SOBRE

LOS

RESIDUOS CUADRÁTICOS

POR

JUAN J. DURÁN-LORIGA

PUBLICADO EN LA «REVISTA DE LA REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE MADRID».—TOMO V.—NÚM. 2.—OCTUBRE, 1906.

MADRID
IMPRENTA DE LA «GACETA DE MADRID»
CALLE DE PONTEJOS, NÚM. 8.
1906

SOBRE

LOS

RESIDUOS CUADRÁTICOS

POR

JUAN J. DURÁN-LORIGA

PUBLICADO EN LA «REVISTA DE LA REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE MADRID».—TOMO V.—NÚM. 2.—OCTUBRE, 1906.

MADRID
IMPRENTA DE LA «GACETA DE MADRID»
CALLE DE PONTEJOS, NÚM. 3.
1906

SOBRE LOS RESIDUOS CUADRÁTICOS

En el tomo VIII, año 1901, de *l'Intermédiaire des mathématiciens* propusimos la cuestión siguiente: «La suma de los *residuos cuadráticos* de un número *primo* $p > 3$ es siempre múltiple de p; pero esta propiedad no es exclusiva de los números primos (ejemplo los números compuestos 14 y 15). ¿Qué condición ha de cumplir un número compuesto para gozar de dicha propiedad?»

Dos respuestas se dieron á esta cuestión, la una completamente errónea, por haber interpretado mal la pregunta, y la otra debida al ilustre matemático suizo Sr. M. Lerch, profesor en la Universidad de Fribourg, que respondía *parcialmente* á esta difícil cuestión. Más tardé, este mismo profesor volvió á ocuparse del asunto en un notable trabajo publicado en la Revista italiana *Annali di matematica pura ed applicata*, bajo el título «Sus quelques applications des sommes de Gauss», en el que también trata otros puntos importantes. La propiedad que en el enunciado de la cuestión se cita para los números primos, mayores que tres, se puede demostrar de un modo completamente elemental. Basta recordar que para un número primo p los restos cuadráticos son en número $\frac{p-1}{2}$ y todos resultan de la serie

$1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$ y que siendo la suma de los elemen-

tos de ésta, congruente con la que se busca, bastará demostrar la propiedad para la expresión

$$\frac{p\,(p-1)\,(p+1)}{24},$$

lo cual es inmediato, pues siendo 24 primo con p debe dividir al producto de los otros dos factores y la citada expresión será, por lo tanto, múltipla de p.

Obsérvese de paso que el hecho de dividir 24 á $(p-1)$ $(p+1)$ ó sea p^2-1, demuestra por incidencia la conocida proposición de que siendo p primo y *mayor que tres* se verifica la congruencia

$$p^2 \equiv 1 \text{ (mód. 24)},$$

ó en otros términos: *El cuadrado de un número primo mayor que tres disminuído en una unidad es siempre divisible por 24.*

Pero cuando se trata de *números compuestos,* ocurre, que si bien los restos cuadráticos se derivan como antes de las series

$$1^2,\ 2^2,\ 3^2,\ \ldots\ldots \left(\frac{n}{2}\right)^2 \text{ si } n \text{ es par,}$$

$$1^2,\ 2^2,\ 3^2,\ \ldots\ldots \left(\frac{n-1}{2}\right)^2 \text{ si } n \text{ es impar;}$$

estos números no dan *por precisión* restos diferentes como en el caso de ser el módulo primo y, por consiguiente, la anterior demostración no es aplicable. Se impone *en general* el empleo de doctrinas elevadas de esta rama de la ciencia. El Sr. Lerch, *limitándose al caso de ser* n *impar* y á otras circunstancias que restringen la cuestión, utiliza como punto de partida la célebre igualdad de Gauss,

$$\sum_{\alpha=0}^{\alpha=n-1} e^{\frac{2\alpha^2 m\pi i}{n}} = \left(\frac{m}{n}\right) i^{\frac{1}{2}(n-1)^2} \sqrt{n}, \qquad (1)$$

