134.

Ahora nos dirigimos a deducir estas proposiciones.

I. Como antes, tómese P resuelto en sus factores primos sin tomar en consideración los signos y Q resuelto en factores de cualquier modo pero donde, no obstante, se considera el signo de Q. Se combina cada uno de aquellos factores con cada uno de éstos. Si s denota el número de todas las combinaciones en las cuales el factor de Q es un no residuo del factor de P, entonces p y s serán al mismo tiempo pares o impares. De hecho, sean f, f', f'', etc. los factores primos de P, y entre los factores en los que está resuelto Q, sea m el número que son no residuos de f, m' el de los no residuos de f', m'' el de los no residuos de f'', etc. Entonces se verá fácilmente que

$$s = m + m' + m'' + \text{ etc.}$$

y que p expresa cuántos números entre m, m', m'', etc. son impares. De donde es evidente que s será par cuando p sea par, pero impar cuando p sea impar.

II. Esto vale generalmente para cualquier forma en que Q sea resuelto en factores. Pasemos a los casos particulares. Consideraremos primero el caso donde uno de los números P es positivo, pero el otro, Q, es o bien de la forma $+A$ o bien de la forma $-B$. Se resuelven P y Q en sus factores primos, donde se les da un signo positivo a cada uno de los factores de P, pero a los factores individuales de Q el signo positivo o el negativo según sean de la forma a o b. Entonces, como se requiere, es evidente que Q será de la forma $+A$ o $-B$. Se combinan cada uno de los factores de P con cada uno de los de Q y se denotará como antes por s el número de combinaciones en que cada factor de Q es un no residuo del factor de P, y de modo semejante por t el número de combinaciones en que cada factor de P es un no residuo del factor de Q. Se sigue del teorema fundamental que estas combinaciones serán idénticas, de donde $s = t$. Finalmente de lo que hemos demostrado se sigue que $p \equiv s \pmod 2$, $q \equiv t \pmod 2$, y así $p \equiv q \pmod 2$.

Así pues se tienen las proposiciones 1, 3, 4 y 6 del art. 133.

Las restantes proposiciones pueden derivarse directamente por métodos similares, pero requieren de una nueva consideración. Sin embargo, se derivan más fácilmente de lo anterior por los métodos siguientes.

III. De nuevo P y Q denotan números impares cualesquiera, primos entre sí, p y q el número de factores primos de P y Q de los que Q y P son no residuos respectivamente. Finalmente sea p' el número de factores primos de P de los cuales

$-Q$ es un no residuo (cuando Q es negativo es evidente que $-Q$ indicará un número positivo). Ahora se distribuyen todos los factores primos de P en cuatro clases.

1) Factores de la forma a, de los cuales Q es un residuo.

2) Factores de la forma b, de los cuales Q es un residuo. Sea χ el número de ellos.

3) Factores de la forma a, de los cuales Q es un no residuo. Sea ψ el número de ellos.

4) Factores de la forma b, de los cuales Q es un no residuo. Sea ω el número de ellos.

Entonces se ve fácilmente que $p = \psi + \omega$, $p' = \chi + \psi$.

Cuando P es de la forma $\pm A$, $\chi + \omega$ y también $\chi - \omega$, serán números pares: por lo que $p' = p + \chi - \omega \equiv p \pmod 2$. Pero cuando P es de la forma $\pm B$, se descubre por un razonamiento similar que los números p y p' serán incongruentes, según mod. 2.

IV. Apliquemos esto a cada uno de los casos. Primero, sean tanto P como Q de la forma $+A$, entonces de la proposición 1 tendremos $p \equiv q \pmod 2$; pero $p' \equiv p \pmod 2$; por lo que también $p' \equiv q \pmod 2$. Lo cual concuerda con la proposición 2.— De modo semejante si P es de la forma $-A$, Q de la forma $+A$, será $p \equiv q \pmod 2$ de la proposición 2 la que ya hemos demostrado. De esto si $p' \equiv p$ tendremos $p' \equiv q$. Así pues, también la proposición 5 está demostrada.

De la misma manera se deriva la proposición 7 de la 3, la proposición 8 o de la 4 o de la 7; la 9 de la 6; la 10 de la 6.

Demostración rigurosa del teorema fundamental.

135.

Las proposiciones del artículo 133 no se han demostrado por medio del artículo precedente, sino que se mostró que la validez de ellas depende de la validez del teorema fundamental que hemos supuesto. Por el método de esta misma deducción es evidente que estas proposiciones valdrán para números P y Q si el teorema fundamental vale para todos los factores primos de estos números comparados entre sí, y aún si no fuera válido en general. Por lo tanto ahora avanzamos hacia la demostración del teorema fundamental. Enunciamos antes de ella la siguiente aclaración.

Diremos que el teorema fundamental es verdadero hasta algún número M, si vale para dos números primos cualesquiera de los cuales ninguno supera a M.

De modo semejante debe entenderse si decimos que los teoremas de los artículos 131, 132 y 133 son verdaderos hasta algún término. Se nota fácilmente que si el teorema fundamental es válido hasta algún término, estas proposiciones tendrán que ser válidas hasta el mismo término.

136.

Por inducción puede confirmarse fácilmente que el teorema fundamental vale para números pequeños, de tal manera se determina un límite hasta el cual sea válido. Suponemos que esta inducción está hecha; es completamente indiferente hasta donde la hayamos realizado. De tal manera bastaría confirmarlo hasta al número 5, pero esto se logra con la simple observación de que $+5N3$, $\pm 3N5$.

