Sobre el número de clases ambiguas.

257.

Entre todas las clases en un orden dado con determinante dado, las clases ambiguas especialmente demandan un tratamiento mayor, y la determinación del número de clases abre la vía a varios otros resultados interesantes. Es suficiente considerar el número de clases en el orden propiamente primitivo solamente, dado que los otros casos pueden ser fácilmente reducidos a éste. Haremos esto de la siguiente manera. Primero determinaremos todas las formas propiamente primitivas ambiguas (A, B, C) de determinante D para las cuales ya sea $B = 0$ ó $B = \frac{1}{2}A$ y, entonces, a partir del número de éstos podemos encontrar el número de todas las clases propiamente primitivas ambiguas con determinante D.

I. Se encuentran todas las formas propiamente primitivas $(A, 0, C)$ de determinante D, tomando por A a cada divisor de D (ambos positivos y negativos) para el cual $C = -\frac{D}{A}$ es relativamente primo a A. De esta manera cuando $D = -1$ habrá dos de estas formas: $(1, 0, 1)$, $(-1, 0, -1)$; y el mismo número cuando $D = 1$, sean éstas $(1, 0, -1)$, $(-1, 0, 1)$; cuando D es un número primo o la potencia de un número primo (ya sea el signo positivo o negativo), habrá cuatro $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. En general, cuando D es divisible por n números primos distintos (aquí contamos al número 2 entre ellos), se darán en total 2^{n+1} formas de este tipo; es decir si $D = \pm PQR\ldots$ donde P, Q, R, etc. son números primos diferentes o potencias de primos y si su número $= n$, los valores de A serán 1, P, Q, R, etc. y los productos de todas las combinaciones de estos números. Por la teoría de combinaciones, el número de estos valores es 2^n, pero debe ser doblado dado que cada valor debe ser tomado con un signo positivo y un signo negativo.

II. Similarmente es claro que todas las formas propiamente primitivas $(2B, B, C)$ de determinante D serán obtenidas si por B tomamos todos los divisores (positivos y negativos) de D para los cuales $C = \frac{1}{2}(B - \frac{D}{B})$ es un entero y es relativamente primo a $2B$. Dado que de ahí C es necesariamente impar y $C^2 \equiv 1$ (mod. 8), a partir de la ecuación $D = B^2 - 2BC = (B - C)^2 - C^2$ se sigue que D o es $\equiv 3$ (mod. 4) cuando B es impar, ó $\equiv 0$ (mod. 8) cuando B es par; toda vez que, por esto, D sea congruente (mod. 8) con alguno de los números 1, 2, 4, 5, 6 no habrá ninguna forma de este tipo. Cuando $D \equiv 3$ (mod. 4), C será un entero e impar, no importa cual divisor de D tomemos por B; pero a razón de que C no tenga un divisor en común con $2B$, debemos escoger a B de tal manera que $\frac{D}{B}$ y B sean relativamente primos; así para $D = -1$ tenemos dos formas $(2, 1, 1)$, $(-2, -1, -1)$, y en general si el número de todos los divisores primos de D es n, habrá

2^{n+1} formas en total. Cuando D es divisible por 8, C será un entero si tomamos por B a cualquier divisor par de $\frac{1}{2}D$; en tanto para la otra condición, de que $C = \frac{1}{2}B - \frac{D}{2B}$ sea relativamente primo a $2B$, se satisfacerá *primero* tomando por B a todos los divisores $\equiv 2 \pmod 4$ de D para los cuales $\frac{D}{B}$ y B no tengan un divisor en común. El número de éstos (contando a ambos signos) será 2^{n+1} si D es divisible por n números primos impares distintos. *Segundo*, se toma por B a todos los divisores $\equiv 0 \pmod 4$ de $\frac{1}{2}D$ para los cuales $\frac{D}{2B}$ y B son relativamente primos. Su número también será 2^{n+1}, de modo que en este caso tendremos 2^{n+2} formas en total. Por esto, si $D = \pm 2^{\mu} PQR \ldots$ donde μ es un exponente mayor que 2, P, Q, R, etc. son números primos impares diferentes o potencias de números primos, y si el número de éstos es n: entonces *tanto* para $\frac{1}{2}B$ *como* para $\frac{D}{2B}$ se pueden tomar todos los valores 1, P, Q, R, etc. y los productos de cualquier número de estos números, cada uno con un signo positivo o un signo negativo.