en la cual *n es impar* y *además m* y *n son primos entre sí.*

La igualdad (1), llamada *Suma de Gauss*, fué consecuencia de los trabajos del gran analista acerca de la determinación de la suma de potencias de las *raíces primitivas* de una *ecuación binomia*, teniendo por exponentes los cuadrados de los números inferiores á un módulo dado, investigación á que también se consagraron otros eminentes matemáticos, como Dirichlet, Cauchy y Kronecker. En la Memoria del célebre geómetra de Göttingen, *Teoría de la división del círculo*, se determina el cuadrado de la suma, pero se presenta incertidumbre acerca del signo al pasar de la potencia á la raíz, dificultad que al fin venció en un trabajo posterior *(Summatio quarundam serierium singularium)* por la transformación de la mencionada suma en un producto de senos.

En la expresión (1) el factor $\sqrt{n}$ es precisamente positivo y el $\left(\frac{m}{n}\right)$ es el *símbolo* de *Legendre*, pero con la extensión que le dió *Jacobi*, y sobre el cual creemos conveniente decir algo á los lectores que no estén familiarizados con esta clase de investigaciones.

Legendre representó por el símbolo $\left(\frac{m}{n}\right)$ á la unidad *positiva* ó *negativa*, según sea *m (no divisible por* n), *residuo* ó *no residuo* cuadrático del número *primo n*, es decir, según sea ó no posible la congruencia

$$x^2 \equiv m \text{ (mód. } n\text{)}.$$

Son consecuencia inmediata de la definición las igualdades

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = +1 \quad , \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \text{(mód. } p\text{)},$$

así como también el que un conocido teorema de la *Teoría de los residuos cuadráticos* se exprese por la siguiente igualdad:

$$\left(\frac{m\,n\,l\,\ldots\ldots}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\left(\frac{l}{p}\right)\ldots\ldots$$

Se ve también que si se tiene $m \equiv n$ (mód. p) resultará

$$\left(\frac{m}{p}\right)=\left(\frac{n}{p}\right).$$

El símbolo de Legendre juega importantísimo papel en la *Teoría de los números*, y en particular la bellísima proposición llamada *Ley de reciprocidad*, que se traduce en la siguiente igualdad:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

en la que p es un número *primo impar* (es decir, distinto de 2) y *positivo* y q un número *impar* cualquiera no divisible por p.

Jacobi introdujo una generalización importante en el símbolo de Legendre. Si el número *impar* P, descompuesto en factores primos, da la igualdad $P = p\,p'\,p''\,\ldots\ldots$, se tendrá *por definición:*

$$\left(\frac{m}{P}\right)=\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\ldots\ldots,$$

debiendo dar al primer miembro el valor $+1$ ó -1, según el que le corresponda al segundo, es decir, en vista de si los factores primos, de los que m es *no residuo* cuadrático, están en número *par* ó *impar*. Claro está que si P es primo se cae en el símbolo de Legendre, y que si $P = 1$, el símbolo vale la unidad positiva.

La generalidad de las fórmulas en que entre el simbolo de Legendre exige que se admita que, si m es divisible por el número primo p, se verifique

$$\left(\frac{m}{p}\right) = 0,$$

y más generalmente que si m y P no son primos entre si, se establezca

$$\left(\frac{m}{P}\right) = 0.$$

Volviendo á considerar la igualdad (1), observaremos con el Sr. Lerch que, si se le da á su primer miembro la forma

$$\sum_{a=0}^{n-1} e^{\frac{2a^2 m \pi i}{n}},$$

se puede establecer la siguiente:

$$\sum_{a=0}^{n-1} e^{\frac{2a^2 m \mu \pi i}{n}} = \left(\frac{m\mu'}{d'_\mu}\right) i^{\frac{1}{4}(d'_\mu - 1)^2} d_\mu \sqrt{d'_\mu}$$

siendo μ' y d'_μ los cocientes de dividir μ y n por su máximo común divisor d_μ, puesto que, evidentemente, la suma se compone de d_μ grupos iguales.

