma primitiva $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}) \ldots \mathfrak{F}$ y es claro que el género de la forma F dependerá del de la forma $\mathfrak{F}$. Es fácil ver que si $\mathfrak{F}$ es transformado en $\mathfrak{f}\mathfrak{f}'$ por la misma sustitución que transforma a F en ff' y de tal modo que $\mathfrak{F}$ está compuesto por $\mathfrak{f}$ y $\mathfrak{f}'$, su género puede ser determinado por el problema del artículo 246. Pero si ambas $\mathfrak{f}$ y $\mathfrak{f}'$ son impropiamente primitivas, el máximo común divisor de los números A, B, C será $2\mathfrak{m}\mathfrak{m}'$, y la forma $\mathfrak{F}$, que está todavía compuesta por $\mathfrak{f}$ y $\mathfrak{f}'$, será manifiestamente derivada de la forma propiamente primitiva $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$. El género de esta

forma puede ser determinado por el artículo 246 y dado que F está derivado de la misma manera, su género será conocido asímismo.

A partir de esta solución es manifiesto que el teorema en el artículo precedente, que ha sido restringido a las formas primitivas, es válido para cualquier forma, a saber: *si f' y g' son de los mismos géneros respectivamente que f y g, la forma compuesta por f' y g' será del mismo género que la forma compuesta por f y g.*

Composición de Clases.

249.

TEOREMA. *Si las formas f y f' son de los mismos órdenes, géneros y clases que g y g' respectivamente, entonces la forma compuesta por f y f' será de la misma clase que la forma compuesta por g y g'.*

De este teorema (cuya verdad se sigue inmediatamente del artículo 239) es evidente lo que queremos decir cuando hablamos de una *clase compuesta por dos (o más) clases dadas.*

Si cualquier clase K está compuesta con una clase principal, el resultado será la clase K misma; esto es, en composición con otras clases del mismo determinante una clase principal puede ser ignorada. De la composición de dos clases propiamente primitivas opuestas siempre obtendremos una clase principal del mismo determinante (véase artículo 243). Dado que por este motivo cualquier clase ambigua es opuesta a sí misma, siempre obtendremos una clase principal del mismo determinante si componemos cualquier clase propiamente primitiva ambigua consigo misma.

El recíproco de la última proposición también vale; esto es *si de la composición de una clase K propiamente primitiva consigo misma proviene una clase principal H con el mismo determinante, K necesariamente será una clase ambigua.* Puesto que si K' es una clase opuesta a K, la misma clase surgirá de la composición de H y K' como de las tres clases K, K y K'; a partir de las últimas proviene K (dado que K y K' producen a H, y H y K producen a K). De las primeras obtenemos K'; de ahí que K y K' coinciden y la clase es ambigua.

Ahora se nota la proposición siguiente: *Si las clases K y L son opuestas a las clases K' y L' respectivamente, la clase compuesta por K y L será opuesta a la clase compuesta por K' y L'.* Sean f, g, f' y g' las formas de las clases K, L, K' y L' respectivamente, y sea F compuesta por f y g, y F' compuesta por f' y g'. Dado que f' es impropiamente equivalente a f, y g' impropiamente equivalente a g, mientras que F está compuesto por ambas f y g directamente: F estará también compuesta

por f' y g' pero con cada una de ellas indirectamente. De este modo cualquier forma que es impropiamente equivalente a F estará compuesta por f' y g' directamente y así será propiamente equivalente a F' (art. 238, 239). De ahí que F y F' serán impropiamente equivalentes y las clases a las que pertenecen son opuestas.

Sigue de esto que, si se compone una clase ambigua K con una clase ambigua L, siempre se produce una clase ambigua. En efecto, ella será opuesta a la clase que es compuesta de las clases opuestas a K y L; a saber, a sí misma, ya que estas clases son opuestas a sí mismas.

Finalmente observamos que si se proponen dos clases cualesquiera K y L del mismo determinante y la primera es propiamente primitiva, siempre podemos encontrar una clase M con el mismo determinante tal que L esté compuesta por M y K. Manifiestamente esto puede hacerse tomando por M la clase que está compuesta por L y la clase opuesta a K; es fácil ver que esta clase es la única que disfruta de esta propiedad; es decir, si componemos diferentes clases del mismo determinante con la misma clase propiamente primitiva, se producen distintas clases.