A raíz de todo esto vemos que si D es divisible por n números impares primos distintos (siendo $n = 0$ cuando $D = \pm 1$ ó ± 2 ó una potencia de 2), el número de todas las formas propiamente primitivas (A, B, C) para las cuales B es, ya sea 0 ó $\frac{1}{2}A$, será 2^{n+1} cuando $D \equiv 1$ ó $\equiv 5 \pmod 8$; será 2^{n+2} cuando $D \equiv 2$, 3, 4, 6, ó $7 \pmod 8$; finalmente será 2^{n+3} cuando $D \equiv 0 \pmod 8$. Si comparamos este resultado con lo que encontramos en el artículo 231 con respecto al número de todos los caracteres posibles de las formas primitivas con determinante D, observamos que el primer número es precisamente el doble de éste en todos los casos. Pero es claro que, cuando D es negativo, habrá tantas formas positivas como negativas entre ellas.

258.

Todas las formas consideradas en el artículo previo pertenecen manifiestamente a las clases ambiguas. Por otro lado, al menos una de estas formas debe ser contenida en cada clase ambigua propiamente primitiva de determinante D; pues, ciertamente, hay formas ambiguas en tal clase y toda forma ambigua propiamente primitiva (a, b, c) de determinante D es equivalente a alguna de las formas del artículo anterior, a saber, o

$$\left(a,\, 0,\, -\frac{D}{a}\right) \qquad \text{o} \qquad \left(a,\, \frac{1}{2}a,\, \frac{1}{4}a - \frac{D}{a}\right)$$

según b sea $\equiv 0$ ó $\equiv \frac{1}{2}a \pmod a$. De este modo, el problema se reduce a encontrar cuántas clases son determinadas por estas formas.

Si la forma $(a,\ 0,\ c)$ aparece entre las formas del artículo precedente, la forma $(c,\ 0,\ a)$ también aparecerá y ellas serán distintas, excepto cuando $a = c = \pm 1$ y luego $D = -1$, un caso que dejaremos a un lado, por el momento. Ahora, dado que estas formas pertenecen manifiestamente a la misma clase, es suficiente retener una, y rechazaremos aquélla cuyo primer término es mayor que el tercero; también dejaremos a un lado el caso donde $a = -c = \pm 1$ y $D = 1$. De esta manera, podemos reducir todas las formas $(A,\ 0,\ C)$ a la mitad, reteniendo sólo una de cada par; y en aquéllas que restan siempre resulta $A < \sqrt{\pm D}$.

Similarmente, si la forma $(2b,\ b,\ c)$ aparece entre las formas del artículo previo, lo siguiente también aparecerá

$$(4c - 2b,\ 2c - b,\ c) = \left(-\frac{2D}{b},\ -\frac{D}{b},\ c\right)$$

Estas dos serán propiamente equivalentes, pero diferentes entre sí, excepto en el caso que hemos omitido, donde $c = b = \pm 1$ ó $D = -1$. Es suficiente retener aquélla, de estas dos formas, cuyo primer término es menor que el primer término de la otra (en este caso no pueden ser iguales en magnitud pero diferentes en signo). De modo que todas las formas $(2B,\ B,\ C)$ pueden ser reducidas a la mitad, rechazando una de cada par; y en aquéllas que quedan siempre tendremos $B < \frac{D}{B}$ ó $B < \sqrt{\pm D}$. De acuerdo con esto, permanece sólo la mitad de todas las formas del artículo previo. Designaremos el conjunto con la letra W, y sólo resta mostrar cuántas clases diferentes surgen a partir de estas formas. Manifiestamente, en el caso cuando D es negativo habrá tantas formas positivas en W como negativas.