Ahora, si el teorema fundamental no es verdadero en general, existirá algún límite T hasta el cual valdrá, de manera que ya no valga más para el próximo número mayor $T+1$. Esto es lo mismo que si dijéramos que existen dos números primos, de los cuales el mayor es $T+1$ y que comparados entre sí contradicen el teorema fundamental, y dijéramos que otros pares cualesquiera de números primos, siendo ambos menores que $T+1$, cumplen con este teorema. De donde se sigue que las proposiciones de los artículos 131, 132, 133 también deberán ser válidas hasta T. Pero mostraremos ahora que esta suposición no puede subsistir. Los casos siguientes deberán distinguirse según las formas diferentes que pueden tener, tanto $T+1$ como el número primo menor que $T+1$ que contradiría el teorema. Denotemos este número primo por p.

Cuando tanto $T+1$ como p son de la forma $4n+1$, el teorema fundamental puede ser falso de dos maneras, a saber, si al mismo tiempo fuera

o bien $\quad \pm pR(T+1) \quad \text{y} \quad \pm(T+1)Np$

o bien a la vez $\quad \pm pN(T+1) \quad \text{y} \quad \pm(T+1)Rp$

Cuando tanto $T+1$ como p son de la forma $4n+3$, el teorema fundamental sería falso si al mismo tiempo tuvieramos

o bien $\quad +pR(T+1) \quad \text{y} \quad -(T+1)Np$

(o lo que es lo mismo $\quad -pN(T+1) \quad \text{y} \quad +(T+1)Rp)$

o bien $\quad +pN(T+1) \quad \text{y} \quad -(T+1)Rp$

(o sea $\quad -pR(T+1) \quad \text{y} \quad +(T+1)Np)$

Cuando $T+1$ es de la forma $4n+1$, y p es de la forma $4n+3$, el teorema fundamental sería falso si tuvieramos

o bien $\quad \pm pR(T+1) \quad \text{y} \quad +(T+1)Np \text{ (o } -(T+1)Rp)$

o bien $\pm pN(T+1)$ y $-(T+1)Np$ (o $+(T+1)Rp$)

Cuando $T+1$ es de la forma $4n+3$ y p de la forma $4n+1$, el teorema fundamental sería falso si tuvieramos

o bien $+pR(T+1)$ (o $-pN(T+1)$) y $\pm(T+1)Np$
o bien $+pN(T+1)$ (o $-pR(T+1)$) y $\pm(T+1)Rp$

Si se puede demostrar que ninguno de estos ocho casos puede tener lugar, sería cierto al mismo tiempo que la validez del teorema fundamental no está acotada por ningún límite. Ahora pasamos a este asunto, pero, puesto que algunos de estos casos son dependientes de otros, no convendrá mantener el mismo orden que hemos usado aquí para enumerarlos.

137.

Primer caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, y p es de la misma forma, si $\pm pRa$, entonces no puede ser que $\pm aNp$. Esto era el primer caso arriba.

Sea $+p \equiv e^2 \pmod{a}$, donde e es par y $< a$ (esto siempre es posible). Ahora deben distinguirse dos casos.

I. Cuando e no es divisible por p, se pone $e^2 = p + af$ y f será positivo de la forma $4n+3$ (o sea de la forma B), $< a$, y no divisible por p. Además tendremos $e^2 \equiv p \pmod{f}$, i.e., pRf de donde por la proposición 11 del art. 132 $\pm fRp$ (en efecto $p, f < a$, y para ellos, estas proposiciones valdrán). Pero también $afRp$, por lo tanto $\pm aRp$.

II. Cuando e es divisible por p, se pone $e = gp$ y así $e^2 = p + aph$ o sea $pg^2 = 1 + ah$. Entonces, h será de la forma $4n+3$ (B), y primo a g^2 y p. Además, tendremos pg^2Rh pues también pRh, y de esto (proposición 11, art. 132) $\pm hRp$. Y también $-ahRp$, porque $-ah \equiv 1 \pmod{p}$; por lo tanto también será $\mp aRp$.

138.

Segundo caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, p de la forma $4n+3$, y $\pm pR(T+1)$, no puede ser ni $+(T+1)Np$ ni $-(T+1)Rp$. Este caso fue el quinto arriba.

Sea como antes $e^2 = p + fa$, donde e es par y $< a$.

I. Cuando e no es divisible por p, tampoco f será divisible por p. Además de esto f será positivo de la forma $4n+1$ (o sea A), y $< a$, pero $+pRf$; por lo tanto (proposición 10 del art. 132) $+fRp$. Pero también $+faRp$, de donde tendremos $+aRp$, o $-aNp$.

II. Cuando e es divisible por p, sea $e = pg$ y $f = ph$. Así que tendremos $g^2p = 1 + ha$. Entonces h será positivo de la forma $4n+3$ (B), y primo a p y g^2. Además $+g^2pRh$, así que $+pRh$; de esto (proposición 13, art. 132) $-hRp$. Pero $-haRp$, de donde $+aRp$ y $-aNp$.

139.

Tercer caso. Cuando $T+1$ es de la forma $4n+1$ ($= a$), p de la misma forma y $\pm pNa$, entonces no puede ser que $\pm aRp$. (Segundo caso arriba).

Tomemos algún número primo menor que a, del cual $+a$ sea un no residuo, el cual, hemos demostrado arriba, existe. Conviene considerar aquí dos casos por separado, según que este número primo sea de la forma $4n+1$ o $4n+3$; pues no se ha demostrado que existan tales números primos de *ambas* formas.