Es conveniente denotar la composición de clases por el signo de adición, $+$, y la identidad de clases por el signo de igualdad. Usando estos signos la proposición recién considerada puede ser enunciada como sigue: Si la clase K' es opuesta a K, $K+K'$ será una clase principal del mismo determinante, de modo que $K+K'+L = L$; si se toma $K' + L = M$, tenemos $K + M = L$, como se desea. Ahora, si además de M tenemos otra clase M' con la misma propiedad, esto es $K + M' = L$, tendremos $K+K'+M' = L+K' = M$ y así $M' = M$. Si muchas clases idénticas son compuestas, esto puede indicarse (como en la multiplicación) prefijando su número, así que $2K$ significa lo mismo que $K + K$, $3K$ lo mismo que $K + K + K$, etc. Podríamos también transferir los mismos signos a formas de tal modo que $(a, b, c) + (a', b', c')$ indicaría a la forma compuesta por (a, b, c) y (a', b', c'); pero para evitar ambigüedad preferimos no usar esta abreviación, especialmente puesto que ya habíamos asignado un significado especial al símbolo $\sqrt{M}(a, b, c)$. Diremos que la clase $2K$ surge de la *duplicación* de la clase K, la clase $3K$ de la *triplicación*, etc.

250.

Si D es un número divisible por m^2 (suponemos a m positivo), habrá un orden de formas de determinante D derivado del orden propiamente primitivo del determinante $\frac{D}{m^2}$ (cuando D es negativo habrá *dos* de ellos, uno positivo y uno negativo); manifiestamente la forma $(m, 0, -\frac{D}{m})$ pertenecerá a aquel orden (el

positivo) y puede ser correctamente considerada la *forma más simple* en el orden (justo como $(-m,\, 0,\, \frac{D}{m})$ será la más simple en el orden negativo cuando D es negativo). Si además tenemos $\frac{D}{m^2} \equiv 1 \pmod 4$, habrá también un orden de formas de determinante D derivado del determinante impropiamente primitivo $\frac{D}{m^2}$. La forma $(2m,\, m,\, \frac{m^2-D}{2m})$ pertenecerá a éste y será la más simple en el orden. (Cuando D es negativo, habrá de nuevo dos órdenes y en el orden negativo $(-2m,\, -m,\, \frac{D-m^2}{2m})$ será la forma más simple.) Así, e.g., si aplicamos esto al caso donde $m = 1$, el siguiente será el más simple entre los cuatro órdenes de formas con determinante 45; $(1,\, 0,\, -45)$, $(2,\, 1,\, -22)$, $(3,\, 0,\, -15)$, $(6,\, 3,\, -6)$.

Todas estas consideraciones dan lugar a lo siguiente.

PROBLEMA. *Dada cualquier forma F del orden O, encontrar una forma propiamente primitiva (positiva) del mismo determinante que produzca F cuando está compuesta con la forma más simple en O.*

Solución. Sea la forma $F = (ma,\, mb,\, mc)$ derivada de la forma primitiva $f = (a,\, b,\, c)$ de determinante d y supondremos *primero* que f es propiamente primitiva. Observamos que si a y $2dm$ no son primos entre sí, ciertamente hay otras formas propiamente equivalentes a $(a,\, b,\, c)$ cuyos primeros términos tienen esta propiedad. Debido al artículo 228, hay números primos a $2dm$ representables por esta forma. Sea tal número $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ y supondremos (es legítimo hacerlo) que α y γ son primos entre sí. Ahora si escogemos β y δ tales que $\alpha\delta - \beta\gamma = 1$, f será transformada por la sustitución $\alpha,\, \beta,\, \gamma,\, \delta$ en la forma $(a',\, b',\, c')$ que es propiamente equivalente a ella y tiene la propiedad prescrita. Ahora, dado que F y $(a'm,\, b'm, c'm)$ son propiamente equivalentes es suficiente considerar el caso donde a y $2dm$ son relativamente primos. Ahora $(a,\, bm,\, cm^2)$ será una forma propiamente primitiva del mismo determinante que F (pues si $a, 2bm, cm^2$ tuvieran un divisor común, también significaría que él divide a $2dm = 2b^2m - 2acm$). Es fácil confirmar que F será transformada en el producto de las formas $(m,\, 0,\, -dm)$ y $(a,\, bm,\, cm^2)$ por la sustitución $1,\, 0,\, -b,\, -cm;\ 0,\, m,\, a,\, bm$. Note que, a no ser que F sea una forma negativa, $(m,\, 0,\, -dm)$ será la forma más simple del orden O. Usando el criterio de la cuarta observación en el artículo 235, se concluye que F está compuesta por $(m,\, 0,\, -dm)$ y $(a,\, bm,\, cm^2)$. Cuando de todos modos F es una forma negativa, será transformada por la sustitución $1,\, 0,\, b,\, -cm;\ 0,\, -m,\, -a,\, bm$ en el producto de $(-m,\, 0,\, dm)$, la forma más simple del mismo orden, y la forma positiva $(-a,\, bm,\, -cm^2)$ y así estará compuesta por estas dos.