I. Cuando D es negativo, cada una de las formas en W pertenecerá a una clase distinta. Pues todas las formas $(A,\ 0,\ C)$ se verán reducidas; y todas las formas $(2B,\ B,\ C)$ serán reducidas, excepto aquéllas para las cuales $C < 2B$; pues en tal forma $2C < 2B + C$; luego (dado que $B < \frac{D}{B}$, eso es $B < 2C - B$, y que $2B < 2C$ o sea $B < C$), $2C - 2B < C$ y $C - B < \frac{1}{2}C$ y la forma reducida es $(C,\ C - B,\ C)$, la cual obviamente es equivalente a ésta. De esta manera habrá tantas formas reducidas como formas haya en W, y dado que cualesquiera dos de ellas no serán idénticas u opuestas (excepto para el caso donde $C - B = 0$, en el cual $B = C = \pm 1$ y por ende $D = 1$, que es el caso que habíamos dejado de lado), todas pertenecerán a clases distintas. Así, el número de todas las clases ambiguas propiamente primitivas de determinante D será igual al número de formas en W ó a la mitad del número de formas en el artículo previo. Con respecto al caso exceptuado, cuando $D = -1$, ocurre lo mismo por compensación; esto es, hay dos clases; una a la cual pertenecen las formas $(1,\ 0,\ 1)$,

(2, 1, 1), la otra a la cual pertenecen (−1, 0, −1), (−2, −1, −1). En general, por todo esto, para un determinante negativo, el número de todas las clases ambiguas propiamente primitivas es igual al número de todos los caracteres asignables de las formas primitivas de este determinante; el número de clases ambiguas propiamente primitivas que son positivas será la mitad de éste.

II. Cuando D es un cuadrado positivo $= h^2$, no es difícil mostrar que cada forma en W pertenece a una clase diferente; pero este problema puede ser resuelto más simplemente de la siguiente manera. Por el artículo 210, debe haber una forma reducida $(a, h, 0)$ contenida en cada clase ambigua propiamente primitiva de determinante h^2, donde a es el valor de la expresión $\sqrt{1} \pmod{2h}$, que cae entre 0 y $2h-1$ inclusive. Dado que esto es así, resulta claro que hay tantas clases ambiguas propiamente primitivas de determinante h^2 como hay valores para esta expresión. Del artículo 105, el número de estos valores es 2^n, 2^{n+1} o 2^{n+2}, dependiendo de si h es impar, o $\equiv 2 \pmod 4$ o $\equiv 0 \pmod 4$; esto es, según sea $D \equiv 1$, $\equiv 4$ o $\equiv 0 \pmod 8$ donde n designa al número de divisores primos impares de h o de D. De este modo, el número de clases ambiguas propiamente primitivas será siempre la mitad del número de formas consideradas en el artículo previo e igual al número de formas en W, o sea, el número de todos los posibles caracteres.