I. Sea ese número primo $= a'$ y de la forma $4n+1$. Entonces tendremos $\pm a'Na$ (art. 131) ya que $\pm a'pRa$. Sea por lo tanto $e^2 \equiv a'p \pmod{a}$ y e par, $< a$. Entonces deberán distinguirse cuatro casos.

1) Cuando e no es divisible ni por p ni por a'; ponemos $e^2 = a'p \pm af$ tomado el signo de tal manera que f sea positivo. Entonces será $f < a$, primo a a' y a p y para el signo superior, de la forma $4n+3$, para el inferior de la forma $4n+1$. Por brevedad denotaremos por $[x, y]$ el número de factores primos del número y de los cuales x es un no residuo. Entonces será $a'pRf$ y así $[a'p, f] = 0$. De esto $[f, a'p]$ será un número par (las proposiciones 1 y 3 del art. 133), i.e., o bien $= 0$, o bien $= 2$. Por lo que f será o bien un residuo de ambos números a' y p o bien de ninguno. Pero lo primero es imposible ya que $\pm af$ es un residuo de a' y $\pm aNa'$ (hipótesis); de donde $\pm fNa'$. De esto f tiene que ser un no residuo de ambos números a' y p. Pero puesto que $\pm afRp$, tendremos $\pm aNp$. *Q. E. D.*

2) Cuando e es divisible por p pero no por a', sea $e = gp$ y $g^2p = a' \pm ah$, el signo determinado tal que h sea positivo. Entonces tendremos $h < a$, primo a a', g y p, para el signo superior de la forma $4n+3$, pero para el inferior de la forma $4n+1$. De la ecuación $g^2p = a' \pm ah$, si se la multiplica por p y a', puede deducirse

sin dificultad alguna que

$$pa'Rh \ldots\ldots (\alpha)$$
$$\pm ahpRa' \ldots\ldots (\beta)$$
$$aa'hRp \ldots\ldots (\gamma)$$

Sigue de (α) que $[pa', h] = 0$, por lo que (proposiciones 1 y 3, art. 133) $[h, pa']$ es par, i.e., h será un no residuo o de ambos p y a', o de ninguno. *En el primer caso,* sigue de (β) que $\pm apNa'$, y ya que por hipótesis $\pm aNa'$, será $\pm pRa'$. De esto, por el teorema fundamental que vale para los números p y a', puesto que son menores que $T+1$, tendremos $\pm a'Rp$. Ya que hNp, entonces por (γ), $\pm aNp$. *Q. E. D. En el segundo caso,* sigue de (β) que $\pm apRa'$, de esto $\pm pNa'$, $\pm a'Np$, y finalmente de esto y de hRp se tiene de (γ) que $\pm aNp$. *Q. E. D.*

3) Cuando e es divisible por a' pero no por p. Para este caso la demostración procede de un modo semejante al precedente y no es necesario detenerse en ésta.

4) Cuando e es divisible tanto por a' como por p, y por tanto también por el producto $a'p$ (hemos supuesto que los números a' y p son *diferentes,* puesto que en el caso contrario, aNp estará contenido en la hipótesis aNa'). Sea $e = ga'p$ y $g^2a'p = 1 \pm ah$. Entonces tendremos $h < a$, primo a a' y p, para el signo superior de la forma $4n+3$, y para el inferior de la forma $4n+1$. Pero se observa fácilmente que de esta ecuación pueden deducirse las siguientes:

$$a'pRh \ldots\ldots (\alpha)$$
$$\pm ahRa' \ldots\ldots (\beta)$$
$$\pm ahRp \ldots\ldots (\gamma)$$

De (α), que coincide con (α) en 2), se sigue igualmente como allí. Esto es, al mismo tiempo se tiene o bien hRp, hRa', o bien hNp, hNa'. Pero en el primer caso, por (β) será aRa', contrariamente a la hipótesis; por lo cual será hNp, y así también por (γ), aNp.

II. Cuando ese número primo es de la forma $4n+3$, la demostración es tan similar a la precedente que no es importante adjuntarla. Para quienes desean desarrollarla (lo que recomendamos bastante), notamos que después de haber llegado a la ecuación $e^2 = bp \pm af$ (denotando a b como aquel número primo) será útil si se consideran por separado ambos signos.

140.

Cuarto caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, p de la forma $4n+3$, y $\pm pNa$, no podrán ser ni $+aRp$ ni $-aNp$. (El sexto caso arriba).

También por brevedad omitimos la demostración de este caso, puesto que es completamente similar a la demostración del tercer caso.

141.

Quinto caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la misma forma, y $+pRb$ o $-pNb$, no será ni $+bRp$ ni $-bNp$. (Tercer caso arriba).

Sea $p \equiv e^2 \pmod{b}$, y e par y $< b$.

I. Cuando e no es divisible por p. Póngase $e^2 = p+bf$ y f será positivo, de la forma $4n+3$, $< b$ y primo a p. Además tendremos pRf, por tanto por la proposición 13, art. 132, $-fRp$. De esto y de $+bfRp$ tenemos $-bRp$ y así $+bNp$. *Q. E. D.*

II. Cuando e es divisible por p, sea $e = pg$ y $g^2p = 1 + bh$. Entonces tendremos h de la forma $4n+1$ y primo a p, $p \equiv g^2p^2 \pmod{h}$, por tanto pRh. De esto es $+hRp$ (proposición 10, art. 132), y de $-bhRp$ se sigue que $-bRp$ o sea $+bNp$. *Q. E. D.*

142.

Sexto caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la forma $4n+1$, y pRb, no puede ser $\pm bNp$. (El séptimo caso arriba.)

Omitimos la demostración, que es totalmente semejante a la precedente.