Segundo, si f es una forma impropiamente primitiva, se puede suponer que

$\frac{1}{2}a$ y $2dm$ son primos entre sí; pues si esta propiedad no es cierta ya, de la forma f se puede encontrar una forma propiamente equivalente a f que tenga la propiedad. De esto se sigue fácilmente que $(\frac{1}{2}a,\ bm,\ 2cm^2)$ es una forma propiamente primitiva del mismo determinante que F; y es igualmente fácil confirmar que F será transformada en el producto de las formas

$$(\pm 2m,\ \pm m,\ \pm\frac{1}{2}(m - dm)) \quad \text{y} \quad (\pm\frac{1}{2}a,\ bm,\ \pm 2cm^2)$$

por la sustitución

$$1,\ 0,\ \frac{1}{2}(1 \mp b),\ -cm \quad ; \quad 0,\ \pm 2m,\ \pm\frac{1}{2}a,\ (b+1)m$$

donde los signos inferiores deben ser tomados cuando F es una forma negativa y los signos superiores en caso contrario. Concluimos que F está compuesta por estas dos formas y la primera es la más simple de orden O, la última es una forma propiamente primitiva (positiva).

251.

PROBLEMA. *Dadas dos formas F y f del mismo determinante D y pertenecientes al mismo orden O: encontrar una forma propiamente primitiva de determinante D que produzca a F cuando ésta esté compuesta con f.*

Solución. Sea φ la forma más simple de orden O; $\mathfrak{F}$ y $\mathfrak{f}$ formas propiamente primitivas de determinante D que producen a F y f respectivamente cuando están compuestas con φ; y sea f' la forma propiamente primitiva que produce a $\mathfrak{F}$ cuando está compuesta con $\mathfrak{f}$. Entonces la forma F estará compuesta de las tres formas φ, $\mathfrak{f}$ y f' ó de las dos formas f y f'. *Q. E. I.*

De ahí que toda clase de un orden dado puede ser considerada como compuesta por cualquier clase dada del mismo orden y otra clase propiamente primitiva del mismo determinante.

Para un determinante dado existe el mismo número de clases en cada género del mismo orden.

252.

TEOREMA. *Para un determinante dado existe el mismo número de clases en cada género del mismo orden.*

Demostración. Suponga que los géneros G y H pertenecen al mismo orden, que G está compuesta por n clases K, K', K'', $\ldots K^{n-1}$ y que L es cualquier clase del género H. Por el artículo precedente se encuentra una clase propiamente primitiva M del mismo determinante cuya composición con K produce a L, y se designan por L', L'', $\ldots L^{n-1}$ a las clases que surgen de la composición de la clase M con K', K'', $\ldots K^{n-1}$ respectivamente. Entonces a partir de la última observación del artículo 249, se sigue que todas las clases L, L', L'', $\ldots L^{n-1}$ son distintas, y por el artículo 248 que todas ellas pertenecen al mismo género H. Finalmente es fácil ver que H no puede contener ninguna otra clase más que éstas, dado que cada clase del género H puede ser considerada como compuesta por M y otra clase del mismo determinante, y éste necesariamente debe ser del género G. De ahí que H, como G, contendrá n clases distintas. *Q. E. D.*

Se compara el número de clases contenidas
en géneros individuales de órdenes distintos.

253.

El teorema precedente supone la identidad del orden y no puede ser extendido a distintos órdenes. Así por ejemplo para el determinante -171 hay 20 clases positivas que son reducidas a cuatro órdenes: en el orden propiamente primitivo hay dos géneros y cada cual contiene seis clases; en el orden impropiamente primitivo dos géneros tienen cuatro clases, dos en cada cual; en el orden derivado a partir del orden propiamente primitivo de determinante -19 hay sólo un género que contiene tres clases; finalmente, el orden derivado del orden impropiamente primitivo de determinante -19 tiene un género con una clase. Lo mismo es cierto para las clases negativas. Es útil, por ende, inquirir sobre el principio general que gobierna la relación entre el número de clases en órdenes diferentes. Supóngase que K y L son dos clases del mismo orden (positivo) O de determinante D, y M es una clase propiamente primitiva del mismo determinante que produce a L cuando está compuesta con K. Por el artículo 251 tal clase siempre puede ser encontrada. Ahora bien, en algunos casos ocurre que M es la *única* clase propiamente primitiva con esta propiedad; en otros casos puede existir varias clases propiamente primitivas con esta propiedad. Supongamos en general que hay r clases propiamente primitivas de este tipo M, M', M'', $\ldots M^{r-1}$ y que cada uno de ellas produce a L cuando está compuesta con K. Designaremos este conjunto por la letra W. Ahora sea L' otra clase del orden O (distinta de la clase L), y sea N' una clase propiamente primitiva

