Sección Cuarta

SOBRE

LAS CONGRUENCIAS DE SEGUNDO GRADO

Residuos y no residuos cuadráticos.

94.

TEOREMA. *Al tomar un número cualquiera m como módulo, de los números* 0, 1, 2, 3 , $\ldots m-1$, *más de* $\frac{1}{2}m+1$ *no pueden ser congruentes a un cuadrado si* m *es par, ni más de* $\frac{1}{2}m+\frac{1}{2}$ *pueden serlo cuando* m *es impar.*

Demostración. Puesto que los cuadrados de números congruentes son congruentes, cualquier número que pueda ser congruente a algún cuadrado, también será congruente a algún cuadrado cuya raíz sea $< m$. Por consiguiente, basta considerar los residuos mínimos de los cuadrados 0, 1, 4, 9 , $\ldots (m-1)^2$. Pero se nota fácilmente que $(m-1)^2$ es $\equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, etc. De aquí también, cuando m es par, los residuos mínimos de los cuadrados $(\frac{1}{2}m-1)^2$ y $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ y $(\frac{1}{2}m+2)^2$, etc. serán los mismos: cuando m es impar, los cuadrados $(\frac{1}{2}m-\frac{1}{2})^2$ y $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ y $(\frac{1}{2}m+\frac{3}{2})^2$, etc. serán congruentes. De donde es evidente que otros números no pueden ser congruentes a un cuadrado, mas que aquéllos que sean congruentes a alguno de los cuadrados 0, 1, 4, 9 , $\ldots (\frac{1}{2}m)^2$ cuando m es par; y cuando m es impar, cualquier número que sea congruente a algún cuadrado necesariamente es congruente a alguno de los números 0, 1, 4, 9 , $\ldots (\frac{1}{2}m-\frac{1}{2})^2$. Por lo tanto, en el primer caso se presentarán a lo sumo $\frac{1}{2}m+1$ residuos mínimos diferentes; en el segundo caso a lo sumo $\frac{1}{2}m+\frac{1}{2}$. *Q. E. D.*

Ejemplo. Según el módulo 13, los números 0, 1, 4, 9, 3, 12, 10 se encuentran como los residuos mínimos de los cuadrados de 0, 1, 2, 3, $\ldots 6$; después de esto

aparecen en el orden inverso 10, 12, 3 etc. Por lo tanto, si algún número no es congruente a ninguno de estos residuos mínimos, o sea, no es congruente a ninguno de 2, 5, 6, 7, 8, 11, entonces no puede ser congruente a ningún cuadrado.

Según el módulo 15 se encuentran los residuos 0, 1, 4, 9, 1, 10, 6, 4; después de esto aparecen en el orden inverso. Aquí, por lo tanto, el número de residuos que pueden ser congruentes a un cuadrado es menor que $\frac{1}{2}m + \frac{1}{2}$, puesto que son 0, 1, 4, 6, 9, 10. Pero los números 2, 3, 5, 7, 8, 11, 12, 13, 14, y los que son congruentes a alguno de éstos, no pueden ser congruentes a ningún cuadrado según el módulo 15.

95.

De esto resulta que para cualquier módulo, todos los números pueden separarse en dos clases, una de las cuales contiene los números que pueden ser congruentes a algún cuadrado, la otra contiene los que no pueden serlo. Llamaremos a los primeros *residuos cuadráticos* del número que tomamos como módulo*), y los segundos *no residuos cuadráticos,* o también, cuando no se origina ambigüedad alguna simplemente *residuos* y *no residuos.* Es claro que basta poner en clases a los números 0, 1, 2, $\ldots m-1$, puesto que todos los números congruentes deberán pertenecer a una misma clase.

Iniciaremos esta investigación con los módulos primos, lo cual deberá por consiguiente entenderse aunque no se exprese verbalmente. Hay que excluir el número primo 2: se considerarán solamente los números primos *impares.*

Cuando el módulo es un número primo, el número de residuos menores que el módulo es igual al número de no residuos menores.

96.

Al tomar un número primo p como módulo, la mitad de los números 1, 2, 3, $\ldots p-1$ *serán residuos cuadráticos, los restantes serán no residuos, i.e., se presentarán* $\frac{1}{2}(p-1)$ *residuos y otros tantos no residuos.*

---

*) En este caso, propiamente lo usamos con un sentido diferente al que hemos uasado hasta ahora. En efecto, conviene decir: r es un residuo del cuadrado a^2 según el módulo m cuando $r \equiv a^2 \pmod{m}$. Pero, por brevedad, en esta sección decimos siempre que r es un residuo cuadrático de m mismo, para no tener ninguna ambigüedad. Entonces desde ahora en adelante no usaremos la expresión *residuo* para denotar un número congruente, salvo si se trata de residuos *mínimos* donde no pueda haber duda alguna.

De hecho, se demuestra fácilmente que todos los cuadrados 1, 4, 9, $\ldots \frac{1}{4}(p-1)^2$ son incongruentes. En efecto, si pudiera ser $r^2 \equiv (r')^2 \pmod{p}$ y los números r, r' distintos y no mayores que $\frac{1}{2}(p-1)$, poniendo $r > r'$, resultaría $(r-r')(r+r')$ positivo y divisible por p. Pero cada factor $r-r'$ y $r+r'$ es menor que p, por tanto la suposición no puede valer (art. 13). Así, se tienen $\frac{1}{2}(p-1)$ residuos cuadráticos contenidos entre los números 1, 2, 3 , $\ldots p-1$; de hecho, no puede haber más de ellos puesto que al agregar el residuo 0, se producen $\frac{1}{2}(p+1)$ de ellos, y este número no puede exceder el número de todos los residuos. Por consiguiente, los restantes números serán no residuos y el número de ellos $= \frac{1}{2}(p-1)$.

Puesto que cero siempre es un residuo, lo excluimos de nuestras investigaciones, lo mismo que a los números divisibles por el módulo. Puesto que este caso es claro por sí mismo, únicamente dificultaría la simetría del teorema. Por las mismas razones también hemos excluido el módulo 2.

97.

Puesto que mucho de lo que expondremos en esta sección también podrá derivarse de los principios de las secciones anteriores, y como no es inútil estudiar a fondo la misma verdad por medio de métodos diferentes, explicaremos esta relación. Se comprende fácilmente que todos los números congruentes a un cuadrado tienen índices *pares*; mientras que los que no pueden de ningún modo ser congruentes a un cuadrado, los tienen impares. Puesto que $p-1$ es un número par, tantos índices serán pares como impares, a saber $\frac{1}{2}(p-1)$, y entonces se presentarán tantos residuos como no residuos.

Ejemplo. Para el módulo..... los residuos son

3..... 1.
5..... 1, 4.
7..... 1, 2, 4.
11..... 1, 3, 4, 5, 9.
13..... 1, 3, 4, 9, 10, 12.
17..... 1, 2, 4, 8, 9, 13, 15, 16
etc.

y el resto de los números menores que el módulo son no residuos.

La cuestión de si un número compuesto es un residuo o un no residuo de un número primo dado depende de la naturaleza de los factores.

98.

TEOREMA. *El producto de dos residuos cuadráticos de un número primo p es un residuo; el producto de un residuo con un no residuo es un no residuo; finalmente, el producto de dos no residuos es un residuo.*

Demostración. I. Sean A y B los residuos resultantes de los cuadrados a^2 y b^2 o sea $A \equiv a^2, B \equiv b^2$. El producto AB será congruente al cuadrado del número ab, i.e., es un residuo.

II. Cuando A es un residuo, por ejemplo $\equiv a^2$, pero B es un no residuo, AB será un no residuo. Si fuera un residuo, póngase $AB \equiv k^2$, y sea el valor de la expresión $\frac{k}{a} \pmod{p} \equiv b$; así tendríamos $a^2B \equiv a^2b^2$, de donde $B \equiv b^2$, i.e., B es un residuo, contrariamente a la hipótesis.

Otra demostración. Entre los números 1, 2, 3 , $\ldots p-1$ (el número de ellos $= \frac{1}{2}(p-1)$), multiplíquense por A todos los que sean residuos. Todos los productos serán residuos cuadráticos, y ciertamente todos serán incongruentes. Ahora, si se multiplica el no residuo B por A, el producto no será congruente a ninguno de los productos que ya se tienen; por lo tanto si fuera un residuo, se tendrían $\frac{1}{2}(p+1)$ residuos incongruentes, entre los cuales todavía no está el residuo 0, contrariamente al art. 96.

III. Sean A y B no residuos. Entre los números 1, 2, 3 , $\ldots p-1$, multiplíquense por A todos los que sean residuos. Se tendrán $\frac{1}{2}(p-1)$ no residuos incongruentes entre sí (II); ahora el producto AB no puede ser congruente a ninguno de ellos. Entonces, si fuera un no residuo, se tendrían $\frac{1}{2}(p+1)$ no residuos incongruentes entre sí, contra el art. 96. Por lo tanto el producto etc. *Q. E. D.*

Estos teoremas pueden ser derivados más fácilmente de los principios de la sección anterior. De hecho, puesto que los índices de los residuos siempre son pares, y los índices de los no residuos impares, el índice del producto de dos residuos o de dos no residuos será par, de donde el producto mismo será un residuo. Por el contrario, el índice del producto de un residuo y un no residuo será impar y, por lo tanto, el producto mismo un no residuo.