143.

Séptimo caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la misma forma, y $+pNb$ o $-pRb$, no pueden ser $+bNp$, ni $-bRp$. (Cuarto caso arriba).

Sea $-p \equiv e^2 \pmod{b}$, y e par y $< b$.

I. Cuando e no es divisible por p. Sea $-p = e^2 - bf$, y f será positivo, de la forma $4n+1$, primo a p y menor que b (ya que ciertamente e no es mayor que $b-1$, $p < b-1$, por lo que tendremos $bf = e^2 + p < b^2 - b$ i.e., $f < b-1$). Además tendremos $-pRf$, de esto (proposición 10, art. 132) $+fRp$, de $+bfRp$ tendremos $+bRp$, o $-bNp$.

II. Cuando e es divisible por p, sea $e = pg$, y $g^2p = -1 + bh$. Entonces será h positivo, de la forma $4n+3$, primo a p y $< b$. Además tendremos $-pRh$, de donde (proposición 14, art. 132) $+hRp$. De $bhRp$ sigue que $+bRp$ o $-bNp$. *Q. E. D.*

144.

Octavo caso. Cuando $T+1$ *es de la forma* $4n+3$ *(*$= b$*),* p *de la forma* $4n+1$*,* y $+pNb$ *o* $-pRb$*, no puede ser* $\pm bRp$*.* (El último caso arriba).

La demostración es como en el caso precedente.

Método análogo para la demostración del teorema del art. 114.

145.

En la demostración precedente siempre tomamos para e un valor par (art. 137–144). Conviene observar también que pudimos usar un valor impar, pero entonces hubiéramos tenido que introducir para esto más distinciones. Quienes se deleitan con estas investigaciones las encontrarán útiles si ponen esfuerzo en el desarrollo de estos casos. Además, los teoremas pertenecientes a los residuos $+2$ y -2 entonces deberían suponerse; pero como nuestra demostración está completa sin usar estos teoremas, obtenemos de esto un método nuevo para demostrarlos. Este no se debe desdeñar, ya que es más directo que los métodos que utilizamos arriba para demostrar que ± 2 es un residuo de cualquier número primo de la forma $8n+1$. Supondremos que los casos restantes (que abarcan los números primos de las formas $8n+3$, $8n+5$, $8n+7$) ya han sido demostrados mediante los métodos tratados arriba, y que este teorema solamente ha sido establecido por inducción. No obstante, llevaremos esta inducción a un nivel de certidumbre mediante las siguientes reflexiones.

Si ± 2 no es un residuo de todos los números primos de la forma $8n+1$, póngase el menor primo de esta forma del cual ± 2 es un no residuo $= a$, así que el teorema vale para todos los primos menores que a. Entonces, se toma algún número primo $< \frac{1}{2}a$, del cual a es un no residuo (del articulo 129 se deduce con facilidad que tal número existe). Sea este número $= p$, por el teorema fundamental resultará pNa. De esto, $\pm 2pRa$.— Por eso, sea $e^2 \equiv 2p \pmod{a}$, de manera que e sea impar y $< a$. Entonces deberán distinguirse dos casos.

I. Cuando e no es divisible por p. Sea $e^2 = 2p + aq$, así que q será positivo, de la forma $8n+7$ o de la forma $8n+3$ (según que p sea de la forma $4n+1$ o $4n+3$), $< a$, y no divisible por p. Todos los factores primos de q se distribuirán en

cuatro clases, a saber: sean e aquéllos de la forma $8n+1$, f de la forma $8n+3$, g de la forma $8n+5$, h de la forma $8n+7$. Sea E el producto de los factores de la primera clase y los productos de los factores de la segunda, tercera, y cuarta clases respectivamente F, G, H*). Hecho esto, consideraremos *primero* el caso donde p es de la forma $4n+1$ y q de la forma $8n+7$. Entonces se ve fácilmente que $2RE$ y $2RH$, de donde pRE y pRH y de esto finalmente ERp y HRp. Además 2 será un no residuo de cualquier factor de la forma $8n+3$ u $8n+5$, y por eso también p; y este factor será un no residuo de p; de donde se concluye fácilmente que FG será un residuo de p si $f+g$ es par, no residuo si $f+g$ es impar. Pero $f+g$ no puede ser impar; de hecho, enumerando todos los casos se nota fácilmente que $EFGH$ o sea q será de la forma $8n+3$ u $8n+5$ si $f+g$ es impar, sean como sean e, f, g, h por separado, contrariamente a la hipótesis. Por lo tanto, tendremos $FGRp$, $EFGHRp$, o sea qRp, y finalmente $aqRp$ implica aRp, contrariamente a la hipótesis. *Segundo*, cuando p es de la forma $4n+3$, puede demostrarse de modo semejante que será pRE, así que ERp y $-pRF$, y en consecuencia FRp, finalmente $g+h$ es par y así $GHRp$, de donde finalmente se sigue que qRp y aRp, contrariamente a la hipótesis.

II. Cuando e es divisible por p, la demostración puede prepararse de modo semejante y puede ser desarrollada sin dificultad por los expertos (para quienes se escribió este artículo). Por brevedad la omitimos.

La resolución del problema general.

146.

Por el teorema fundamental y las proposiciones pertenecientes a los residuos -1 y ± 2, siempre puede determinarse si un número dado cualquiera es un residuo o un no residuo de un número primo dado. Pero será útil presentar de una manera clara lo que hemos dicho arriba para que se tenga reunido todo lo necesario para la resolución.