Por medio de diversas transformaciones, y teniendo en cuenta la conocida relación de Dirichlet y Kronecher,

$$\frac{2}{\tau_\Delta} Cl(-\Delta) = \sqrt{\Delta} \sum_1^\infty \left(\frac{-\Delta}{\nu}\right) \frac{1}{\nu\pi}, \qquad (2)$$

llega el Sr. Lerch á la expresión

$$\sum_{a=1}^{n-1} \left\{ \frac{a^2 m}{n} - E\left(\frac{a^2 m}{n}\right) \right\} = \frac{n-q}{2} - \sum_d \left(\frac{m}{d}\right) \frac{2}{\tau_d} Cl(-d) \ldots \qquad (3)$$

en la cual d recorre los divisores de n de la forma $4x + 3$ y q^2 es el mayor divisor cuadrado del número n (que ya hemos dicho es impar); q es, pues, un número impar que puede valer la unidad. En cuanto al símbolo τ_d, se tiene $\tau_d = 2$ para $d > 4$ y $\tau_d = 6$ para $d = 3$.

En la igualdad (2), la cantidad $-\Delta$ es un *discriminante negativo* de la forma cuadrática $ax^2 + bx + cy^2$ (algunos autores le llaman *determinante*, en vez de *discriminante*, palabra que, según creemos, introdujo en la ciencia el matemático inglés Salmon), y el símbolo $Cl(-\Delta)$ indica el número de *clases positivas* y *primitivas* de las formas cuadráticas para un discriminante *negativo* dado. Conviene recordar que dos formas son *equivalentes* cuando el sistema de números que representa la una es idéntico al que representa la otra, y que es condición *necesaria*, pero *no suficiente*, para la equivalencia que los discriminantes respectivos sean iguales. También debe tenerse presente que un sistema de formas equivalentes constituye *una clase*. Asimismo debe saberse que se llama *forma primitiva*, según Gauss, aquella en que los tres coeficientes son primos relativos, y que una forma es *positiva* cuando lo son los coeficientes extremos.

Si en la igualdad (3) se hace $m = 1$, resulta:

$$\sum_{a=1}^{n-1} a^2 = n \sum_{a=1}^{a-1} E\left(\frac{a^2}{n}\right) + \frac{n(n-q)}{2} - n \sum_{d} \frac{2}{\tau_d} Cl(-d) \quad \ldots\ldots \quad (4)$$

Esta relación demuestra, considerando ahora todos los residuos cuadráticos *iguales* y *desiguales* que da la serie de un sistema completo de restos respecto al módulo n, que su suma es divisible por n si n no lo es por 3, pues si lo fuese, hay en el segundo miembro el término $-\frac{n}{3}$, puesto

que $\frac{2}{\tau_3} = \frac{2}{6} = \frac{1}{3}$, y la suma es congruente con $-\frac{n}{3}$, según el módulo n.

Podemos llegar al mismo resultado á que llega el señor Lerch por una vía más elemental, pues la suma de cuadrados (congruente con la de resíduos cuadráticos) es

$$S = \frac{n(n-1)(2n-1)}{6},$$

y al ser el número impar n no divisible por 3, es primo con 6, y se tendrá: $S =$ multp. n.

Si n es múltiplo de 3, no se puede hacer el razonamiento anterior; pero se puede establecer haciendo $n = 3p$:

$$S + p = \frac{3p(18p^2 - 9p - 3)}{6};$$

y se ve que el factor $\frac{18p^2 - 9p - 3}{6}$ es entero, pues es igual á $3p^2 - \frac{3p+1}{2}$, resulta, pues, $S + \frac{n}{3} =$ multp. n, ó bien $S \equiv -\frac{n}{3}$ (mód. n).