de determinante D la cual resulta en L' cuando está compuesta con L. Usaremos W' para designar el conjunto de las clases $N'+M$, $N'+M'$, $N'+M''$, $\ldots N'+M^{r-1}$ (todas éstas serán propiamente primitivas y distintas una de la otra). Es fácil ver que K producirá a L' si ésta está compuesta con cualquier otra clase de W', y por eso concluimos que W y W' no tienen clases en común; y cada clase propiamente primitiva que produzca a L' cuando esté compuesta con K está contenida en W'. De la misma manera, si L'' es otra clase de orden O distinta de L y L', entonces habrá r formas propiamente primitivas todas distintas una de la otra y de las formas en W y W', cada una de ellas producirá a L'' cuando esté compuesta con K. Lo mismo es cierto para todas las otras clases del orden O. Ahora bien, dado que cualquier clase propiamente primitiva (positiva) de determinante D produce una clase de orden O cuando está compuesta con K, es claro que si el número de todas las clases de orden O es n, el número de todas las clases propiamente primitivas (positivas) del mismo determinante será rn. De este modo tenemos una regla general: Si denotamos por K y L dos clases cualesquiera de orden O y por r el número de clases propiamente primitivas distintas pero del mismo determinante, cada una de las cuales produce a L cuando está compuesta con K, entonces el número de todas las clases en el orden propiamente primitivo (positivo) será r veces mayor que el número de clases de orden O.

Dado que en el orden O las clases K y L pueden ser escogidas arbitrariamente, es permisible tomar clases idénticas y será particularmente ventajoso escoger aquella clase que contenga a la forma más simple de este orden. Si, por esta razón, escogemos aquella clase para K y L, la operación se verá reducida a asignar todas las clases propiamente primitivas que producen a K misma cuando estén compuestas con K. Desarrollaremos este método en lo que sigue.

254.

Teorema. *Si $F=(A, B, C)$ es la forma más simple de orden O y de determinante D, y $f=(a, b, c)$ es una forma propiamente primitiva del mismo determinante: entonces el número A^2 puede ser representado por esta forma siempre y cuando F resulte de la composición de las formas f y F; y recíprocamente F estará compuesta por sí misma y f si A^2 puede ser representada por f.*

Demostración. I. Si F es transformada en el producto $f\,F$ por la sustitución

p, p', p'', p'''; q, q', q'', q''' luego, por el artículo 235, tendremos

$$A(aq''^2 - 2bqq'' + cq^2) = A^3$$

y por ende

$$A^2 = aq''^2 - 2bqq'' + cq^2 \qquad Q.\ E.\ P.$$

II. *Presumiremos* que A^2 puede ser representado por f y designaremos los valores desconocidos por medio de los cuales es hecho esto como q'', $-q$; esto es, $A^2 = aq''^2 - 2bqq'' + cq^2$. Seguidamente póngase que

$$\begin{array}{lll} q''a - q(b+B) = Ap, & -qC = Ap', & q''(b-B) - qc = Ap'' \\ -q''C = Ap''', & q''a - q(b-B) = Aq', & q''(b+B) - qc = Aq''' \end{array}$$

Es fácil confirmar que F es transformada en el producto $f\,F$ por la sustitución p, p', p'', p'''; q, q', q'', q'''. Si los números p, p', etc. son enteros entonces F estará compuesta por f y F. Ahora, de la descripción de la forma más simple, B es 0 ó $\frac{1}{2}A$, así que $\frac{2B}{A}$ es un entero; de la misma manera es claro que $\frac{C}{A}$ es también siempre un entero. De este modo $q' - p$, p', $q''' - p''$ y p''' serán enteros y sólo queda probar que p y p'' son enteros. Ahora tenemos

$$p^2 + \frac{2pqB}{A} = a - \frac{q^2C}{A}, \qquad p''^2 + \frac{2p''q''B}{A} = c - \frac{q''^2C}{A}$$

Si $B = 0$ obtenemos

$$p^2 = a - \frac{q^2C}{A}, \qquad p''^2 = c - \frac{q''^2C}{A}$$

y así p y p'' son enteros; pero si $B = \frac{1}{2}A$ tenemos

$$p^2 + pq = a - \frac{q^2C}{A}, \qquad p''^2 + p''q'' = c - \frac{q''^2C}{A}$$

y en este caso también p y p'' son enteros. De ahí que F está compuesta por f y F. *Q. E. S.*

255.