PROBLEMA. *Propuestos dos números cualesquiera P y Q, descubrir si uno de ellos Q es un residuo o no residuo del otro P.*

Resolución. I. Sea $P = a^\alpha b^\beta c^\gamma$ etc. donde a, b, c, etc. denotan números primos diferentes positivos (puesto que se toma el valor absoluto de P). Por brevedad, en este artículo hablaremos simplemente de una *relación* de dos números x e y si el

*) Si no hubiera factores de una clase, debería escribirse 1 en vez del producto de ellos.

primero x es un residuo o no residuo de y. Por tanto, la relación de Q y P depende de las relaciones de Q y a^α; Q y b^β etc. (art. 105).

II. Para saber la relación de Q y a^α (y de los restantes Q y b^β etc.) deben distinguirse dos casos.

1. Cuando Q es divisible por a. Póngase $Q = Q'a^e$ de manera que Q' no sea divisible por a. Entonces si $e = \alpha$ o $e > \alpha$ tendremos QRa^α, pero si $e < \alpha$ e impar tendremos QNa^α: finalmente si $e < \alpha$ y par, Q tendrá con a^α la misma relación que tiene Q' con $a^{\alpha-e}$. Así este caso se reduce al caso:

2. Cuando Q no es divisible por a. Aquí de nuevo distinguimos dos casos.

(A) Cuando $a = 2$. Entonces siempre tendremos QRa^α cuando $\alpha = 1$; pero cuando $\alpha = 2$, se requiere que Q sea de la forma $4n + 1$. Finalmente, cuando $\alpha = 3$ o > 3, Q debe ser de la forma $8n + 1$. Si se cumple esta condición tendremos QRa^α.

(B) Cuando a es algún otro número primo. Entonces Q tendrá con a^α la misma relación que tiene con a. (Véase art. 101).

III. Investíguese la relación de un número cualquiera Q con un número primo (impar) a de la manera siguiente. Cuando $Q > a$, sustitúyase en lugar de Q el menor residuo positivo de él según el módulo a*). Este tendrá la misma relación con Q que tiene a.

Ahora resuélvase Q, o el número tomado en su lugar, en sus factores primos p, p', p'', etc., adjuntando el factor -1 cuando Q es negativo. Entonces resulta que la relación de Q con a depende de las relaciones de cada uno de p, p', p'', etc. con a. A saber, si entre aquellos factores, $2m$ son no residuos de a, resultará QRa, pero si son $2m + 1$ factores, tendremos QNa. Se nota fácilmente que si entre los factores p, p', p'', etc. dos o cuatro o seis de ellos o en general $2k$ resultan iguales, ellos pueden con seguridad eliminarse.

IV. Si entre los factores p, p', p'' se encuentran -1 y 2, la relación de éstos con a puede encontrarse en los artículos 108, 112, 113, 114. La relación de los restantes con a depende de las relaciones de a con ellos (teorema fundamental y proposiciones del art. 131). Sea p uno de ellos, y se encontrará (tratando los números a y p del mismo modo como antes se trataron Q y a, que eran respectivamente mayores) que la relación de a con p o puede determinarse mediante los artículos 108–114 (si en efecto el menor residuo de a (mod. p) no tiene ningún factor primo impar), o depende de la relación de p con ciertos números primos menores que p. Lo mismo vale para los restantes factores p', p'', etc. Ahora se ve fácilmente que continuando con esta

*) Residuo en el sentido del art. 4. En general conviene tomar el menor residuo *absoluto.*

operación finalmente se llega a números cuyas relaciones pueden determinarse por las proposiciones de los art. 108–114. Con un ejemplo será más claro.

Ejemplo. Se quiere la relación del número $+453$ con 1236. Tenemos $1236 = 4 \cdot 3 \cdot 103$; $+453R4$ por II.2(A); $+453R3$ por II.1. Por lo tanto queda examinar la relación de $+453$ con 103. Ella será la misma que tendrá $+41$ ($\equiv 453 \pmod{103}$) con 103; la misma que $+103$ con 41 (teorema fundamental) o sea de -20 con 41. Pero $-20R41$; puesto que $-20 = -1 \cdot 2 \cdot 2 \cdot 5$; $-1R41$ (art. 108); y $+5R41$ porque $41 \equiv 1$ y es un residuo de 5 (teorema fundamental). De esto se sigue que $+453R103$, y finalmente de esto $+453R1236$. Y es cierto que $453 \equiv 297^2 \pmod{1236}$

Sobre las formas lineales que contienen todos los números primos de los cuales un número dado cualquiera es un residuo o no residuo.

147.

Dado un número cualquiera A, pueden presentarse ciertas *fórmulas* bajo las cuales estarán contenidos todos los números primos a A de los cuales el residuo es A, o sea todos los que pueden ser *divisores* de los números de la forma $x^2 - A$ (denotando x^2 como un cuadrado indeterminado)*). Pero por brevedad examinaremos únicamente los divisores que son impares y primos a A, puesto que los restantes fácilmente pueden reducirse a este caso.