Cualquier método de demostración también puede aplicarse para estos teoremas: *el valor de la expresión* $\frac{a}{b} \pmod{p}$ *será un residuo cuando los números a y b sean a la vez residuos o a la vez no residuos; al contrario, será un no residuo cuando uno de los números a o b sea un residuo y el otro un no residuo.* También pueden obtenerse al aplicar los teoremas precedentes.

99.

En general, el producto de factores cualesquiera es un residuo ya sea cuando todos los factores son residuos o cuando todos son no residuos y el número de ellos es par. Pero cuando el número de los no residuos que quedan entre los factores es impar, el producto será un no residuo. Así puede decidirse fácilmente si un número compuesto es residuo o no, si de algún modo se conoce cada uno de sus factores. Por lo tanto, hemos incluido solamente los números primos en la tabla II. Esta es la organización de la tabla. En la orilla se han colocado los módulos*), con los números primos consecutivos arriba. Cuando uno de éstos es un residuo de algún módulo, se coloca un guión en el espacio correspondiente a los dos, pero cuando el número primo es un no residuo del módulo, el espacio correspondiente queda en blanco.

Sobre los módulos que son numeros compuestos.

100.

Antes de proceder a temas más difíciles, debemos agregar algo acerca de los módulos no primos.

Si se toma como módulo alguna potencia p^n del número primo p (donde suponemos que p no es 2) la mitad de todos los números no divisibles por p y menores que el módulo serán residuos, la otra mitad será no residuos, i.e., el número de cada uno $= \frac{1}{2}(p-1)p^{n-1}$.

De hecho, si r es un residuo, será congruente a algún cuadrado cuya raíz no supera la mitad del módulo, véase art. 94. Ahora se nota fácilmente que se presentan $\frac{1}{2}(p-1)p^{n-1}$ números menores que la mitad del módulo y no divisibles por p. Así, falta demostrar que los cuadrados de todos estos números son incongruentes, o sea producen residuos cuadráticos diferentes. Si los cuadrados de dos números a y b no divisibles por p y menores que la mitad del módulo fueran congruentes, tendríamos $a^2 - b^2$ o sea $(a-b)(a+b)$ divisible por p^n (suponemos que $a > b$). Pero esto no puede suceder a menos que, o bien uno de los números $a-b, a+b$ sea divisible por p^n, lo que no puede ser, puesto que los dos son $< p^n$; o bien uno por p^m y el otro por p^{n-m}, i.e., ambos por p. Pero esto tampoco puede suceder. En efecto, es claro que la suma y diferencia de $2a$ y $2b$ también serían divisibles por p, de donde también a y b, contrariamente a la hipótesis.— De esto se sigue, finalmente, que entre los números no divisibles por p y menores que el módulo se presentan $\frac{1}{2}(p-1)p^n$ residuos;

*) Pronto mostraremos cómo podemos tratar con los módulos compuestos también.

los restantes, que son la misma cantidad, son no residuos. Q.E.D.— Este teorema también puede derivarse de las consideraciones de los índices tal como en el art. 97.

101.

Cualquier número no divisible por p, que es un residuo de p, también será un residuo de p^n; pero si es un no residuo de p, también será un no residuo de p^n.

La última parte de esta proposición es muy clara. Si la primera parte fuera falsa, entre los números menores que p^n y a la vez no divisibles por p, habría más residuos de p que de p^n, i.e., más de $\frac{1}{2}p^{n-1}(p-1)$. Pero, puede verse con facilidad que el número de residuos del número p entre esos números es precisamente $= \frac{1}{2}p^{n-1}(p-1)$.

Es igualmente fácil encontrar explícitamente un cuadrado congruente, según el módulo p^n, a un residuo dado, si se tiene el cuadrado congruente a este residuo según el módulo p.

En efecto, si se tiene un cuadrado a^2 que es congruente al residuo dado A según el módulo p^μ, se puede encontrar un cuadrado congruente a A según el módulo p^ν (donde se supone $\nu > \mu$ e $= $ ó $< 2\mu$) de la siguiente manera. Póngase la raíz del cuadrado deseado $= \pm a + xp^\mu$. Se ve fácilmente que debe tener esta forma, y debe ser $a^2 \equiv \pm 2axp^\mu + x^2p^{2\mu} \equiv A \pmod{p^\nu}$, o sea, puesto que $2\mu > \nu$, $A - a^2 \equiv \pm 2axp^\mu \pmod{p^\nu}$. Si $A - a^2 = p^\mu d$, x será un valor de la expresión $\pm\frac{d}{2a} \pmod{p^{\nu-\mu}}$, que es equivalente a $\pm\frac{A-a^2}{2ap^\mu} \pmod{p^\nu}$.

Por lo tanto, dado un cuadrado congruente a A según el módulo p, se deduce de allí un cuadrado congruente a A según el módulo p^2; de aquí podemos ascender a p^4, de allí a p^8 etc.

Ejemplo. Propuesto el residuo 6 que es congruente al cuadrado 1 según el módulo 5, encontramos que es congruente al cuadrado 9^2 según 25, congruente a 16^2 según 125, etc.

102.

Con respecto a los números divisibles por p, es claro que sus cuadrados serán divisibles por p^2, de donde todos los números divisibles por p pero no por p^2 serán no residuos de p^n. En general, si se propone un número p^kA, donde A no es divisible por p, podemos distinguir los siguientes casos:

1) Cuando $k =$ ó $> n$, tendremos $p^k A \equiv 0 \pmod{p^n}$, i.e., un residuo.

2) Cuando $k < n$ e impar, $p^k A$ será un no residuo.

De hecho, si tuvieramos $p^k A = p^{2\chi+1} A \equiv s^2 \pmod{p^n}$, s^2 sería divisible por $p^{2\chi+1}$ y éste únicamente podría ser el caso si s fuera divisible por $p^{\chi+1}$. Entonces, también s^2 será divisible por $p^{2\chi+2}$ y así también (puesto que en realidad $2\chi + 2$ no es mayor que n) $p^k A$ i.e., $p^{2\chi+1} A$; o sea, A es divisible por p, contrariamente a la hipótesis.

3) Cuando $k < n$ y par. Entonces $p^k A$ será un residuo o un no residuo de p^n, según que A sea un residuo o un no residuo de p. De hecho, cuando A es un residuo de p, será también un residuo de p^{n-k}. Suponiendo que $A \equiv a^2 \pmod{p^{n-k}}$, obtendremos que $Ap^k \equiv a^2 p^k \pmod{p^n}$ y que $a^2 p^k$ es un cuadrado. Pero, cuando A es un no residuo de p, $p^k A$ no puede ser un residuo de p^n. De hecho, si $p^k A \equiv a^2 \pmod{p^n}$, necesariamente a^2 será divisible por p^k. El cociente será un cuadrado congruente a A según el módulo p^{n-k}, de donde también según el módulo p, contrariamente a la hipótesis.

103.

Puesto que hemos excluido el caso $p = 2$, hay que decir algo sobre él. Cuando el número 2 es el módulo, cualquier número será un residuo y ninguno será un no residuo. Pero cuando 4 es el módulo, todos los números impares de la forma $4k + 1$ serán residuos, mientras que todos los de la forma $4k + 3$ serán no residuos. Finalmente, cuando 8 o una potencia mayor del número 2 es el módulo, todos los números impares de la forma $8k + 1$ serán residuos, pero los restantes que son de las formas $8k+3$, $8k+5$, y $8k+7$ serán no residuos. La última parte de esta proposición es clara porque el cuadrado de cualquier número impar, sea bien de la forma $4k + 1$, o bien de la forma $4k - 1$, será de la forma $8k + 1$. La primera parte la demostramos a continuación:

1) Si la suma o diferencia de dos números es divisible por 2^{n-1}, los cuadrados de dichos números serán congruentes según el módulo 2^n. Pues, si se pone uno de ellos $= a$, el otro será de la forma $2^{n-1}h \pm a$, cuyo cuadrado es $\equiv a^2 \pmod{2^n}$.

2) Cualquier número impar que es un residuo cuadrático de 2^n, será congruente a algún cuadrado cuya raíz es un número impar y $< 2^{n-2}$. Sea pues a^2 cualquier cuadrado al cual el número es congruente y sea el número $a \equiv \pm\alpha \pmod{2^{n-1}}$ de manera que α no supere la mitad del módulo (art. 4). Entonces tendremos $a^2 \equiv \alpha^2$,

y el número propuesto será también $\equiv \alpha^2$. Pero entonces es claro que tanto a como α serán impares y $\alpha < 2^{n-2}$.

3) Los cuadrados de todos los números impares menores que 2^{n-2} serán incongruentes según 2^n. De hecho, si r y s son dos números tales, cuyos cuadrados fueran congruentes según 2^n, $(r-s)(r+s)$ sería divisible por 2^n (suponiendo que $r > s$). Pero se ve fácilmente que los números $r-s$ y $r+s$, no pueden ser divisibles a la vez por 4; por lo tanto si uno es divisible sólo por 2, el otro deberá ser divisible por 2^{n-1} para que el producto sea divisible por 2^n. Q.E.A., puesto que cada uno es $< 2^{n-2}$.