Así, el problema se ve reducido a encontrar todas las clases propiamente primitivas de determinante D cuyas formas puedan representar a A^2. Manifiestamente A^2 puede ser representado por cualquier forma cuyo primer término es A^2 ó el cuadrado de un factor de A; recíprocamente si A^2 puede ser representado por la forma f, f será transformado en una forma cuyo primer término es $\frac{A^2}{e^2}$ por la sustitución α, β, γ, δ siempre y cuando asignemos αe y γe, cuyo máximo común divisor es e, como los valores de las incógnitas. Esta forma será propiamente equivalente a la forma f si β y δ son escogidas de tal modo que $\alpha\delta - \beta\gamma = 1$. Así resulta claro que en cualquier clase que tenga formas que puedan representar a A^2, se puede encontrar formas cuyo primer término es A^2 ó el cuadrado de un factor de A. El proceso entero depende entonces de encontrar todas las clases propiamente primitivas de determinante D que contengan formas de este tipo. Hacemos esto del siguiente modo. Sean a, a', a'' etc. todos los divisores (positivos) de A; ahora encuentre todos los valores de la expresión $\sqrt{D}$ (mod. a^2) entre 0 y $a^2 - 1$ inclusive y llámelos b, b', b'', etc. Haga

$$b^2 - D = a^2 c, \qquad b'^2 - D = a^2 c', \qquad b''^2 - D = a^2 c'', \quad \text{etc.}$$

y desígnese el conjunto de formas (a^2, b, c), (a^2, b', c'), etc. por la letra V. Obviamente cada clase de determinante D que tenga una forma con primer término a^2 también debe contener alguna forma de V. De un modo similar determinamos todas las formas de determinante D con primer término a'^2 y segundo término entre 0 y $a'^2 - 1$ inclusive y designamos el conjunto con la letra V'; por una construcción similar sea V'' el conjunto de formas similares cuyo primer término es a''^2 etc. Ahora elimine de V, V', V'', etc. todas las formas que no sean propiamente primitivas y reduzca el resto a clases. Si hubiera muchas formas que pertenecen a la misma clase, retenga sólo una de ellas. De este modo tendremos todas las clases que se buscan, y la razón de este número con respecto a la unidad será la misma que la razón del número de todas las clases propiamente primitivas (positivas) con respecto al número de todas las clases en el orden O.

Ejemplo. Sea $D = -531$ y O el orden positivo derivado a partir del orden propiamente primitivo de determinante -59; su forma más simple es $(6, 3, 90)$, así que $A = 6$. Aquí a, a', a'' y a''' serán 1, 2, 3 y 6, V contendrá a la forma $(1, 0, 531)$, V' contendrá a (4, 1, 133) y (4, 3, 135), V'' a (9, 0, 59), (9, 3, 60) y (9, 6, 63), y V''' a (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35) y (36, 33, 45). Pero de estas doce formas seis deben ser rechazadas, la segunda y la tercera de V'', la

primera, la tercera, la cuarta, y la sexta de V'''. Todas éstas son formas derivadas; todas las seis restantes pertenecen a distintas clases. De hecho el número de clases propiamente primitivas (positivas) de determinante -531 es 18; el número de clases propiamente primitivas (positivas) de determinante -59 (o el número de clases de determinante -531 derivadas de éstas) es 3, y así la razón es de 6 a 1.

256.

Esta solución se hará más clara por medio de las siguientes observaciones generales.

I. Si el orden O es derivado a partir de un orden propiamente primitivo, A^2 dividirá a D; pero si O es impropiamente primitivo o derivado a partir de un orden impropiamente primitivo, A será par, D será divisible por $\frac{1}{4}A^2$ y el cociente será $\equiv 1 \pmod 4$. Así el cuadrado de cualquier divisor de A dividirá a D o al menos a $4D$ y en el último caso el cociente será siempre $\equiv 1 \pmod 4$.