Primero, sea A o un número primo positivo de la forma $4n + 1$, o negativo de la forma $4n - 1$. Entonces, según el teorema fundamental, todos los números primos que, tomados positivamente, son residuos de A, serán divisores de $x^2 - A$; todos los números primos (excepto el número 2 que siempre es divisor), que son no residuos de A serán no divisores de $x^2 - A$. Denótense todos los residuos de A menores que A (excluyendo cero) por r, r', r'', etc.; todos los no residuos por n, n', n'', etc. Entonces cualquier número primo contenido en alguna de las formas $Ak + r$, $Ak + r'$, $Ak + r''$, etc. será divisor de $x^2 - A$, pero cualquier primo contenido en alguna de las formas $Ak + n$, $Ak + n'$, etc. será un no divisor, k es un número entero indeterminado. Llamamos *formas de los divisores de* $x^2 - A$ a las primeras, y *formas de los no divisores* a las segundas. El número de cada una de las dos será $\frac{1}{2}(A - 1)$. Ahora, si B es un número compuesto impar y ARB, todos los factores primos de B estarán contenidos en alguna de las primeras formas y por tanto lo estará B mismo. Por lo

*) De este modo, simplemente llamaremos a estos números los *divisores* de $x^2 - A$; es claro cuales son los *no divisores.*

que *cualquier* número impar contenido en una forma de los no divisores, será un no divisor de la forma $x^2 - A$. Pero este teorema no puede invertirse puesto que, si B es un no divisor compuesto impar de la forma $x^2 - A$, habrá entre los factores primos de B algunos no divisores. Si el número de ellos es *par,* B mismo se encontrará en alguna forma de los divisores. Véase art. 99.

Ejemplo. Para $A = -11$ se encuentran éstas : $11k + 1$, 3, 4, 5, 9 como las formas de los divisores de $x^2 + 11$, mientras que las formas de los no divisores serán $11k+2$, 6, 7, 8, 10. Por lo tanto, -11 será un no residuo de todos los números impares que están contenidos en algunas de las segundas formas, pero será un residuo de todos los primos pertenecientes a algunas de las primeras formas.

Se presentarán formas semejantes para divisores y no divisores de $x^2 - A$, donde A denota un número cualquiera. Pero se observa fácilmente que conviene considerar los valores de A que no sean divisibles por ningún cuadrado. En efecto, si $A = a^2A'$, todos los divisores*) de $x^2 - A$ también serán divisores de $x^2 - A'$, y de modo semejante los no divisores. Distinguiremos tres casos, 1) cuando A es de la forma $+(4n + 1)$ o $-(4n - 1)$. 2) cuando A es de la forma $-(4n + 1)$ o $+(4n - 1)$. 3) cuando A es par o sea de la forma $\pm(4n + 2)$.

148.

Primer caso, cuando A es de la forma $+(4n+1)$ o $-(4n-1)$. Resuélvase A en sus factores primos y asígnese a los que son de la forma $4n+1$ el signo positivo, y a los de la forma $4n - 1$, el signo negativo (de donde el producto de todos ellos será $= A$). Sean a, b, c, d, etc. estos factores. Distribúyanse todos los números menores que A y primos a A en dos clases: en la primera clase, todos los números que son no residuos o de ninguno de los números a, b, c, d, etc., o de dos, o de cuatro, o en general de un número par de ellos; en la segunda clase, los que son no residuos de uno de los números a, b, c, etc., o de tres etc., o generalmente de un número impar de ellos. Se denotarán los primeros por r, r', r'', etc.; los últimos por n, n', n'', etc. Entonces las formas $Ak + r$, $Ak + r'$, $Ak + r''$, etc. serán formas de los divisores de $x^2 - A$, y las formas $Ak + n$, $Ak + n'$, etc. serán formas de los no divisores de $x^2 - A$ (i.e., *un número primo cualquiera, aparte de* 2*, será divisor o no divisor de* $x^2 - A$ *según que esté contenido en alguna de las primeras formas o de las segundas respectivamente*). En efecto, si p es un número primo positivo y un residuo o no residuo de uno de

*) A saber, que sean primos a A.

los números a, b, c, etc., este mismo número será un residuo o un no residuo de p (teorema fundamental). Por lo tanto, si entre los números a, b, c, etc. hay m de los cuales p es un no residuo, otros tantos serán no residuos de p; de donde, si p está contenido en alguna de las primeras formas, m será par y ARp, pero si lo está en alguna de las últimas, m será impar y ANp.

Ejemplo. Sea $A = +105 = (-3)(+5)(-7)$. Entonces los números r, r', r'', etc. serán éstos: 1, 4, 16, 46, 64, 79 (que son no residuos de ninguno de los números 3, 5 y 7); 2, 8, 23, 32, 53, 92 (que son no residuos de los números 3 y 5); 26, 41, 59, 89, 101, 104 (que son no residuos de los números 3 y 7); 13, 52, 73, 82, 97, 103 (que son no residuos de los números 5 y 7). Los números n, n', n'', etc. serán éstos: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Los primeros seis son no residuos de 3, los seis posteriores no residuos de 5, luego siguen los no residuos de 7 y finalmente los que son no residuos de todos los tres a la vez.

Se deduce fácilmente de la teoría de combinaciones y de los artículos 32 y 96, que el número de enteros r, r', r'', etc. será:

$$= t(1 + \frac{l(l-1)}{1 \cdot 2} + \frac{l(l-1)(l-2)(l-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots)$$

el número de enteros n, n', n'', etc. será:

$$= t(l + \frac{l(l-1)(l-2)}{1 \cdot 2 \cdot 3} + \frac{l(l-1) \cdots (l-4)}{1 \cdot 2 \cdots 5} + \cdots)$$

donde l denota el número de enteros a, b, c, etc.;

$$t = 2^{-l}(a-1)(b-1)(c-1) \text{ etc.}$$

y se deben continuar ambas series hasta que se paren. (En efecto, se presentarán t números que son residuos de todos los a, b, c, etc., $\frac{t \cdot l(l-1)}{1 \cdot 2}$ que son no residuos de dos, etc., pero la brevedad no permite explicar esta demostración ampliamente). La suma*) de cada una de las series es $= 2^{l-1}$. De hecho, la primera proviene de ésta

$$1 + (l-1) + \frac{(l-1)(l-2)}{1 \cdot 2} + \cdots$$

sumando el segundo y tercer término, el cuarto y el quinto etc.; la segunda se deriva de esta misma, sumando el primer término y el segundo, el tercero y el cuarto etc. Por tanto se presentarán tantas formas divisores de $x^2 - A$ como se presentan formas no divisores, a saber $\frac{1}{2}(a-1)(b-1)(c-1)$ etc.