4) Si finalmente se reducen estos cuadrados a sus *residuos mínimos positivos,* se obtendrán 2^{n-3} residuos cuadráticos diferentes menores que el módulo*) y cada uno será de la forma $8k+1$. Sin embargo, como existen precisamente 2^{n-3} números de la forma $8k+1$ menores que el módulo, todos estos números deben ser residuos. *Q. E. D.*

Para encontrar un cuadrado congruente a un número dado de la forma $8k+1$ según el módulo 2^n, puede emplearse un método como en el art. 101; véase también art. 88. — Finalmente, lo mismo que hemos expuesto en general en el art. 102 vale para los números pares.

104.

Si A es un residuo de p^n, se deriva con facilidad de lo anterior lo siguiente acerca del número de valores diferentes (i.e., de los incongruentes según el módulo) que admiten una expresión como $V = \sqrt{A} \pmod{p^n}$. (Suponemos, como antes, que el número p es primo y, por brevedad, incluimos aquí el caso $n = 1$).

I. Si A no es divisible por p, V tiene un valor *único* para $p = 2$, $n = 1$, a saber $V = 1$; *dos* valores cuando p es impar, o cuando $p = 2$, $n = 2$, a saber, al poner uno de ellos $\equiv v$, el otro será $\equiv -v$; *cuatro* valores para $p = 2$, $n > 2$, en efecto, al poner uno de ellos $\equiv v$, los restantes serán $\equiv -v$, $2^{n-1} + v$, $2^{n-1} - v$.

II. Si A es divisible por p, pero no por p^n, sea $p^{2\mu}$ la potencia más alta de p que divide a A, (de hecho, es claro que este exponente deberá ser par) y tendremos $A = ap^{2\mu}$. Entonces, es claro que todos los valores de V serán divisibles por p^μ, y los cocientes que resultan de la división serán valores de la expresión $V' = \sqrt{a} \pmod{p^{n-2\mu}}$; de donde producirán todos los valores diferentes de V, al multiplicar

*) Porque el número de enteros impares menores que 2^{n-2} es 2^{n-3}.

todos los valores de la expresión V' situados entre 0 y $p^{n-\mu}$ por p^μ. Por lo tanto se representarán por

$$vp^\mu,\ vp^\mu + p^{n-\mu},\ vp^\mu + 2p^{n-\mu},\ \ldots\ vp^\mu + (p^\mu - 1)p^{n-\mu}$$

donde el valor indeterminado v representa todos los valores *diferentes* de la expresión V', de modo que el número de ellos será p^μ, $2p^\mu$, o $4p^\mu$, según que el número de valores de V' (por el caso I) sea 1, 2 o 4.

III. Si A es divisible por p^n, se ve fácilmente, al colocar $n = 2m$ ó $= 2m-1$, según sea par o impar, que todos los números divisibles por p^m son valores de V y no hay otros. Por consiguiente todos los valores diferentes serán 0, p^m, $2p^m$, $\ldots (p^{n-m} - 1)p^m$ y el número de ellos es p^{n-m}.

105.

Falta el caso donde el módulo m está compuesto de varios números primos. Sea $m = abc\ldots$ donde a, b, c, etc. denotan números primos diferentes o potencias de números primos diferentes. Es claro aquí que si n es un residuo de m, también será n un residuo de cada uno de los números a, b, c, etc., de donde n ciertamente será un no residuo de m, si es un no residuo de alguno de los números a, b, c, etc. Y vice-versa: si n es un residuo de cada uno de a, b, c, etc., también será un residuo del producto m. Pues, al suponer que $n \equiv A^2$, B^2, C^2, etc., mod. a, b, c, etc. respectivamente, es claro, si se deriva un número N congruente a A, B, C, etc. según el módulo a, b, c, etc. respectivamente (art. 32), se tendrá $n \equiv N^2$ según todos estos módulos y también según su producto m. Se nota fácilmente cómo de una combinación de *cualquier* valor de A, es decir $\sqrt{n}$ (mod. a), con *cualquier* valor de B, y con *cualquier* valor de C etc. resulta un valor de N, o de la expresión $\sqrt{n}$ (mod. m). Además, diferentes combinaciones del producto dan diferentes valores de N y todas las combinaciones dan todos los valores de N. El número de todos los diferentes valores de N será igual al producto de los números de valores de A, B, C, etc. que enseñamos a determinar en el artículo anterior. — Además, es claro que si un valor de la expresión $\sqrt{n}$ (mod. m) o de N es conocido, a la vez será éste un valor de A, B, C, etc. Puesto que según el artículo anterior, pueden deducirse todos los restantes valores de estas cantidades, sigue fácilmente que, de un valor de N, pueden obtenerse todos los restantes.

Ejemplo. Sea el módulo 315, del cual se desea saber si 46 es residuo o no residuo. Los divisores primos del número 315 son 3, 5, y 7; y el número 46 es un residuo de cada uno y por tanto también residuo de 315. Además, puesto que $46 \equiv 1$, y $\equiv 64 \pmod 9$; $\equiv 1$ y $\equiv 16 \pmod 5$; $\equiv 4$ y $\equiv 25 \pmod 7$, se encuentran las raíces de los cuadrados a los que 46 es congruente según el módulo 315, que son los números 19, 29, 44, 89, 226, 271, 289, 296.

Criterio general sobre si un número dado es un residuo de un número primo dado.

106.

De lo anterior se concluye: si sólo se puede decidir si un *número primo* dado es un residuo o un no residuo de un *número primo dado,* todos los casos restantes pueden reducirse a esto. Por lo tanto debemos dirigir todos nuestros estudios a investigar criterios verdaderos para este caso. Antes de llevar a cabo esta investigación presentaremos un criterio derivado de la sección anterior, el cual en la práctica casi nunca tiene utilidad, pero que por su simplicidad y generalidad debe mencionarse.

Cualquier número A no divisible por un número primo $2m+1$ es un residuo o no residuo de este número primo según $A^m \equiv +1$ o $\equiv -1 \pmod{2m+1}$.

Sea pues a el índice del número A para el módulo $2m+1$ en un sistema cualquiera; a será par cuando A es un residuo de $2m+1$, e impar cuando es un no residuo. Pero, el índice del número A^m será ma, i.e., $\equiv 0$ o $\equiv m \pmod{2m}$ según a sea par o impar. De aquí finalmente en el primer caso A^m será $\equiv +1$, pero en el siguiente $\equiv -1 \pmod{2m+1}$. Véase artículos 57 y 62.

Ejemplo. 3 es un residuo de 13 ya que $3^6 \equiv 1 \pmod{13}$, pero 2 es un no residuo de 13, puesto que $2^6 \equiv -1 \pmod{13}$.

Tan pronto como los números por examinarse sean moderadamente grandes, este criterio será completamente inútil a causa de la inmensidad del cálculo.

Investigaciones sobre los números primos cuyos residuos o no residuos sean números dados.

107.

Dado un módulo, es muy fácil caracterizar todos los números que son residuos o no residuos. Es claro: si se coloca este número $= m$, deben determinarse los cuadrados cuyas raíces no superan la mitad de m, o también números congruentes a

estos cuadrados según m (en la práctica se presentan métodos más fáciles). Entonces, todos los números congruentes a alguno de éstos según m serán residuos de m, y todos los números no congruentes a ninguno de ellos serán no residuos. — Pero la situación inversa, *propuesto algún número, asignar todos los números, de los cuales aquél sea un residuo o no residuo,* es un obstáculo mucho más grande. Este problema, de cuya solución depende lo que hemos propuesto en el artículo precedente, será estudiado a fondo en lo siguiente, comenzando con los casos más sencillos.

Residuo −1.

108.

TEOREMA. -1 *es un residuo cuadrático de todos los números primos de la forma* $4n+1$*, pero es un no residuo de todos los números primos de la forma* $4n+3$.

Ejemplo. -1 es un residuo de los números 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc. originado de los cuadrados de los números 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, etc. respectivamente; al contrario, es un no residuo de los números 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, etc.

Ya hemos mencionado este teorema en el artículo 64. La demostración se obtiene fácilmente del art. 106. Pues, para un número primo de la forma $4n+1$ se tiene $(-1)^{2n} \equiv 1$, pero para un número de la forma $4n+3$ se tiene $(-1)^{2n+1} \equiv -1$. Esta demostración concuerda con la del artículo mencionado. Sin embargo, por la elegancia y utilidad del teorema, mostraremos otra solución.

109.

Denotamos al conjunto de todos los residuos del número primo p, menores que p, excluyendo el residuo 0, por la letra C. Puesto que el número de estos residuos siempre será $= \frac{p-1}{2}$, es claro que será par si p es de la forma $4n+1$, pero impar si p es de la forma $4n+3$. Por semejanza con el art. 77 donde se hablaba sobre números en general, se llaman *residuos asociados* a dos números cuyo producto $\equiv 1 \pmod{p}$. De hecho, es claro que si r es un residuo, también $\frac{1}{r} \pmod{p}$ será un residuo. Puesto que un mismo residuo no puede tener más asociados entre los residuos C, es evidente que todos los residuos C pueden distribuirse en clases, de las cuales cada una contenga dos residuos asociados. Ahora, es claro, si no se presenta ningún residuo que no esté asociado a sí mismo, i.e., si cada clase contuviera dos residuos *diferentes,* el número de todos los residuos sería el doble del número de todas las clases. Pero, si se presenta

algunos residuos que son sus propios asociados, i.e., algunas clases que contienen un residuo único, o, si se quiere, contienen el mismo residuo dos veces, y si se pone el número de estas clases $= a$, y el número de las restantes $= b$, entonces el número de todos los residuos C será $= a + 2b$. De donde, cuando p es de la forma $4n + 1$, a será un número par. Cuando p es de la forma $4n + 3$, a será impar. Pero, no hay números menores que p, salvo 1 y $p - 1$, que puedan estar asociados consigo mismos (véase art. 77). En el primer caso, 1 está entre los residuos; por lo tanto $p - 1$ (ó -1 que vale lo mismo) debe ser un residuo, pero en el segundo caso, debe ser un no residuo. Pues, en un caso será $a = 1$, y en el otro $= 2$, lo cual es imposible.