III. Cuando D es un entero positivo no cuadrado, deduciremos, a partir de cada una de las formas (A, B, C) en W a otras formas (A', B', C'), tomando a $B' \equiv B \pmod A$, que está entre los límites $\sqrt{D}$ y $\sqrt{D} \mp A$ (el signo superior o inferior será usado según sea A positivo o negativo), y $C' = \frac{B'^2 - D}{A}$; designaremos este conjunto con la letra W'. Manifiestamente, estas formas serán propiamente primitivas y ambiguas de determinante D, todas distintas, y, más aún, todas serán formas reducidas. Pues cuando $A < \sqrt{D}$, B' será $< \sqrt{D}$ y positivo; además, $B' > \sqrt{D} \mp A$ y $A > \sqrt{D} - B'$ y luego A, tomado positivamente, cae entre $\sqrt{D} + B'$ y $\sqrt{D} - B'$. Cuando $A > \sqrt{D}$, no se puede tener $B = 0$ (habíamos rechazado estas formas), pero B debe ser $= \frac{1}{2}A$. De ahí que B' será igual, en magnitud, a $\frac{1}{2}A$ y de signo positivo (pues dado que $A < 2\sqrt{D}$, $\pm\frac{1}{2}A$ caerá entre los límites asignados a B' y será congruente con B según el modulo A; así $B' = \pm\frac{1}{2}A$). Como resultado $B' < \sqrt{D}$ y $2B' < \sqrt{D} + B'$, o bien, $A < \sqrt{D} + B'$, de tal modo que $\pm A$ necesariamente caerá entre los límites $\sqrt{D} + B'$ y $\sqrt{D} - B'$. Finalmente W' contendrá a todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues si (a, b, c) es de esta forma, resultará, ya sea $b \equiv 0$ ó $b \equiv \frac{1}{2}a \pmod a$. En el primer caso, no se puede tener $b < a$, ni por esto último $a > \sqrt{D}$, así que la forma $(a, 0, -\frac{D}{a})$ ciertamente estará contenida en W y la forma correspondiente (a, b, c) en W'; en el último caso,

ciertamente $a < 2\sqrt{D}$ y, por ende, $(a,\ \frac{1}{2}a,\ \frac{1}{4}a - \frac{D}{a})$ estará contenida en W y la forma correspondiente $(a,\ b,\ c)$ en W'. Así, el número de formas en W es igual al número de todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues, dado que cada clase ambigua contiene un *par* de formas reducidas ambiguas (art. 187, 194), el número de todas las clases ambiguas propiamente primitivas de determinante D será la mitad del número de formas en W, ó bien, la mitad del número de todos los caracteres posibles.

259.

El número de clases ambiguas impropiamente primitivas de un determinante D dado es igual al número de ellas propiamente primitivas del mismo determinante. Sea K la clase principal y K', K'', etc. las restantes clases ambiguas propiamente primitivas del mismo determinante; sea L una clase ambigua impropiamente primitiva del mismo determinante, p. ej. aquélla que contiene a la forma $(2,\ 1,\ \frac{1}{2} - \frac{1}{2}D)$. Si componemos la clase L con K, obtenemos la clase L misma; supongamos que la composición de la clase L con K', K'', etc. produce las clases L', L'', etc. respectivamente. Manifiestamente, todas ellas pertenecerán al mismo determinante y serán impropiamente primitivas y ambiguas. Es claro que el teorema será probado tan pronto como probemos que todas las clases L, L', L'', etc. son diferentes y que no hay otras clases ambiguas impropiamente primitivas de determinante D además de éstas. Para este propósito, distinguimos los siguientes casos.

I. Cuando el número de clases impropiamente primitivas es igual al número de clases propiamente primitivas, cada una de las primeras resultará de la composición de la clase L con una clase propiamente primitiva determinada, y así todas las L, L', L'', etc. serán diferentes. Si designamos por $\mathfrak{L}$ a cualquier clase ambigua impropiamente primitiva de determinante D, existirá una clase propiamente primitiva $\mathfrak{R}$ tal que $\mathfrak{R} + L = \mathfrak{L}$; si $\mathfrak{R}'$ es la clase opuesta a $\mathfrak{R}$, resultará también (dado que las clases L y $\mathfrak{L}$ son sus propias opuestas) $\mathfrak{R}' + L = \mathfrak{L}$, de donde necesariamente $\mathfrak{R}$ y $\mathfrak{R}'$ serán idénticas, o sea una clase ambigua. Como resultado de ésto, $\mathfrak{R}$ se encontrará entre las clases K, K', K'', etc. y $\mathfrak{L}$ entre las clases L, L', L'', etc.