*) Desechado el factor t.

149.

Podemos contemplar a la vez el *segundo y tercer caso.* De hecho A siempre puede ponerse $= (-1)Q$, o $= (+2)Q$, o $= (-2)Q$, donde Q designa un número de la forma $+(4n+1)$, o $-(4n-1)$, los cuales consideramos en el artículo precedente. Sea en general $A = \alpha Q$ de manera que también $\alpha = -1$ o $\alpha = \pm 2$. Entonces A será un residuo de todos los números de los cuales ambos α y Q son residuos, o ambos no residuos; pero será un no residuo de todos los números de los cuales únicamente uno u otro de los números α y Q es un no residuo. De esto, las formas de los divisores y de los no divisores de $x^2 - A$ se derivan fácilmente. Si $\alpha = -1$, se distribuyen todos los números menores que $4A$ y primos al mismo en dos clases: en la primera, los que están en alguna forma de los divisores de $x^2 - Q$ y a la vez de la forma $4n+1$, junto con los que están en alguna forma de los no divisores de $x^2 - Q$ y al mismo tiempo de la forma $4n+3$; en la segunda, todos los demás. Sean los miembros de la primera clase r, r', r'', etc.; los de la segunda n, n', n'', etc. A será un residuo de todos los números primos contenidos en alguna de las formas $4Ak + r$, $4Ak + r'$, $4Ak + r''$, etc. y un no residuo de todos los números primos contenidos en alguna de las formas $4Ak + n$, $4Ak + n'$, etc. Si $\alpha = \pm 2$, distribúyanse todos los números menores que $8Q$ y primos al mismo, en dos clases: en la primera, los que están contenidos en alguna forma de los divisores de $x^2 - Q$ y a la vez en alguna de las formas $8n+1$ y $8n+7$ para el signo superior, o de las formas $8n+1$ y $8n+3$ para el inferior, junto con los que están contenidos en alguna forma de los no divisores de $x^2 - Q$ y al mismo tiempo en alguna de estas formas $8n+3$ y $8n+5$ para el signo superior, o de éstas $8n+5$ y $8n+7$ para el inferior; en la segunda clase, todos los demás. Entonces, denotados los números de la primera clase por r, r', r'', etc., y los números de la segunda clase por n, n', n'', etc., $\pm 2Q$ será un residuo de todos los números primos contenidos en alguna de las formas $8Qk + r$, $8Qk + r'$, $8Qk + r''$, etc.; pero un no residuo de todos los primos en alguna de las formas $8Qk + n$, $8Qk + n'$, $8Qk + n''$, etc. Además, puede demostrarse fácilmente que aquí también hay tantas formas divisores de $x^2 - A$ como no divisores.

Ejemplo. De este modo se encuentra que $+10$ es un residuo de todos los números primos contenidos en alguna de las formas $40k + 1$, 3, 9, 13, 27, 31, 37, 39; pero un no residuo de todos los primos contenidos en alguna de las formas $40k + 7$, 11, 17, 19, 21, 23, 29, 33.

150.

Estas formas tienen muchas propiedades bastante notables, de las cuales, sin embargo, indicamos únicamente una. Si B es un número compuesto, primo a A, tal que $2m$ de sus factores primos estén contenidos en alguna forma de los no divisores de $x^2 - A$, B estará contenido en alguna forma divisor de $x^2 - A$; pero si el número de factores primos de B contenidos en alguna forma de los no divisores de $x^2 - A$ es impar, B también estará contenido en una forma de los no divisores. Omitimos la demostración que no es difícil. De esto, sigue que no sólo cada número primo sino también todo número impar primo a A, que está contenido en alguna forma de los no divisores, será un no divisor, pues necesariamente algún factor primo de tal número debe ser un no divisor.

Sobre los trabajos de otros acerca de estas investigaciones.

151.

El teorema fundamental, que ha sido considerado como uno de los más elegantes de este género, no ha sido presentado hasta ahora en la forma tan simple como está enunciado arriba. Esto tiene que sorprendernos aún más; ya que otras proposiciones fundamentadas en él, de las cuales hubiera podido deducirse fácilmente el teorema, ya eran conocidas por el ilustre Euler. Sabía que existen ciertas formas en las cuales están contenidos todos los divisores primos de los números de la forma $x^2 - A$, y otras formas en las cuales están comprendidos todos los no divisores primos de los mismos números, de tal manera que unas excluyan las otras y había descubierto un método para hallar estas formas. Pero todos sus esfuerzos para hallar una demostración fueron en vano, y sólo dió un poco de validez a lo que había descubierto por inducción. En una memoria titulada *Novae demostrationes circa divisores numerorum formae* $xx + nyy$, que fue presentada en la academia de San Petersburgo el 20 de noviembre de 1775, y que fue conservada después de la muerte de este hombre ilustre en T. I. *Nov. Act.* de esta academia p. 47 y siguientes, parece haber creído que había logrado sus propósitos, pero se cometió un error. En efecto en la p. 65 está supuesto tácitamente que existen tales formas de los divisores y de los no divisores*), de donde no era difícil derivar *cuales* deben ser; pero el método que

*) A saber, existen números r, r', r'', etc., n, n', n'', etc., todos diferentes y $< 4A$ tales que todos los divisores primos de $x^2 - A$ estén contenidos en alguna de las formas $4Ak + r$, $4Ak + r'$, etc. y todos los no divisores primos en alguna de éstas $4Ak + n$, $4Ak + n'$, etc. (donde k es un número indeterminado).