110.

También esta demostración se debe al ilustre Euler, quien también encontró por primera vez el método anterior (véase *Opuscula Analytica*, T.1, *p.* 135). Con facilidad, se verá que ella está basada en principios semejantes a los de nuestra segunda demostración del teorema de Wilson (art. 77). Pero si suponemos este teorema, la demostración podría simplificarse mucho. Es claro que entre los números 1, 2, 3 , $\ldots p-1$ habrá $\frac{p-1}{2}$ residuos cuadráticos de p y otros tantos no residuos. Por lo que el número de residuos será par cuando p es de la forma $4n + 1$; impar, cuando p es de la forma $4n + 3$. De aquí concluimos que el producto de todos los números 1, 2, 3, , $\ldots p - 1$ será un residuo en el primer caso, un no residuo en el otro caso (art. 99). Pero este producto siempre $\equiv -1 \pmod{p}$; de donde -1 es un residuo en el primer caso y en el segundo caso será un no residuo.

111.

Así, si r es un residuo de algún número primo de la forma $4n + 1$, también $-r$ será un residuo de este primo; todos los no residuos de tal número se mantendrán como no residuos, aunque se cambie el signo*). Lo contrario vale para los números primos de la forma $4n + 3$, cuyos residuos, cuando se cambia de signo, se convierten en no residuos y viceversa (véase art. 98).

Además de lo que precede, es fácil derivar una regla general: -1 *es un residuo de todos los números no divisibles ni por* 4 *ni por ningún número primo de la forma* $4n + 3$. *El es un no residuo de todos los restantes.* Véanse art. 103 y 105.

*) Por eso, cuando hablamos de cualquier número, sea un residuo o no residuo de un número de la forma $4n + 1$, podremos ignorar completamente el signo o bien emplear el signo doble $\pm$.

Residuos $+2$ *y* -2.

112.

Llegamos a los residuos $+2$ y -2.

Si de la tabla II recogemos todo número primo del cual $+2$ es un residuo, tendremos: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Es fácil observar que entre estos números ninguno es de la forma $8n+3$ ni $8n+5$.

Veamos si de esta inducción puede hacerse una certidumbre.

Notamos primero que todo número compuesto de la forma $8n+3$ u $8n+5$ necesariamente involucra un factor primo de una de las dos formas $8n+3$ u $8n+5$. Pues, es claro que números primos de la forma $8n+1$ u $8n+7$ pueden formar únicamente números que son de la forma $8n+1$ u $8n+7$. Por lo tanto, si nuestra inducción es cierta en general, no se presentará ningún número de la forma $8n+3$ u $8n+5$ cuyo residuo sea $+2$. Pero, ciertamente, no existe ningún número de esta forma menor que 100 del cual $+2$ es un residuo. Sin embargo, si se encuentran tales números más allá de este límite, sea el menor de todos ellos $= t$. Así pues t será o de la forma $8n+3$ o de la forma $8n+5$; $+2$ será un residuo de t, pero un no residuo de todos los números semejantes menores que t. Si se pone $2 \equiv a^2 \pmod{t}$, siempre a podrá tomarse como impar y a la vez $< t$, (puesto que a tendrá al menos dos valores positivos menores que t cuya suma $= t$, de los cuales uno es par y el otro impar, véanse art. 104 y 105). Por la misma razón, sea $a^2 = 2 + tu$, es decir $tu = a^2 - 2$, a^2 será de la forma $8n+1$, tu por lo tanto de la forma $8n-1$, y así u será de la forma $8n+3$ u $8n+5$ según sea t de la segunda forma o de la primera forma. Pero, de la ecuación $a^2 = 2 + tu$ se sigue también que $2 \equiv a^2 \pmod{u}$, i.e., 2 también será un residuo de u. Pero con facilidad se percibe que $u < t$, de donde t no es el número menor en nuestra inducción, contrariamente a la hipótesis. Así se sigue claramente que lo que habíamos encontrado por inducción para el caso general es verdadero.

Al combinar esto con la proposición del art. 111, encontramos los siguientes teoremas:

I. $+2$ *será un no residuo y* -2 *un residuo de todos los números primos de la forma* $8n+3$.

II. *Tanto* $+2$ *como* -2 *serán no residuos de todos los números primos de la forma* $8n+5$.

113.

Mediante una inducción semejante a la de la tabla II se encuentran que -2

es un residuo de los siguientes números primos: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97*). Puesto que ningúno de ellos es de la forma $8n+5$ u $8n+7$, investigaremos entonces si es que esta inducción puede tener la fuerza de un teorema general. Se demuestra de modo semejante al artículo anterior que todo número compuesto de la forma $8n+5$ u $8n+7$ involucra un factor primo de la forma $8n+5$ u $8n+7$, de tal manera que, si nuestra generalización es cierta, -2 no puede ser un residuo de ningún número de la forma $8n+5$ u $8n+7$. Pero si tales números existen, sea el menor de ellos $= t$ y tendremos $-2 = a^2 - tu$. Si como antes se toma a impar y menor que t, u será de la forma $8n+5$ u $8n+7$ según que t sea de la forma $8n+7$ u $8n+5$. Pero de $a^2+2 = tu$ y $a < t$ podrá derivarse fácilmente también que u será menor que t. Finalmente, -2 será un residuo de u, i.e., t no será el menor número de los que -2 es residuo, contradiciendo la hipótesis de nuestra inducción. Por lo que -2 necesariamente es un no residuo de todos los números de las formas $8n+5$ y $8n+7$.

Al combinarse esto con la proposición del art. 111, se obtienen estos teoremas:

I. *Tanto* -2 *como* $+2$ *son no residuos de todos los números primos* $8n+5$, tal como vimos en el artículo anterior.

II. -2 *es un no residuo y* $+2$ *es un residuo de todos los números primos de la forma* $8n+7$.

Además, en ambas demostraciones habríamos podido tomar a como un número par. Pero entonces, habríamos tenido que distinguir el caso donde a fuera de la forma $4n+2$ del caso en donde a fuera de la forma $4n$. El desarrollo procede tal como antes sin dificultad alguna.

114.

Falta el caso en que el número primo es de la forma $8n+1$. Pero esto no se puede resolver por el método anterior y exige artificios muy particulares.

Sea a cualquier raíz primitiva para el módulo $8n+1$, por lo que $a^{4n} \equiv -1 \pmod{8n+1}$ (art. 62). Tal congruencia puede también expresarse en la forma $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n+1}$, o bien por $(a^{2n}-1)^2 \equiv -2a^{2n}$. De donde se sigue que tanto $2a^{2n}$ como $-2a^{2n}$ son residuos de $8n+1$; pero puesto que a^{2n} es un cuadrado no divisible por el módulo, es claro también que tanto $+2$ como -2 serán residuos (art. 98).

*) Esto es considerando a -2 como producto de $+2$ y -1. Véase art. 111.

115.

No será inútil agregar ahora otra demostración de este teorema. Esta guarda una relación con la anterior como la segunda demostración (art. 109) del teorema del art. 108 con la primera (art. 108). Los peritos notarán fácilmente que las dos demostraciones no son tan diferentes como quizás aparentan al principio, tanto en el primer caso como en el segundo.

I. Entre los números 1, 2, 3, ... $4m$ menores que un módulo primo cualquiera de la forma $4m + 1$, aparecerán m números que pueden ser congruentes a un bicuadrado, mientras que los restantes $3m$ no podrán ser congruentes.

Esto se deriva fácilmente de los principios de la sección anterior, pero también sin éstos la demostración es fácil. En efecto, hemos demostrado que para tal módulo -1 siempre es un residuo cuadrático. Sea así $f^2 \equiv -1$. Es claro que si z es un número cualquiera no divisible por el módulo, los bicuadrados de los cuatro números $+z$, $-z$, $+fz$, $-fz$ (se percibe con facilidad que dos cualesquiera de ellos son incongruentes) son congruentes entre sí. Además, es claro que el bicuadrado de un número cualquiera que no es congruente a ninguno de estos cuatro no puede ser congruente a los bicuadrados de ellos (en efecto, la congruencia $x^4 \equiv z^4$, la cual es de cuarto grado, tendría más de cuatro raíces, contrariamente al art. 43). De esto se deduce fácilmente que todos los números 1, 2, 3, ... $4m$ dan lugar a m bicuadrados no congruentes y que entre estos mismos números se encontrarán m números congruentes a éstos, mientras que los restantes no podrán ser congruentes a ningún bicuadrado.

II. Según un módulo primo de la forma $8n + 1$, -1 podrá ser congruente a un bicuadrado (-1 será un *residuo bicuadrático* de este número primo).