II. Cuando el número de clases impropiamente primitivas es un tercio del número de clases propiamente primitivas, sea H la clase en la cual aparece la forma $(4,\ 1,\ \frac{1-D}{4})$, y H' aquélla en la cual aparece $(4,\ 3,\ \frac{9-D}{4})$. H y H' serán propiamante primitivas, distintas entre sí y de la clase principal K, y $H + H' = K$, $2H = H'$, $2H' = H$; y si $\mathfrak{L}$ es cualquier clase impropiamente primitiva de determinante D que

surge de la composición de L con la clase propiamente primitiva $\mathfrak{R}$, también se tendrá $\mathfrak{L} = L + \mathfrak{R} + H$ y $\mathfrak{L} = L + \mathfrak{R} + H'$. Además de las tres clases (propiamente primitivas y distintas) $\mathfrak{R}$, $\mathfrak{R} + H$, $\mathfrak{R} + H'$ no hay otras que produzcan a $\mathfrak{L}$ cuando se componen con L. Dado que, a raíz de esto, si $\mathfrak{L}$ es ambigua y $\mathfrak{R}'$ es opuesta a $\mathfrak{R}$, también tendremos $L + \mathfrak{R}' = \mathfrak{L}$, $\mathfrak{R}'$ será necesariamente idéntica a una de las tres clases. Si $\mathfrak{R}' = \mathfrak{R}$, $\mathfrak{R}$ será ambigua; si $\mathfrak{R}' = \mathfrak{R} + H$, resulta $K = \mathfrak{R} + \mathfrak{R}' = 2\mathfrak{R} + H = 2(\mathfrak{R} + H')$ y, por lo tanto, $\mathfrak{R} + H'$ es ambigua; similarmente, si $\mathfrak{R}' = \mathfrak{R} + H'$, $\mathfrak{R} + H$ será ambigua y concluimos que $\mathfrak{L}$ necesariamente se encuentra entre las clases L, L', L'', etc. Es fácil ver que no puede haber más de una clase ambigua entre las tres clases $\mathfrak{R}$, $\mathfrak{R} + H$, $\mathfrak{R} + H'$; pues si ambas $\mathfrak{R}$ y $\mathfrak{R} + H$ fueran ambiguas y, por lo tanto, idénticas a sus opuestas $\mathfrak{R}'$, $\mathfrak{R}' + H'$, tendríamos $\mathfrak{R} + H = \mathfrak{R} + H'$; la misma conclusión resulta a partir de la suposición de que $\mathfrak{R}$ y $\mathfrak{R} + H'$ son ambiguas; finalmente, si $\mathfrak{R} + H$ y $\mathfrak{R} + H'$ son ambiguas e idénticas con sus opuestas $\mathfrak{R}' + H'$ y $\mathfrak{R}' + H$, tendríamos $\mathfrak{R} + H + \mathfrak{R}' + H = \mathfrak{R}' + H' + \mathfrak{R} + H'$ y así $2H = 2H'$, ó bien, $H' = H$. Por esta razón, sólo habrá una clase ambigua propiamente primitiva que produce a $\mathfrak{L}$ cuando ésta es compuesta con L, y, por lo tanto, todas las L, L', L'', etc. serán diferentes.

El número de clases ambiguas en un orden *derivado* es obviamente igual al número de clases ambiguas en el orden primitivo a partir del cual es derivado, y así, este número siempre puede determinarse.

260.

PROBLEMA. *La clase propiamente primitiva K de determinante D surge a partir de la duplicación de una clase propiamente primitiva k del mismo determinante. Se buscan todas las clases similares cuya duplicación produzca a K.*