él usó para comprobar esta proposición no parece idóneo. En otra obra, *De criteriis aequationis* $fxx + gyy = hzz$ *utrumque resolutionem admittat necne,* Opusc. Anal. T. I. (donde f, g, h son dados, x, y, z indeterminados) él descubrió por inducción que si la ecuación era resoluble para algún valor de $h = s$, también era resoluble para todo valor primo congruente a s según el módulo $4fg$. De esta proposición, la suposición sobre la cual hemos hablado puede demostrarse sin mucha dificultad. Pero la demostración de este teorema también eludió sus esfuerzos*), lo cual no es raro ya que a nuestro juicio se debía proceder a partir del teorema fundamental. Además, la verdad de esta proposición saldrá con espontaneidad de lo que enseñaremos en la siguiente sección.

Después de Euler, el gran Lagrange trabajó activamente en el mismo argumento en el distinguido tratado *Recherches d'analyse indéterminée,* Hist.de l'Ac. des Sc., 1785, p. 465 y los siguientes, donde llegó al teorema que si se observa es idéntico al teorema fundamental. En efecto, al designar p y q dos números primos positivos, los residuos absolutamente mínimos de las potencias $p^{\frac{q-1}{2}}$ y $q^{\frac{p-1}{2}}$ según los módulos q y p respectivamente serán ambos $+1$ o ambos -1 cuando p o q sea de la forma $4n + 1$. Pero cuando tanto p como q sean de la forma $4n + 3$, un residuo mínimo será $+1$, y el otro -1, p. 516, de lo que, según el artículo 106, se deriva que *la relación* (en el significado del art. 146) de p a q y de q a p es *la misma* cuando o p o q sea de la forma $4n + 1$; *la opuesta* cuando tanto p como q sean de la forma $4n + 3$. Esta proposición está contenida entre las proposiciones del artículo 131 y sigue también de las proposiciones 1, 3 y 9 del art. 133; alternativamente el teorema fundamental puede derivarse de ella. El gran Legendre también intentó una demostración, sobre la cual, puesto que es muy ingeniosa, hablaremos ampliamente en la siguiente sección. Sin embargo, ya que en ella se suponen muchas cosas sin demostración (como él mismo confiesa p. 520: *Nous avons supposé seulement* etc.), algunas de las cuales hasta ahora no han sido demostradas por nadie, y otras, según nuestro juicio, no pueden demostrarse sin el teorema fundamental mismo, parece que el método que siguió no se puede llevar a su fin, y que nuestra demostración tendrá que ser la primera. Además más abajo presentaremos *otras dos demostraciones* del

*) Como él mismo confiesa, l. c. p. 216: "Una demostración de este muy elegante teorema se desea todavía, aunque se ha investigado en vano durante mucho tiempo. Por tal razón será considerado excelentísimo el que tenga el éxito de encontrar la demostración de este teorema." Con cuánto ardor este hombre inmortal buscaba la demostración de este teorema y de otros que son solamente casos especiales del teorema fundamental, puede verse en muchos otros lugares, e.g., Opuscula Analytica, I, (*Additamentum ad Diss.* VIII) y II, (*Diss.* XIII) y en varias disertaciones en Comm. acad. Petrop. que hemos citado en varias ocasiones.

importante teorema, diferentes de la anterior y diferentes entre sí.

Sobre las congruencias no puras del segundo grado.

152.

Hasta este momento hemos tratado la congruencia pura $x^2 \equiv A \pmod{m}$ y hemos enseñado a determinar si es resoluble o no. La investigación de las *raíces mismas* se reduce por el artículo 105 al caso donde m o es primo o la potencia de un primo; pero el segundo por art. 101 se reduce al caso donde m es primo. Para este caso, lo que presentamos en el artículo 61 y siguientes junto con lo que enseñaremos en las Secciones V y VIII, comprende todo lo que puede hacerse por métodos directos. Sin embargo, éstos son infinitamente más prolijos donde son aplicables que los indirectos que enseñaremos en la Sección VI, y por tanto son memorables no tanto por su utilidad en la práctica sino por su propia belleza. *Las congruencias no puras del segundo grado* fácilmente pueden reducirse a las puras. Dada la congruencia

$$ax^2 + bx + c \equiv 0$$

para resolverse según el módulo m, equivaldrá a la congruencia

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$$

i.e., cualquier número que satisfaga una de ellas también satisfará la otra. Pero esta segunda puede ponerse de la forma

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}$$

de donde todos los valores de $2ax + b$ menores que $4am$ pueden encontrarse si es que existen. Si designamos éstos por r, r', r'', etc., todas las soluciones de la congruencia propuesta podrán deducirse de las soluciones de las congruencias

$$2ax \equiv r - b, \quad 2ax \equiv r' - b, \quad \text{etc.} \pmod{4am}$$

las cuales aprendimos a encontrar en la Sección II. Además, observamos que la solución puede acortarse bastante mediante varios artificios; por ejemplo, en lugar de la congruencia propuesta puede encontrarse otra

$$a'x^2 + 2b'x + c' \equiv 0$$

que le sea equivalente, y en la cual a' divida a m; la brevedad no permite aquí explicarlo, pero puede referirse a la última sección.