II. Si a^2 divide a D, todos los valores de la expresión $\sqrt{D} \pmod{a^2}$ que caen entre 0 y $a^2 - 1$ serán $0, a, 2a, \ldots a^2 - a$ y así a será el número de formas en V; pero entre ellas habrá sólo tantas formas propiamente primitivas como hayan números entre

$$\frac{D}{a^2}, \frac{D}{a^2} - 1, \frac{D}{a^2} - 4, \ldots \frac{D}{a^2} - (a-1)^2$$

que no tengan un divisor común con a. Cuando $a = 1$, V consistirá de sólo una forma $(1, 0, -D)$ que será siempre propiamente primitiva. Cuando a es 2 o una potencia de 2, la mitad de los a números será par, la mitad impar; por lo cual habrá $\frac{1}{2}a$ formas propiamente primitivas en V. Cuando a es cualquier otro número primo p o una potencia del número primo p, se deben distinguir tres casos: a saber, si $\frac{D}{a^2}$ no es divisible por p y no es un residuo cuadrático de p, todos estos a números serán relativamente primos a a de tal modo que todas las formas en V serán propiamente primitivas; pero si p divide a $\frac{D}{a^2}$ habrá $\frac{(p-1)a}{p}$ formas propiamente primitivas en V; finalmente si $\frac{D}{a^2}$ es un residuo cuadrático de p no divisible por p, habrá $\frac{(p-2)a}{p}$ formas propiamente primitivas. Todo esto puede ser demostrado sin ninguna dificultad. En general, si $a = 2^\nu p^\pi q^\chi r^\rho \ldots$ donde p, q, r etc. son números primos impares distintos,

el número de formas propiamente primitivas en V será $NPQR\ldots$, donde

$N = 1$ (si $\nu = 0$) ó $N = 2^{\nu-1}$ (si $\nu > 0$)
$P = p^{\pi}$ (si $\frac{D}{a^2}$ es un no residuo cuadrático de p) o
$P = (p-1)p^{\pi-1}$ (si $\frac{D}{a^2}$ es divisible por p) o
$P = (p-2)p^{\pi-1}$ (si $\frac{D}{a^2}$ es un residuo cuadrático de p no divisible por p)

y Q, R, etc. serán definidos de la misma manera por q, r, etc. como lo es P por p.

III. Si a^2 no divide a D, $\frac{4D}{a^2}$ será un entero y $\equiv 1 \pmod 4$ y los valores de la expresión $\sqrt{D} \pmod{a^2}$ serán $\frac{1}{2}a$, $\frac{3}{2}a$, $\frac{5}{2}a, \ldots a^2 - \frac{1}{2}a$. De ahí que el número de formas en V será a y habrá tantas propiamente primitivas entre ellas como haya números entre

$$\frac{D}{a^2} - \frac{1}{4}, \frac{D}{a^2} - \frac{9}{4}, \frac{D}{a^2} - \frac{25}{4}, \ldots \frac{D}{a^2} - \left(a - \frac{1}{2}\right)^2$$

que son relativamente primos a a. Toda vez que $\frac{4D}{a^2} \equiv 1 \pmod 8$, todos estos números serán pares y así no habrá ninguna forma propiamente primitiva en V; pero cuando $\frac{4D}{a^2} \equiv 5 \pmod 8$, todos estos números serán impares, de modo que todas las formas en V serán propiamente primitivas si a es 2 o una potencia de 2. En este caso, como una norma general, habrá tantas formas propiamente primitivas en V como haya números no divisibles por algún divisor primo impar de a. Habrá $NPQR\ldots$ de ellas si $a = 2^{\nu}p^{\pi}q^{\chi}r^{\rho}\ldots$. Aquí $N = 2^{\nu}$ y P, Q, R, etc. serán derivados a partir de p, q, r, etc. de la misma manera que en el caso precedente.

IV. Hemos, por tanto, mostrado cómo determinar el número de formas propiamente primitivas en V, V', V'', etc. Podemos encontrar el número total por medio de la siguiente regla general. Si $A = 2^{\nu}\mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma}\ldots$, donde $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. son números primos impares distintos, el número total de todas las formas propiamente primitivas en V, V', V'', etc. será $= \frac{A\mathfrak{n}\mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\cdots}$ donde

$\mathfrak{n} = 1$ (si $\frac{4D}{A^2} \equiv 1 \pmod 8$), o
$\mathfrak{n} = 2$ (si $\frac{D}{A^2}$ es un entero), o
$\mathfrak{n} = 3$ (si $\frac{4D}{a^2} \equiv 5 \pmod 8$); y
$\mathfrak{a} = \mathfrak{A}$ (si $\mathfrak{A}$ divide a $\frac{4D}{A^2}$), o
$\mathfrak{a} = \mathfrak{A} \pm 1$ (si $\mathfrak{A}$ no divide a $\frac{4D}{A^2}$; el signo superior e inferior se toma de acuerdo a si $\frac{4D}{A^2}$ es un no residuo o un residuo de $\mathfrak{A}$)

Finalmente, $\mathfrak{b}$, $\mathfrak{c}$, etc. serán derivados a partir de $\mathfrak{B}$, $\mathfrak{C}$, etc. de la misma manera que $\mathfrak{a}$ a partir de $\mathfrak{A}$. La brevedad no nos permite demostrar esto más completamente.