Solución. Sea H la clase principal de determinante D y sean H', H'', H''', etc. las otras clases ambiguas propiamente primitivas del mismo determinante; $k + H'$, $k + H''$, $k + H'''$, etc. son las clases que surgen a partir de la composición de éstas con k. Las designaremos como k', k'', k''', etc. Ahora bien, todas las clases k', k'', k''', etc. serán propiamente primitivas de determinante D y diferentes entre sí; y la clase K resultará de la duplicación de cualquiera de ellas. Si denotamos por $\mathfrak{R}$ a cualquier clase propiamente primitiva de determinante D que produzca a la clase K cuando sea duplicada, necesariamente estará contenida entre las clases k, k', k'', etc. Pues, supóngase que $\mathfrak{R} = k + \mathfrak{H}$, de tal modo que $\mathfrak{H}$ es una clase propiamente primitiva de determinante D (art. 249), entonces $2k + 2\mathfrak{H} = 2\mathfrak{R} = K = 2k$ y, por tanto, $2\mathfrak{H}$ coincide con la clase principal, $\mathfrak{H}$ es ambigua y, por ende, está contenida entre H,

H', H'', etc. y $\mathfrak{R}$ entre k, k', k'', etc.; por todo esto, estas clases dan una solución completa del problema.

Es evidente que, cuando D es negativo, la mitad de las clases k, k', k'', etc. serán positivas, la mitad negativas.

Dado que, a raíz de esto, toda clase propiamente primitiva de determinante D que pueda surgir a partir de la duplicación de una clase similar, proviene de la duplicación de tantas clases similares como clases ambiguas propiamente primitivas de determinante D hubiere; es claro que, si el número de todas las clases propiamente primitivas de determinante D es r, y si el número de todas las clases ambiguas propiamente primitivas de este determinante es n, entonces el número de todas las clases propiamente primitivas del mismo determinante que puede ser producido por la duplicación de una clase similar será $\frac{r}{n}$. La misma fórmula resulta si, para un determinante negativo, r y n designan los correspondientes números de clases *positivas*. De este modo, p.ej., para $D = -161$, el número de todas las clases positivas propiamente primitivas es 16, el número de clases ambiguas es 4, así que el número de clases que pueden surgir a partir de la duplicación de cualquier clase debe ser 4. De hecho, encontramos que todas las clases contenidas en el género principal están provistas de esta propiedad; por esto, la clase principal (1, 0, 161) resulta a partir de la duplicación de las cuatro clases ambiguas; (2, 1, 81) a partir de la duplicación de las clases (9, 1, 18), (9, −1, 18), (11, 2, 15), (11, −2, 15); (9, 1, 18) a partir de la duplicación de las clases (3, 1, 54), (6, 1, 27), (5, −2, 33), (10, 3, 17); finalmente (9, −1, 18) duplicando las clases (3, −1, 54), (6, −1, 27), (5, 2, 33), (10, −3, 17).

La mitad de todos los caracteres asignables para un determinante dado no puede estar en un género propiamente primitivo (positivo para un determinante negativo).

261.

TEOREMA. *La mitad de todos los caracteres asignables para un determinante positivo no cuadrado no puede pertenecer a ningún género propiamente primitivo; si el determinante es negativo, a ningún género propiamente primitivo positivo.*

Demostración. Sea m el número de todos los géneros propiamente primitivos (positivos) de determinante D; sea k el número de clases contenidas en cada género, de tal manera que km es el número de todas las clases propiamente primitivas (positivas); sea n el número de todos los caracteres diferentes asignables a este determinante. Entonces, por el artículo 258, el número de todas las clases ambiguas propiamente primitivas (positivas) será $\frac{1}{2}n$; y, por el artículo precedente, el número de todas

las clases propiamente primitivas que puedan resultar a partir de la duplicación de una clase similar será $\frac{2km}{n}$. Pero, por el artículo 247, todas estas clases pertenecen al género principal que contiene a k clases; si, por esta razón, todas las clases del género principal resultan a partir de la duplicación de alguna clase (mostraremos en lo que sigue que esto es siempre cierto), entonces $\frac{2km}{n} = k$, o bien, $m = \frac{1}{2}n$; pero es cierto que no podemos tener $\frac{2km}{n} > k$ ni, consecuentemente, $m > \frac{1}{2}n$. Dado que, por esto, el número de todos los géneros propiamente primitivos (positivos), ciertamente, no puede ser mayor que la mitad de todos los caracteres asignables, al menos la mitad de ellos no puede corresponder con tales géneros. *Q. E. D.* Nótese, sin embargo, que todavía no se sigue a partir de esto que la mitad de todos los caracteres asignables de hecho corresponden a géneros propiamente primitivos (positivos), pero luego estableceremos la validez de esta profunda proposición concerniente al misterio más recóndito de los números.