De hecho, el número de residuos bicuadráticos menores que $8n+1$ (excluyendo a cero) será $= 2n$, i.e., par. Además, se muestra fácilmente que, si r es un residuo bicuadrático de $8n + 1$, también será un residuo el valor de la expresión $\frac{1}{r} \pmod{8n + 1}$. De esto: todos los residuos bicuadráticos podrán distribuirse en clases de modo semejante a como los distribuimos en el art. 109. La parte restante de la demostración procede exactamente de la misma manera que allí.

III. Ahora, sea $g^4 \equiv -1$ y h un valor de la expresión $\frac{1}{g} \pmod{8n + 1}$. Por tanto, será

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$$

(ya que $gh \equiv 1$). Pero $g^4 \equiv -1$ así que $-h^2 \equiv g^4h^2 \equiv g^2$ de donde $g^2 + h^2 \equiv 0$ y $(g \pm h)^2 \equiv \pm 2$, i.e., tanto $+2$ como -2 son residuos cuadráticos de $8n + 1$. *Q. E. D.*

116.

La siguiente regla general se deduce fácilmente de lo anterior: $+2$ *es un residuo de cualquier número que no puede dividirse ni por* 4 *ni por ningún número primo de la forma* $8n+3$ *u* $8n+5$*, pero es un no residuo de los restantes* (por ejemplo, de todos los números de la forma $8n+3$ y $8n+5$ tanto primos como compuestos).

-2 *es un residuo de cualquier número que no puede dividirse ni por* 4*, ni por ningún primo de la forma* $8n+5$ *u* $8n+7$*; pero de todos los restantes es un no residuo.*

El sagaz Fermat también conoció estos teoremas tan elegantes (*Op. Mathem.,* p. 168). Aunque afirmó tener una demostración, nunca la presentó. Luego, el ilustre Euler la buscó siempre en vano, pero fue el ilustre Lagrange quién logró la primera demostración rigurosa, (*Nouv. Mém. de l'Ac. de Berlin, 1775,* p. 349, 351). El ilustre Euler parece no haberla visto cuando escribió su disertación conservada en su *Opusc. Analyt.,* (T. I., p. 259).

Residuos $+3$ *y* -3.

117.

Pasamos a los residuos $+3$ y -3. Iniciamos con el segundo de ellos.

De la tabla II encontramos que -3 es un residuo de estos números primos: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, entre los cuales no se encuentra ninguno de la forma $6n+5$. Demostramos de la manera siguiente que tampoco afuera de los límites de la tabla existen primos de esta forma, de los cuales -3 es un residuo. Primero, es claro que cualquier número compuesto de la forma $6n+5$ involucra necesariamente algún factor primo de la misma forma. Por lo tanto, hasta el punto en que no exista ningún número primo de la forma $6n+5$ cuyo residuo sea -3, tampoco existirá un número compuesto con esta propiedad. Si tales números existen fuera de los límites de nuestra tabla, sea el menor de todos $= t$ y sea $-3 = a^2 - tu$. Por lo tanto, si a se toma par y menor que t, tendremos $u < t$ y -3 será un residuo de u. Pero cuando a es de la forma $6n \pm 2$, tu será de la forma $6n+1$, de donde u es de la forma $6n+5$. Q. E. A., puesto que hemos supuesto que t es el menor de los números contrariamente a nuestra inducción. Pero cuando a es de la forma $6n$, será tu de la forma $36n+3$, así que $\frac{1}{3}tu$ será de la forma $12n+1$, por lo que $\frac{1}{3}u$ será de la forma $6n+5$; pero es claro que -3 será también un residuo de $\frac{1}{3}u$ aunque $\frac{1}{3}u < t$, Q. E. A. Por lo tanto es claro que -3 no puede ser un residuo de ningún número de la forma $6n+5$.

Ya que cualquier número de la forma $6n+5$ está contenido necesariamente entre aquéllos de la forma $12n+5$ o $12n+11$ y puesto que la primera es de la forma

$4n+1$ y la segunda de la forma $4n+3$, se tienen los siguientes teoremas:

I. *Tanto* -3 *como* $+3$ *son no residuos de cualquier número primo de la forma* $12n+5$.

II. -3 *es un no residuo y* $+3$ *es un residuo de cualquier número primo de la forma* $12n+11$.

118.

Los números que encontramos en la tabla II y que tienen residuo $+3$ son: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97; entre ellos, ninguno es de la forma $12n+5$ o $12n+7$. Puede comprobarse exactamente como en los artículos 112, 113 y 117 que no existe ningún número de las formas $12n+5$ ni $12n+7$ cuyo residuo sea $+3$, por lo que suprimimos este desarrollo. Combinando estos resultados con los del art. 111 tenemos los siguentes teoremas:

I. *Tanto* $+3$ *como* -3 *son no residuos de cualquier número primo de la forma* $12n+5$ (tal como ya encontramos en el artículo anterior).

II. $+3$ *es un no residuo y* -3 *es un residuo de cualquier número primo de la forma* $12n+7$.

119.

Mediante este método, no se puede descubrir nada con respecto a los números de la forma $12n+1$, por lo que exigen artificios particulares. Por una inducción se deduce fácilmente que $+3$ y -3 son residuos de todos los números primos de esta forma. Pero, es claro que debe demostrarse solamente que -3 es un residuo de tales números, ya que necesariamente $+3$ será un residuo (art. 111). Sin embargo demostraremos más generalmente que -3 es un residuo de cualquier número primo de la forma $3n+1$.

Sea p un primo de este tipo y a un número que, para el módulo p, pertenece al exponente 3 (los cuales existen por el art. 54, ya que 3 es divisor de $p-1$). Por eso será $a^3 \equiv 1 \pmod{p}$, i.e., a^3-1 o sea $(a^2+a+1)(a-1)$ será divisible por p. Pero es claro que a no puede ser $\equiv 1 \pmod{p}$, ya que 1 pertenece al exponente 1, por lo que $a-1$ no será divisible por p, pero a^2+a+1 lo será, y de allí también $4a^2+4a+4$, i.e., será $(2a+1)^2 \equiv -3 \pmod{p}$ o sea -3 es un residuo de p. *Q. E. D.*

Además, es evidente que esta demostración (que es independiente de las precedentes) también comprende números primos de la forma $12n + 7$, a los que ya nos referimos en un artículo anterior.

Conviene observar que se podría usar el método de los artículos 109 y 115, pero por brevedad no nos detenemos en estos detalles.

120.

De lo precedente se obtienen fácilmente los siguientes teoremas (ver art. 102, 103 y 105).

I. -3 *es un residuo de todos los números que no pueden dividirse ni por* 8, *ni por* 9, *ni por ningún número primo de la forma* $6n+5$, *y es un no residuo de todos los restantes.*

II. $+3$ *es un residuo de todos los números que no pueden dividirse ni por* 4, *ni por* 9, *ni por ningún primo de la forma* $12n + 5$ *o* $12n + 7$, *y es un no residuo de todos los restantes.*

Se tiene aquí este caso particular:

-3 es un *residuo* de todos los números primos de la forma $3n + 1$, o lo que es lo mismo, *de todos los que son residuos de* 3. Pero es un *no residuo* de todos los números primos de la forma $6n + 5$, o excluido 2, de todos los primos de la forma $3n+2$, *i.e., de todos los primos que son no residuos de* 3. Se ve fácilmente que todos los casos restantes se siguen naturalmente de éste.

Fermat ya conocía las proposiciones sobre los residuos $+3$ y -3, *Opera* de Wallis, T. II, p. 857. Pero el ilustre Euler fue el primero en dar demostraciones, *Comm. nov. Petr.,* T. VIII, p. 105 y siguientes. Esto resulta más admirable puesto que las demostraciones de las proposiciones pertenecientes a los residuos $+2$ y -2 están basadas en artificios bastante parecidos. Véase también el comentario del ilustre Lagrange en *Nouv. Mém. de l' Ac. de Berlin,* 1775, p. 352.

Residuos $+5$ *y* -5.

121.

Por inducción se descubre que $+5$ no es un residuo de ningún número impar de la forma $5n + 2$ o $5n + 3$, i.e., de ningún número impar que sea no residuo de 5. Se demuestra que esta regla no tiene excepción alguna. Sea el número menor que constituya una excepción de esta regla $= t$, éste por lo tanto es un no residuo del

número 5, pero 5 es un residuo de t. Sea $a^2 = 5 + tu$ tal que a sea par y menor que t. Entonces u será impar y menor que t, pero +5 será un residuo de u. Ahora si a no es divisible por 5, tampoco lo será u. Pero es claro que tu es un residuo de 5, por lo que, puesto que t es un no residuo de 5, tampoco lo será u, i.e., existe un no residuo impar del número 5 cuyo residuo es +5, pero menor que t, contrariamente a la hipótesis. Si por otro lado a es divisible por 5, se pone $a = 5b$ y $u = 5v$ de donde $tv \equiv -1 \equiv 4 \pmod 5$, i.e., tv será un residuo del número 5. En lo restante la demostración procede de manera análoga al caso anterior.

122.

Tanto +5 como −5 serán no residuos de todos los números primos que simultáneamente son no residuos de 5 y de la forma $4n+1$, i.e., de todos los números primos de la forma $20n + 13$ o $20n + 17$. Pero +5 será un no residuo y −5 un residuo de todos los números primos de la forma $20n + 3$ o $20n + 7$.