Puede también observarse que, aun en el caso de ser n *par*, si lo que se pretende es estudiar como antes la suma de *todos* los residuos cuadráticos *iguales* ó *desiguales* que origina un sistema completo de restos, la investigación es completamente elemental, y se ve que, en este caso, no puede ser esta suma múltiple de n. En efecto: si $n = 3p$ (p par), los factores $(n-1)$ y $(2n-1)$, del valor de S, son primos con 6, y resulta:

$$s \equiv \frac{n}{6} \text{ (mód. } n\text{)};$$

si $n = 3p + 1$ ó $n = 3p + 2$, se ve inmediatamente que se verifica

$$s \equiv \frac{n}{2} \text{ (mód. } n),$$

pues los factores $(n - 1)$ y $(2n - 1)$ son ambos impares y uno de ellos es precisamente múltiplo de 3.

En el caso en que se desee la suma de los residuos cuadráticos *diferentes entre sí*, pero *precisamente primos con el módulo*, es evidente que, llamándola s, se puede establecer la igualdad

$$2^{\omega} s = \sum_{\nu=1}^{n} \left(1 + \left(\frac{\nu}{p_1}\right)\right)\left(1 + \left(\frac{\nu}{p_2}\right)\right) \ldots\ldots \quad (5)$$
$$\left(1 + \left(\frac{\nu}{p_\omega}\right)\right)\left(\frac{n}{\nu}\right)\nu,$$

en la cual $p_1, p_2, \ldots\ldots p_\omega$ son los diferentes factores primos del número n, que suponemos impar, pues al variar ν de 1 á n, cuando pase por un valor no primo con n, el penúltimo factor se hace cero y, por lo tanto, el sumando correspondiente, sucediendo lo mismo á uno de los factores $\left(1 + \left(\frac{\nu}{p}\right)\right)$ cuando pase por valores que no sean residuos cuadráticos. En cambio, cada vez que ν tome el valor de un residuo *primo con el módulo*, el sumando correspondiente se convierte en $2^{\omega} \cdot \nu$.

Pero en la igualdad anterior no es posible estudiar la naturaleza de la suma s; de aquí la importancia de lo que establece el Sr. Lerch, después de diversos é ingeniosos desarrollos, y que es la siguiente:

$$2^{\omega} s = \frac{1}{2} n \varphi(n) - n \sum_{d} \frac{2}{\tau_d} Cl(-d) M_d(n), \quad (6)$$

en la que

$$M_d(n) = \left(1 - \left(\frac{p_1}{d}\right)\right)\left(1 - \left(\frac{p_2}{d}\right)\right) \cdots \left(1 - \left(\frac{p^{\omega}}{d}\right)\right) \quad (7)$$

El examen de las fórmulas (6) y (7) dice que cuando el número *impar* n no tiene el factor 3, entonces τ_d vale siempre 2 y, por consiguiente, n divide al segundo miembro de la (6) y, por lo tanto, á s por ser primo con 2^{ω}. Ahora, si n es divisible por 3 aparece el sumando $-\frac{n}{3} M_3(n)$ (puesto que $\tau_3 = 6$); sin embargo, este término será nulo si hay al menos otro factor de la forma $3k+1$, y entonces s será divisible por n. Pero si al ser n múltiplo de 3 los demás factores son de la forma $3k+2$, entonces se tiene:

$$2^{\omega} s \equiv -\frac{n}{3} 2^{\omega - 1} \text{ (mód. } n),$$

ó bien

$$2s \equiv -\frac{n}{3} \text{ (mód. } n),$$

y, finalmente,

$$s \equiv \frac{n}{3} \text{ (mód. } n).$$

Falta ahora, para responder por completo á la cuestión propuesta, obtener en el caso de *n par* la suma de los residuos cuadráticos diferentes y primos con el módulo, y *sobre todo*, y este es el verdadero espíritu de la cuestión, estudiar, ya sea *n par* ó *impar*, la suma de los residuos cuadráticos *diferentes entre sí* y *primos ó no*, indistintamente, con el módulo que se considere.