V. Ahora, con relación al número de clases que resultan de las formas propiamente primitivas en V, V', V'', etc., debemos distinguir entre los tres casos siguientes.

Primero, cuando D es un número negativo, cada una de las formas propiamente primitivas en V, V', etc. constituye una clase separada. Por eso el número de clases será expresado por la fórmula dada en la observación previa excepto por dos casos, más exactamente cuando $\frac{4D}{A^2}$ es $= -4$ ó $= -3$; esto es, cuando D es $= -A^2$ ó $= -\frac{3}{4}A^2$. Para probar este teorema solamente debemos mostrar que es imposible para dos formas de V, V', V'', etc. distintas, el ser propiamente equivalentes. Supongamos, por tanto, que $(h^2,\ i,\ k)$, $(h'^2,\ i',\ k')$ son dos formas propiamente primitivas de V, V', V'', etc., y ambas pertenecen a la misma clase. Y supongamos que la primera es transformada en la última por medio de la sustitución propia α, β, γ, δ; obtendremos las ecuaciones

$$\alpha\delta - \beta\gamma = 1, \qquad h^2\alpha^2 + 2i\alpha\gamma + k\gamma^2 = h'^2,$$
$$h^2\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i'$$

De esto es fácil concluir, *primero*, que γ ciertamente no es $= 0$ (y se sigue que $\alpha = \pm 1$, $h^2 = h'^2$, $i' \equiv i \pmod{h^2}$, y las formas propuestas son idénticas, contrario a la hipótesis); *segundo*, que γ es divisible por el máximo común divisor de los números h, h' (pues si hacemos este divisor $= r$, manifiestamente también éste divide a $2i$, $2i'$ y es relativamente primo a k; además, r^2 divide a $h^2k - h'^2k' = i^2 - i'^2$; obviamente entonces r debe también dividir a $i - i'$; pero $\alpha i' - \beta h'^2 = \alpha i + \gamma k$ de modo que γk y γ también serán divisibles por r); *tercero*, $(\alpha h^2 + \gamma i)^2 - D\gamma^2 = h^2h'^2$. Si de ahí hacemos $\alpha h^2 + \gamma i = rp$, $\gamma = rq$, p y q serán enteros y q no será $= 0$ y tendremos $p^2 - Dq^2 = \frac{h^2h'^2}{r^2}$. Pero $\frac{h^2h'^2}{r^2}$ es el menor número divisible por ambos h^2 y h'^2 y, por ende, dividirá a A^2 y a $4D$. Como resultado $\frac{4Dr^2}{h^2h'^2}$ será un entero (negativo). Si lo hacemos $= -e$ tenemos $p^2 - Dq^2 = -\frac{4D}{e}$ o $4 = (\frac{2rp}{hh'})^2 + eq^2$, en esta ecuación $(\frac{2rp}{hh'})^2$ es necesariamente un cuadrado menor que 4 y así será ó 0 ó 1. En el primer caso $eq^2 = 4$ y $D = -(\frac{hh'}{rq})^2$ y se sigue que $\frac{4D}{A^2}$ es un cuadrado con signo negativo y, por ello, ciertamente no es $\equiv 1 \pmod{4}$ y de ahí que O no es un orden impropiamente primitivo ni derivado de un orden impropiamente primitivo. Así que $\frac{D}{A^2}$ será un entero, y claramente e será divisible por 4, $q^2 = 1$, $D = -(\frac{hh'}{r})^2$ y $\frac{A^2}{D}$ es también

un entero. Por esta razón, $D = -A^2$ ó $\frac{D}{A^2} = -1$, que es la primera excepción. En el último caso $eq^2 = 3$ de modo que $e = 3$ y $4D = -3(\frac{hh'}{r})^2$. Así que $3(\frac{hh'}{rA})^2$ será un entero, y no puede ser otra cosa que 3, dado que cuando lo multiplicamos por el entero cuadrado $(\frac{rA}{hh'})$ obtenemos 3. Por todo esto, $4D = -3A^2$ ó $D = -\frac{3}{4}A^2$ que es la segunda excepción. En todos los casos restantes todas las formas propiamente primitivas en V, V', V'', etc. pertenecerán a distintas clases. Para los casos de excepción es suficiente dar el resultado que puede encontrarse sin dificultad, pero es demasiado largo para presentarlo aquí. En el primer caso siempre habrá un par de formas propiamente primitivas en V, V', V'', etc. que pertenecen a la misma clase; en el último caso, habrá una terna. De modo que en el primer caso el número de clases será la mitad del valor dado arriba, en el último caso será un tercio.