Puede demostrarse de modo parecido que −5 es un no residuo de todos los números primos de las formas $20n + 11$, $20n + 13$, $20n + 17$ y $20n + 19$. Se nota fácilmente de aquí que +5 es un residuo de todos los números primos de la forma $20n+11$ o $20n+19$, pero no residuo de todos los de la forma $20n+13$ o $20n+17$. Puesto que cada número primo, aparte de 2 y 5 (cuyos residuos son ± 5), está contenido en alguna de las formas $20n + 1$, 3, 7, 9, 11, 13, 17, 19, es claro que se puede juzgar ahora a todos, excepto a los que son de la forma $20n + 1$ o de la forma $20n + 9$.

123.

Por inducción se descubre fácilmente que +5 y −5 son residuos de todos los números primos de la forma $20n+1$ o $20n+9$. Ahora bien, si esto es cierto en general, se tendrá una ley elegante, +5 *es un residuo de todos los números primos que sean residuos de* 5 (pues éstos están contenidos en una u otra de las formas $5n+1$ o $5n+4$, o en una de estas otras $20n+1$, 9, 11, 19, de las cuales la tercera y la cuarta ya se han tratado), *pero es un no residuo de todos los números impares que son no residuos de* 5, como ya lo hemos demostrado antes. Ahora es claro que este teorema es suficiente para juzgar si +5 (y también −5 si se considera como producto de +5 y −1) es un residuo o un no residuo de cualquier número dado. Finalmente se observa la analogía de este teorema con aquél que presentamos en el art. 120 sobre el residuo −3.

Pero la verificación de esta inducción no es tan fácil. Cuando se presenta un número primo de la forma $20n + 1$, o más generalmente de la forma $5n + 1$, este asunto puede resolverse de un modo similar al de los artículos 114 y 119. De hecho, sea a un número cualquiera perteneciente al exponente 5 para el módulo $5n + 1$, el cual evidentemente existe por la sección anterior, y se tendrá $a^5 \equiv 1$, o sea $(a-1)(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{5n+1}$. Pero no puede ser $a \equiv 1$, por eso tampoco $a - 1 \equiv 0$; necesariamente será $a^4 + a^3 + a^2 + a + 1 \equiv 0$. Por lo tanto también $4(a^4 + a^3 + a^2 + a + 1) = (2a^2 + a + 2)^2 - 5a^2$ será $\equiv 0$, i.e., $5a^2$ será un residuo de $5n + 1$, de donde también lo será 5, ya que a^2 es un residuo no divisible por $5n + 1$ (pues a no es divisible por $5n + 1$ porque $a^5 \equiv 1$). *Q. E. D.*

Pero el caso donde se presenta un número primo de la forma $5n + 4$ exige artificios más sutiles. Puesto que las proposiciones que necesitamos aquí se tratarán con más generalidad en lo que sigue, aquí lo tocamos brevemente.

I. Si p es un número primo y b un no residuo cuadrático dado de p, el valor de la expresión

$$(A) \ldots \frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$$

(se observa con facilidad que el desarrollo de ésta carece de irracionales) siempre será divisible por p, cualquiera que sea el número que se tome para x. De hecho, es claro de la inspección de los coeficientes que se obtienen del desarrollo de A, que todos los términos desde el segundo al penúltimo (inclusive) son divisibles por p y que $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}$. Pero ya que b es un no residuo de p, será $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, (art. 106); pero x^p siempre es $\equiv x$ (sección anterior), de donde $A \equiv 0$. *Q. E. D.*

II. En la congruencia $A \equiv 0 \pmod{p}$ la indeterminada x tiene exponente p y todos los números 0, 1, 2, $\ldots p-1$ serán raíces de ella. Ahora, tómese a e como un divisor de $p + 1$. La expresión

$$\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$$

(la cual denotamos por B), si se desarrolla, no tendrá irracionales, la indeterminada x tendrá exponente $e - 1$, y resulta de los primeros elementos del análisis que A es divisible (algebraicamente) por B. Ahora digo que existen $e - 1$ valores de x, que sustituidos en B, hacen B divisible por p. En efecto, si $A \equiv BC$, x tendrá exponente $p - e + 1$ en C, y la congruencia $C \equiv 0 \pmod{p}$ tendrá no más que $p - e + 1$ raíces.

De donde resulta evidente que todos los $e-1$ números restantes entre 0, 1, 2, 3, $\ldots p-1$, serán raíces de la congruencia $B \equiv 0$.

III. Ahora supóngase que p es de la forma $5n+4$, $e=5$, b es un no residuo de p, y el número a se determina tal que

$$\frac{(a+\sqrt{b})^5-(a-\sqrt{b})^5}{\sqrt{b}}$$

es divisible por p. Pero esa expresión es

$$= 10a^4+20a^2b+2b^2 = 2((b+5a^2)^2-20a^4)$$

Por lo tanto, también $(b+5a^2)^2-20a^4$ será divisible por p, i.e., $20a^4$ es un residuo de p; pero ya que $4a^4$ es un residuo no divisible por p (de hecho, se comprueba fácilmente que a no puede dividirse por p), también 5 será un residuo de p. *Q. E. D.*

El teorema enunciado en el comienzo de este artículo resulta verdadero.

Notamos que las demostraciones para ambos casos se deben al ilustre Lagrange, *Mém. de l'Ac. de Berlin,* 1775, p. 352 y siguientes.

Sobre ± 7.

124.

Por un método similar se demuestra:

-7 *es un no residuo de cualquier número que sea no residuo de* 7.

Y por inducción se puede concluir:

-7 *es un residuo de cualquier número primo que sea residuo de* 7.

Pero nadie ha demostrado esto rigurosamente hasta ahora. La demostración es fácil para los residuos de 7 cuya forma es $4n-1$; en efecto, por el método conocido del artículo precedente puede mostrarse que $+7$ siempre es un no residuo de tales números primos y así -7 es un residuo. Pero con esto se logra poco, ya que, los casos restantes no pueden tratarse con este método. Sólo podemos resolver un caso de modo similar a los artículos 119 y 123. A saber: si p es un número primo de la forma $7n+1$, y a pertenece al exponente 7 para el módulo p, se observa fácilmente que:

$$\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2+7(a^2+a)^2$$

es divisible por p, de donde $-7(a^2+a)^2$ será un residuo de p. Pero $(a^2+a)^2$, como un cuadrado, es un residuo de p y no divisible por p; puesto que se supone que a pertenece al exponente 7, no puede ser ni $\equiv 0$, ni $\equiv -1 \pmod{p}$, i.e., ni a ni $a+1$ serán divisibles por p, ni tampoco lo será el cuadrado $(a+1)^2a^2$. De donde también es evidente que -7 será un residuo de p. Q.E.D.— Pero los números primos de la forma $7n+2$ o $7n+4$ no se prestan a ninguno de los métodos tratados hasta ahora. Esta demostración también fue encontrada primeramente por el ilustre Lagrange en la misma obra.— Posteriormente, en la Sección VII, enseñaremos más generalmente que la expresión $\frac{4(x^p-1)}{x-1}$ siempre puede reducirse a la forma $X^2 \mp pY^2$ (donde hay que tomar el signo superior cuando p es número primo de la forma $4n+1$ y el inferior cuando es de la forma $4n+3$). Aquí X e Y denotan funciones racionales de x, libres de fracciones. El ilustre Lagrange no desarrolló su análisis más allá del caso $p = 7$ (vea p. 352 de su obra).

Preparación para la investigación general.

125.

Puesto que los métodos precedentes no son suficientes para asegurar las demostraciones generales, es momento para exponer otro método libre de este defecto. Iniciamos con un teorema cuya demostración por mucho tiempo nos eludió, aunque a primera vista parezca tan obvio como para que algunos ni siquiera hayan reconocido la necesidad de una demostración. Es éste: *Cualquier número, excepto los cuadrados tomados positivamente, es un no residuo de algunos números primos.* Pero ya que usamos este teorema solamente como una ayuda para demostrar otros, no explicamos más que aquellos casos que necesitaremos para este fin. Los casos restantes se darán más adelante. Demostremos por tanto que *cualquier número primo de la forma* $4n+1$ *tomado positiva o negativamente**) *es un no residuo de algunos números primos,* y, de hecho, (si es > 5) de algunos primos que son menores que sí mismo.

Primero, cuando se presenta un número primo p de la forma $4n+1$ (> 17; aunque $-13N3$ y $-17N5$) tomado *negativamente,* sea $2a$ el primer número par mayor que $\sqrt{p}$; entonces se ve fácilmente que $4a^2$ siempre será $< 2p$ o sea $4a^2 - p < p$. Pero $4a^2 - p$ es de la forma $4n+3$ mientras que $+p$ es un residuo cuadrático de $4a^2 - p$ (ya que $p \equiv 4a^2 \pmod{4a^2-p}$). Por eso si $4a^2 - p$ es un número primo, $-p$ será un no residuo de él; si no, necesariamente algún factor de $4a^2 - p$ será de la forma $4n+3$; como $+p$ también debe ser un residuo de él, $-p$ será un no residuo. *Q. E. D.*

*) Es claro que $+1$ debe ser excluido.