Dado que, para un determinante negativo hay siempre tantos géneros negativos como positivos, manifiestamente, no más que la mitad de todos los caracteres asignables pueden pertenecer a los géneros propiamente primitivos negativos. Hablaremos de esto y de géneros impropiamente primitivos abajo. Finalmente, observamos que el teorema no se aplica a determinantes cuadrados positivos. Por esto, es fácil ver que cada carácter asignable corresponde a un género.

Una segunda demostración del teorema fundamental y de los demás teoremas acerca de los residuos -1, $+2$, -2.

262.

Así pues, en el caso donde sólo dos caracteres diferentes pueden ser asignados a un determinante no cuadrado dado D, sólo uno corresponderá a un género propiamente primitivo (positivo) (éste tiene que ser el género principal). El otro no corresponderá a ninguna forma propiamente primitiva (positiva) de ese determinante. Esto ocurre para los determinantes -1, 2, -2, -4, para números positivos primos de la forma $4n + 1$, para negativos de primos de la forma $4n + 3$, para todas las potencias positivas impares de números primos de la forma $4n + 1$, y para potencias pares positivas o impares negativas de números primos de la forma $4n+3$. A partir de este principio, podemos desarrollar un nuevo método, no solamente para el teorema fundamental, sino también para demostrar los otros teoremas de la sección previa que tengan que ver con los residuos -1, $+2$, -2. Este método será completamente diferente de aquéllos usados en la sección anterior y, de ninguna manera, menos

elegante. Sin embargo, omitiremos la consideración del determinante -4 y de los determinantes que son potencias de números primos, dado que no nos enseñarían nada nuevo.

Para el determinante -1, no hay forma positiva con el carácter 3, 4; para el determinante $+2$ no hay ninguna con el carácter 3 *y* 5, 8; para el determinante -2 no habrá forma positiva con el carácter 5 *y* 7, 8; y para el determinante $-p$, donde p es un número primo de la forma $4n+3$, ninguna forma propiamente primitiva (positiva) tendrá al carácter Np; mientras que para el determinante $+p$, donde p es un número primo de la forma $4n+1$, ninguna forma propiamente primitiva tendrá al carácter Np. De este modo, demostraremos los teoremas de la sección previa de la siguiente manera.

I. -1 es un no residuo de cualquier número (positivo) de la forma $4n+3$. Pues si -1 fuera un residuo de tal número A, al tomar $-1 = B^2 - AC$, (A, B, C) sería una forma positiva de determinante -1 con el carácter 3, 4.

II. -1 es un residuo de cualquier número primo p de la forma $4n+1$. Pues el carácter de la forma $(-1, 0, p)$, así como de todas las formas propiamente primitivas de determinante p, será Rp y, por tanto, $-1Rp$.

III. Ambos $+2$ y -2 son residuos de cualquier número primo p de la forma $8n+1$. Pues cualquiera de las formas $(8, 1, \frac{1-p}{8})$, $(-8, 1, \frac{p-1}{8})$, o bien, las formas $(8, 3, \frac{9-p}{8})$, $(-8, 3, \frac{p-9}{8})$ son propiamente primitivas (según sea n impar o par), y así su carácter será Rp; de tal manera que $+8Rp$, y $-8Rp$, y también $2Rp$, y $-2Rp$.

IV. $+2$ es un no residuo de cualquier número de la forma $8n+3$ u $8n+5$. Pues si fuera un residuo de tal número A, habría una forma (A, B, C) de determinante $+2$ con el carácter 3 *y* 5, 8.