Segundo, cuando D es un número cuadrado positivo, cada forma propiamente primitiva en V, V', V'', etc. constituye una clase separada sin excepción. Pues, supongamos que (h^2, i, k), (h'^2, i', k') son dos de tales formas distintas propiamente equivalentes y la primera es transformada en la última por medio de la sustitución propia α, β, γ, δ. Obviamente todos los argumentos que usamos en el caso previo, cuando no supusimos a D negativo, valen aquí. De ahí que si determinamos p, q, r como arriba, $\frac{4Dr^2}{h^2h'^2}$ será un entero aquí también, pero positivo en lugar de negativo y más aún, será un cuadrado. Si lo hacemos $= g^2$ tendremos $(\frac{2rp}{h'^2})^2 - g^2q^2 = 4$. *Q. E. A.* , debido a que la diferencia de dos cuadrados no puede ser 4 a no ser que el menor sea 0; entonces nuestra suposición es inconsistente.

Tercero, adonde D sea positivo pero no un cuadrado no tenemos aún una regla general para comparar el número de formas propiamente primitivas en V, V', V'', etc. con el número de clases diferentes que resultan de ellas. Sólo podemos decir que el último o es igual al primero o es un factor de éste. También hemos descubierto una conexión entre el cociente de estos números y los valores mínimos de t y u que satisfagan la ecuación $t^2 - Du^2 = A^2$, pero tomaría mucho explicarla aquí. No podemos decir con certeza si es posible conocer este cociente en todos los casos simplemente inspeccionando los números D y A (como en los casos previos). Damos algunos ejemplos y el lector puede añadir algunos suyos. Para $D = 13$, $A = 2$ el número de formas propiamente primitivas en V etc. es 3, todas las cuales son equivalentes y por ende conforman una clase simple; para $D = 37$, $A = 2$ también habrá tres formas propiamente primitivas en V etc. que pertenecerán a tres clases diferentes; para $D = 588$, $A = 7$ tenemos ocho formas propiamente primitivas en V etc., y ellas conforman cuatro clases; para $D = 867$, $A = 17$ habrá 18 formas

propiamente primitivas, y el mismo número para $D = 1445$, $A = 17$, pero para el primer determinante se dividirán en dos clases mientras que en el segundo habrá seis.

VI. De la aplicación de esta teoría general al caso donde O es un orden impropiamente primitivo, encontramos que el número de clases contenido en este orden posee la misma razón con respecto al número de todas las clases en el orden propiamente primitivo como 1 lo hace con respecto al número de clases propiamente primitivas distintas producido por las tres formas $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$. Ahora, cuando $D \equiv 1 \pmod 8$, habrá sólo una clase puesto que en este caso la segunda y la tercera formas son impropiamente primitivas; pero cuando $D \equiv 5 \pmod 8$ estas tres formas serán todas propiamente primitivas y producirán el mismo número de distintas clases si D es negativo excepto cuando $D = -3$, en cuyo caso habrá sólo una; finalmente, cuando D es positivo (de la forma $8n+5$) tenemos uno de los casos para el cual no hay regla general. Pero podemos decir que en este caso las tres formas pertenecerán a tres distintas clases o a una sola clase, nunca a dos; pues es fácil ver que si las formas $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ pertenecen respectivamente a las clases K, K', K'', tendremos $K + K' = K'$, $K' + K' = K''$ y así si K y K' son idénticas, K' y K'' también serán idénticas; similarmente si K y K'' son idénticas, K' y K'' también lo serán; finalmente, dado que tendremos $K' + K'' = K$, si suponemos que K' y K'' son idénticas, se sigue que K y K' coincidirán. Así las tres clases K, K', K'' serán o todas distintas o todas idénticas. Por ejemplo, hay 75 números de la forma $8n + 5$ menores que el número 600. Entre ellos hay 16 determinantes para los cuales el caso anterior se aplica; esto es, el número de clases en el orden propiamente primitivo es de tres multiplicado por el número de clases en el orden impropiamente primitivo, o sea, 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573; para los otros 59 casos el número de clases es el mismo en ambos órdenes.

VII. Es escasamente necesario observar que el método precedente se aplica no sólo a los números de clases en órdenes distintos del mismo determinante, sino también a determinantes distintos, siempre que su cociente sea un número cuadrado. Por tanto si O es un orden de determinante dm^2, y O' un orden de determinante dm'^2, O puede ser comparado con un orden propiamente primitivo de determinante dm^2, y éste con un orden derivado a partir de un orden propiamente primitivo de determinante d; o, lo que viene a ser lo mismo, respecto al número de clases, con este último orden en sí; y en una manera similar el orden O' puede ser comparado con este mismo orden.