Para un número primo tomado *positivamente* distinguimos dos casos. *Primero* sea p un número primo de la forma $8n+5$; sea a cualquier número positivo $< \sqrt{\frac{1}{2}p}$. Entonces $8n+5-2a^2$ será un número positivo de la forma $8n+5$ u $8n+3$ (según que a sea par o impar) y por lo tanto necesariamente divisible por algún primo de la forma $8n+3$ u $8n+5$, puesto que el producto de cualquier cantidad de números de la forma $8n+1$ y $8n+7$ no puede tener ni la forma $8n+3$ ni $8n+5$. Sea este producto $= q$, así que $8n+5 \equiv 2a^2 \pmod{q}$. Pero 2 será un no residuo de q (art. 112); así también $2a^2$ *) y $8n+5$. *Q. E. D.*

126.

Que cualquier número primo de la forma $8n+1$ tomado positivamente siempre es un no residuo de algún número primo menor que él, no puede demostrarse por artificios tan obvios. Como esta verdad es de gran importancia, no podemos excluir la demostración rigurosa aunque sea algo prolija. Comencemos como sigue:

LEMA: *Si se tienen dos series de números,*

$$A,\ B,\ C,\ \text{etc.}\ldots.(I), \quad A',\ B',\ C',\ \text{etc.}\ldots.(II)$$

(no interesa si el número de términos en un caso es el mismo que en el otro o no) *confeccionadas de manera que, si p denota un número primo cualquiera o la potencia de un número primo, cuando p divide algún término de la segunda serie (o varios), habrá por lo menos tantos términos de la primera serie divisibles por p. Entonces, afirmo que el producto de todos los números* (I) *será divisible por el producto de todos los números* (II).

Ejemplo. Conste (I) de los números 12, 18, 45; (II) de los números 3, 4, 5, 6, 9. Entonces, si tomamos sucesivamente los números 2, 4, 3, 9, 5, encontramos que hay 2, 1, 3, 2, 1 términos en (I) y 2, 1, 3, 1, 1 términos en (II) que son, respectivamente, divisibles por dichos números y el producto de todos los términos $(I) = 9720$ es divisible por el producto de todos los términos (II), 3240.

Demostración. Sea el producto de todos los términos $(I) = Q$, y el producto de todos los términos de la serie $(II) = Q'$. Es evidente que cualquier número primo que es divisor de Q' también será divisor de Q. Ahora mostraremos que cualquier

*) Art. 98. De hecho a^2 es un residuo de q no divisible por q, pues de lo contrario el número primo p también sería divisible por q. Q.E.A.

factor primo de Q' tiene un grado en Q al menos tan alto como lo tiene en Q'. Sea tal divisor p y supongamos que en la serie (I) hay a términos divisibles por p, b términos divisibles por p^2, c términos divisibles por p^3, etc. Las letras a', b', c', etc. denotan lo similar de la serie (II), y se ve fácilmente que p tiene exponente $a+b+c+$ etc. en Q, y $a'+b'+c'+$ etc. en Q'. Pero ciertamente a' no es mayor que a, b' no es mayor que b etc. (por hipótesis); por lo que $a'+b'+c'+$ etc. ciertamente no será $> a+b+c+$ etc.— Puesto que ningún número primo puede tener mayor exponente en Q' que en Q, Q será divisible por Q' (art. 17). *Q. E. D.*

127.

LEMA: *En la progresión* 1, 2, 3, 4, $\ldots n$ *no puede haber más términos divisibles por cualquier número* h, *que en la progresión* a, $a+1$, $a+2$, $\ldots a+n-1$, *que contiene el mismo número de términos.*

En efecto se nota sin dificultad que si n es un múltiplo de h, en ambas progresiones habrá $\frac{n}{h}$ términos que serán divisibles por h; si n no es múltiplo de h, póngase $n = eh + f$, de manera que f sea $< h$. En la primera serie e términos serán divisibles por h, y en la segunda lo serán e o $e+1$ términos.

Como corolario de esto se sigue una proposición conocida de la teoría de los números figurados; a saber, que

$$\frac{a(a+1)(a+2)\cdots(a+n-1)}{1\cdot 2\cdot 3\cdot \ldots n}$$

siempre es un número entero. Pero si no nos equivocamos, nadie lo ha demostrado directamente.

Finalmente, este lema puede expresarse en forma más general:

En la progresión a, $a+1$, $a+2$, $\ldots a+n-1$ existen por lo menos tantos términos congruentes según el módulo h a un número dado cualquiera r como términos divisibles por h haya en 1, 2, 3, $\ldots n$.

128.

TEOREMA. *Sea* a *un número cualquiera de la forma* $8n+1$, p *cualquier número primo a a cuyo residuo es* $+a$, *y finalmente* m *un número arbitrario: entonces yo afirmo que en la progresión*

$$a,\ \frac{1}{2}(a-1),\ 2(a-4),\ \frac{1}{2}(a-9),\ 2(a-16),\ \ldots 2(a-m^2)\ o\ \frac{1}{2}(a-m^2)$$

según que m sea par o impar, existen por lo menos tantos términos divisibles por p como existan en la progresión:

$$1,\ 2,\ 3,\ \ldots 2m+1$$

Denotamos por (I) la primera progresión, por (II) la segunda.

Demostración. I. Cuando $p = 2$, en (I) todos los términos aparte del primero, i.e., m términos serán divisibles; habrá igual número también en (II).

II. Sea p un número impar, o el doble de un número impar, o el cuádruplo de un número impar, y $a \equiv r^2 \pmod{p}$. Entonces, en la progresión $-m$, $-(m-1)$, $-(m-2)$, $\ldots +m$ (la que tiene el mismo número de términos que (II) y que denotamos por (III)) por lo menos tantos términos serán congruentes a r, según el módulo p, como términos en (II) sean divisibles por p (artículo precedente). Entre ellos no pueden haber dos iguales en magnitud que difieran en signo*). Cada uno de ellos tendrá un valor correspondiente en la serie (I), el cual será divisible por p. Por supuesto, si $\pm b$ es un término de la serie (III) congruente a r según el módulo p, $a - b^2$ será divisible por p. Por lo tanto, si por un lado b es par, el término de la serie (I), $2(a-b^2)$ será divisible por p. Por otro lado, si b es impar, el término $\frac{1}{2}(a-b^2)$ será divisible por p: pues es evidente que $\frac{a-b^2}{p}$ será entero *par,* dado que $a - b^2$ es divisible por 8, pero p es divisible a lo sumo por 4 (de hecho, por hipótesis a es de la forma $8n+1$ y b^2, por ser el cuadrado de un número impar, es de la misma forma; por lo que la diferencia será de la forma $8n$). De esto finalmente se concluye que tantos términos en la serie (I) son divisibles por p, como en (III) sean congruentes a r según el módulo p, i.e., igual número o más de los que son divisibles por p en (II).

III. Sea p de la forma $8n$ y $a \equiv r^2 \pmod{2p}$. Entonces se observa fácilmente que a, que por hipótesis es un residuo de p, será también un residuo de $2p$. Entonces, en la serie (III) habrá por lo menos tantos términos congruentes a r, según p, como en la (II) sean divisibles por p, y todos ellos serán de magnitudes diferentes. Pero a cada uno de ellos corresponderá algún término divisible por p en (I). En efecto, si $+b$ o $-b \equiv r \pmod{p}$, será $b^2 \equiv r^2 \pmod{2p}$ †), de donde el término $\frac{1}{2}(a-b^2)$ será

*) En efecto, si fuera $r \equiv -f \equiv +f \pmod{p}$, $2f$ sería divisible por p; por lo tanto, también $2a$ (puesto que $f^2 \equiv a \pmod{p}$). Pero esto es posible únicamente cuando $p = 2$, pues por hipótesis a es primo a p. Pero sobre este caso ya hemos hablado por separado.

†) De hecho, $b^2 - r^2 = (b-r)(b+r)$ estará compuesto de dos factores, uno de los cuales es divisible por p (hipótesis) y el otro por 2 (puesto que tanto b como r son impares); de donde $b^2 - r^2$ es divisible por $2p$.

divisible por p. Por lo que en (I) serán divisibles por p por lo menos tantos términos como en (II). *Q. E. D.*

129.

TEOREMA. *Si a es un número primo de la forma $8n+1$, necesariamente habrá algún número primo menor que $2\sqrt{a+1}$ del cual a sea un no residuo.*

Demostración. Sea a un residuo de todos los primos menores que $2\sqrt{a+1}$. Entonces, se observará con facilidad que a también será un residuo de todos los números compuestos menores que $2\sqrt{a+1}$ (refiérase a las reglas por las cuales aprendimos a deducir si un número dado es un residuo de un número compuesto o no: art. 105). Sea m el mayor entero menor que $\sqrt{a}$. Entonces en la serie

$$a,\ \frac{1}{2}(a-1),\ 2(a-4),\ \frac{1}{2}(a-9),\ \ldots 2(a-m^2) \text{ o } \frac{1}{2}(a-m^2) \qquad (I)$$

serán divisibles por algún número menor que $2\sqrt{a}+1$ tantos o más términos como en ésta:

$$1,\ 2,\ 3,\ 4,\ \ldots 2m+1 \quad \text{(art. precedente)} \qquad (II)$$

De esto se sigue que el producto de todos los términos en (I) es divisible por el producto de todos los términos en (II) (art. 126). Pero esto o es $= a(a-1)(a-4)\cdots(a-m^2)$ o bien la mitad de este producto (según que m sea par o impar). Por lo que el producto $a(a-1)(a-4)\cdots(a-m^2)$ puede dividirse por el producto de todos los términos en (II), y, puesto que todos estos términos son primos a a, también lo será su producto, omitido el factor a. Pero el producto de todos los términos de (II) también puede presentarse así:

$$(m+1)\cdot((m+1)^2-1)\cdot((m+1)^2-4)\cdot\cdots\cdot((m+1)^2-m^2)$$

Por lo tanto

$$\frac{1}{m+1}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdot\cdots\cdot\frac{a-m^2}{(m+1)^2-m^2}$$

será un número entero, aunque sea un producto de fracciones menores que la unidad: puesto que en efecto $\sqrt{a}$ necesariamente debe ser irracional, será $m+1>\sqrt{a}$. Y por lo tanto $(m+1)^2>a$. De esto finalmente se concluye que nuestra suposición no puede tener lugar. *Q. E. D.*

Ahora, puesto que ciertamente $a>9$, tendremos $2\sqrt{a}+1<a$. Por lo tanto existirá algún primo $<a$ del cual a es un no residuo.