V. Similarmente, -2 es un no residuo de cualquier número de la forma $8n+5$ u $8n+7$, pues, de otro modo, habría una forma (A, B, C) de determinante -2 con el carácter 5 *y* 7, 8.

VI. -2 es un residuo de cualquier número primo p de la forma $8n+3$. Se muestra esta proposición por dos métodos. *Primero,* dado que, por IV, $+2Np$ y, por I, $-1Np$, necesariamente tenemos $-2Rp$. La *segunda* demostración comienza con una consideración del determinante $+2p$. A raíz de éste, cuatro caracteres son asignables, y son éstos Rp, 1 *y* 3, 8; Rp, 5 *y* 7, 8; Np, 1 *y* 3, 8; Np, 5 *y* 7, 8. De éstos, al menos dos no corresponden a ningún género. Ahora bien, la forma $(1, 0, -2p)$ estará de acuerdo con el primer carácter; la forma $(-1, 0, 2p)$ con el cuarto; de ahí que el segundo y el tercero deben ser rechazados. Y dado que el carácter de la forma

$(p,\ 0,\ -2)$ relativo al número 8 es 1 *y* 3, 8, su carácter relativo a p debe ser Rp, y así $-2Rp$.

VII. $+2$ es un residuo de cualquier número primo p de la forma $8n+7$. Esto puede ser mostrado por dos métodos. *Primero,* dado que, por I y V, $-1Np$, $-2Np$, tendrá $+2Rp$. *Segundo,* dado que, ya sea $(8,\ 1,\ \frac{1+p}{8})$ o $(8,\ 3,\ \frac{9+p}{8})$ es una forma propiamente primitiva de determinante $-p$ (dependiendo de si n es par o impar), su carácter será Rp y, por lo tanto, $8Rp$ y $2Rp$.

VIII. Cualquier número primo p de la forma $4n+1$ es un no residuo de cualquier número impar q que sea un no residuo de p. Pues, claramente, si p fuera un residuo de q, habría una forma propiamente primitiva de determinante p con el carácter Np.

IX. Similarmente, si un número impar q es un no residuo de un número primo p de la forma $4n+3$, $-p$ será un no residuo de q; de cualquier otra manera, habría una forma propiamente primitiva de determinante $-p$ con el carácter Np.

X. Cualquier número primo p de la forma $4n+1$ es un residuo de cualquier otro número primo q que sea un residuo de p. Si q es también de la forma $4n+1$, esto se sigue inmediatamente a partir de VIII; pero si q es de la forma $4n+3$, $-q$ será también un residuo de p (por II) y, así, pRq (por IX).

XI. Si un número primo q es un residuo de otro número primo p de la forma $4n+3$, $-p$ será un residuo de q. Pues si q es de la forma $4n+1$, se sigue inmediatamente, a partir de VIII, que pRq y, así, (por II) $-pRq$; este método no funciona cuando q es de la forma $4n+3$, pero puede ser fácilmente resuelto considerando al determinante $+pq$. Pues, dado que, de los cuatro caracteres asignables para este determinante Rp, Rq; Rp, Nq; Np, Rq; Np, Nq, dos de ellos no pueden corresponder a cualquier género y, dado que los caracteres de las formas $(1,\ 0,\ -pq)$ y $(-1,\ 0,\ pq)$ son el primero y el cuarto, respectivamente, entonces el segundo y el tercero son los caracteres que no corresponden a ninguna forma propiamente primitiva de determinante pq. Y, dado que, por hipótesis, el carácter de la forma $(q,\ 0,\ -p)$ con respecto al número p es Rp, su carácter con respecto al número q debe ser Rq y, por ende, $-pRq$. *Q. E. D.*

Si en las proposiciones VIII y IX se supone que q es un número primo, estas proposiciones, junto con X y IX, nos darán el teorema fundamental de la sección previa.