Por inducción se apoya un teorema general (fundamental), y se deducen algunas conclusiones de él.

130.

Después de haber demostrado rigurosamente que cada número primo de la forma $4n + 1$, tomado positivo o negativamente, es un no residuo de algún número primo menor que él mismo, pasamos entonces a una comparación más exacta y más general de los números primos, para ver cuando uno es un residuo o un no residuo del otro.

Con todo rigor, hemos demostrado arriba que -3 y $+5$ son residuos o no residuos de todos los números primos que son residuos o no residuos respectivamente de 3 y 5.

Se encuentra por inducción que los números -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59, etc., son residuos o no residuos de todos los números primos, los cuales tomados positivamente, resultan residuos o no residuos de estos primos respectivamente. Esta inducción puede llevarse a cabo fácilmente con ayuda de la tabla II.

Quienquiera, con un poco de atención, notará que de estos números primos aquéllos con signo positivo son los de la forma $4n + 1$, y los de signo negativo son los de la forma $4n + 3$.

131.

Demostraremos en seguida que lo que descubrimos por inducción tiene lugar en general. Pero, antes de entrar en este trabajo, será necesario extraer todo lo que sigue de este teorema, si se supone verdadero. Enunciamos el teorema mismo así:

Si p es un número primo de la forma $4n + 1$, $+p$ será un residuo o no residuo de cualquier número primo que, tomado positivamente, es un residuo o no residuo del mismo p. Si p es un número primo de la forma $4n + 3$, $-p$ tendrá la misma propiedad.

Ya que casi todo lo que puede decirse sobre los residuos cuadráticos se apoya en este teorema, la denominación *teorema fundamental* que usaremos en lo que sigue no será inconveniente.

Para poder presentar nuestro razonamiento lo más brevemente posible, denotaremos por a, a', a'', etc. los números primos de la forma $4n + 1$, por b, b', b'', etc. los números primos de la forma $4n + 3$; por A, A', A'', etc. los números cualesquiera de la forma $4n + 1$, por B, B', B'', etc. los números cualesquiera de

la forma $4n+3$. Finalmente la letra R puesta entre dos cantidades indicará que la primera es un residuo de la siguiente, mientras que la letra N tendrá el significado contrario. Por ejemplo, $+5R11$, $\pm 2N5$ indicará que $+5$ es un residuo de 11, pero $+2$ y -2 son no residuos de 5. Ahora, al unir el teorema fundamental con los teoremas del art. 111 fácilmente se deducirán las siguientes proposiciones.

	Si		será
1.	$\pm aRa'$	.....	$\pm a'Ra$
2.	$\pm aNa'$	.....	$\pm a'Na$
3.	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right\}$	.....	$\pm bRa$
4.	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right\}$	.....	$\pm bNa$
5.	$\pm bRa$	.....	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right.$
6.	$\pm bNa$	.....	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right.$
7.	$\left\{\begin{matrix}+bRb'\\-bNb'\end{matrix}\right\}$	.....	$\left\{\begin{matrix}+b'Nb\\-b'Rb\end{matrix}\right.$
8.	$\left\{\begin{matrix}+bNb'\\-bRb'\end{matrix}\right\}$	.....	$\left\{\begin{matrix}+b'Rb\\-b'Nb\end{matrix}\right.$

132.

En esta tabla están contenidos todos los casos que pueden ocurrir al comparar dos números primos: lo que sigue corresponderá a números cualesquiera, pero sus demostraciones son menos obvias.

	Si		será
9.	$\pm aRA$	.....	$\pm ARa$
10.	$\pm bRA$	.....	$\left\{\begin{matrix}+ARb\\-ANb\end{matrix}\right.$
11.	$+aRB$	.....	$\pm BRa$
12.	$-aRB$	.....	$\pm BNa$
13.	$+bRB$	.....	$\left\{\begin{matrix}-BRb\\+BNb\end{matrix}\right.$
14.	$-bRB$	.....	$\left\{\begin{matrix}+BRb\\-BNb\end{matrix}\right.$

Puesto que los mismos principios conducen a las demostraciones de todas estas proposiciones, no será necesario desarrollarlas todas: la demostración de la proposición 9 que adjuntamos puede servir como ejemplo. Ante todo se notará que cada número de la forma $4n+1$ puede tener o ningún factor de la forma $4n+3$, o dos, o cuatro, etc., i.e., el número de tales factores (entre los cuales varios pueden ser iguales) siempre será un número par. Por otro lado, cualquier número de la forma $4n+3$ tendrá un número impar de factores de la forma $4n+3$ (i.e., o uno, o tres, o cinco etc.). El número de factores de la forma $4n+1$ permanece indeterminado.

La *Proposición 9* se demuestra de la siguiente forma. Sea A el producto de los factores primos a', a'', a''', etc., b, b', b'', etc.; donde el número de factores b, b', b'', etc. es par (puede también que no haya ninguno, lo que se reduce a lo mismo). Ahora, si a es un residuo de A, también será un residuo de todos los factores a', a'', a''', etc., b, b', b'', etc.; de donde por las proposiciones 1 y 3 del artículo precedente cada uno de estos factores serán residuos de a; por lo tanto también el producto A, lo mismo que $-A$; sin embargo, si $-a$ es un residuo de A y por lo tanto de los factores a', a'', etc., b, b', etc., cada uno de a', a'', etc. será un residuo de a, y cada uno de b, b', etc. un no residuo. Pero como el número de estos últimos es par, el producto de todos, esto es A, será un residuo de a, y así también lo será $-A$.

133.

Iniciamos ahora una investigación más general. Consideraremos dos números impares cualesquiera P y Q, primos entre sí, provistos de signos cualesquiera. Concíbase a P resuelto en sus factores primos sin consideración de su signo, y se denotará por p el número de estos factores para los cuales Q sea un no residuo. Si algún número primo, del cual Q es un no residuo, aparece varias veces entre los factores de P, también deberán ser contados varias veces. De modo semejante, sea q el número de factores primos de Q de los cuales P es un no residuo. Entonces los número p y q tendrán cierta relación dependiente de la naturaleza de los números P y Q. En efecto, si uno de los números p o q es par o impar la forma de los números P y Q mostrará si el otro es par o impar. Se presentará esta relación en la siguiente tabla.

Los números p y q serán al mismo tiempo pares o al mismo tiempo impares,

cuando los números P y Q tienen las formas:

1.	$+A,$	$+A'$
2.	$+A,$	$-A'$
3.	$+A,$	$+B$
4.	$+A,$	$-B$
5.	$-A,$	$-A'$
6.	$+B,$	$-B'$

En el caso contrario, uno de los números p o q será par, y el otro impar, cuando los números P y Q tienen las formas:

7.	$-A,$	$+B$
8.	$-A,$	$-B$
9.	$+B,$	$+B'$
10.	$-B,$	$-B'$*)

Ejemplo. Dados los números -55 y $+1197$, que representan el cuarto caso, entonces 1197 es un no residuo de un solo factor primo de 55, en efecto, del número 5, mientras que -55 es un no residuo de tres factores primos de 1197, a saber, de los números 3, 3 y 19.

Si P y Q denotan números primos, estas proposiciones se convierten en las que hemos tratado en el art. 131. De hecho, aquí p y q no pueden ser mayores que 1; por lo que cuando p se toma par, necesariamente será $= 0$, i.e., Q será un residuo de P, pero cuando p es impar, Q será un no residuo de P, y vice-versa. Así, si se escribe a y b en lugar de A y B, se sigue de 8 que si $-a$ es un residuo o no residuo de b, $-b$ será un no residuo o residuo de a, lo que coincide con 3 y 4 del art. 131.

Por lo general es evidente que Q no puede ser un no residuo de P a no ser que $p = 0$. Por lo tanto, si p es impar, ciertamente Q será un no residuo de P.

De aquí también pueden derivarse sin dificultad las proposiciones del artículo precedente.

Por otra parte, pronto será evidente que esta representación general es más que una observación estéril, puesto que la demostración completa del teorema fundamental apenas podría completarse sin ella.

*) Sea $l = 1$ si ambos P, $Q \equiv 3 \pmod 4$; si no, sea $l = 0$, y sea $m = 1$ si ambos P y Q son negativos, y $m = 0$ en el caso contrario. Así la relación depende de $l + m$.