La Ley de Reciprocidad Cuadrática

Paulo Tirao

Vaquerías, 9 al 14 de agosto de 2004

Contenidos

Ocupado con otro trabajo, me encontré con una verdad aritmética extraordinaria. Como la consideré muy bella en si misma, concentré en ella todos mis esfuerzos para entender los principios de los cuales dependía y para obtener una prueba rigurosa.

C. F. Gauss

La Ley de Reciprocidad Cuadrática es uno de los resultados mas probados en matemática. Existen hoy más de 200 pruebas. Originalmente conjeturada por Euler y Legendre, fue probada por primera vez por Gauss, quién en el curso de su vida dio 8 pruebas distintas. El mismo Gauss lo llamo *Aureum Theorema* (el Teorema de oro).

Su importancia en la teoría de números es indiscutida. Al respecto, Hecke afirmó: "La teoría de números moderna comenzó con el descubrimiento de la Ley de Reciprocidad".

1 PRIMERA CLASE
Aritmética modular

En esta primera clase hacemos un breve repaso de la aritmética de enteros módulo m, $\mathbb{Z}_m$. Introducimos la función ϕ de Euler y mostramos sus propiedades básicas.

Estudiamos y resolvemos todas las ecuaciones de primer grado en $\mathbb{Z}_m$ y probamos los Teoremas de Fermat y Euler. Al final analizamos rapidamente las ecuaciones polinomiales en general y enunciamos el Teorema de Lagrange.

Los Teoremas de Fermat, Euler y Lagrange son llamados los teoremas fundamentales de la aritmética modular.

1.1 El anillo $\mathbb{Z}_m$ y la función ϕ de Euler

Definición 1.1. Sea m un entero positivo y a y b dos enteros cualesquiera. Decimos que a y b son congruentes módulo m, y escribimos $a \equiv b \mod m$, si $m|a-b$, es decir si $a - b = km$ para algún k.

Cuando el entero m esté implícito denotaremos simplemente $a \equiv b$.

Proposición 1.2. *Sea m un entero positivo.*

(i) *$\equiv$ es una relación de equivalencia en $\mathbb{Z}$.*

(ii) *Todo entero a es congruente a un único r, con $0 \leq r < m$, el resto de la división de a por m.*

(iii) *Si $a \equiv b$ y $c \equiv d$, entonces $a + c \equiv b + d$ y $ac \equiv bd$.*

Esta proposición nos permite definir una estructura de anillo conmutativo en el conjunto de clases de equivalencia que denotamos por $\mathbb{Z}_m$.

Definición 1.3. Un elemento $a \in \mathbb{Z}_m$ es una unidad, si existe un $b \in \mathbb{Z}_m$ tal que $ab \equiv 1 \mod m$. El grupo de unidades de $\mathbb{Z}_m$ es $U(\mathbb{Z}_m)$.

Proposición 1.4. $U(\mathbb{Z}_m) = \{a \in \mathbb{Z}_m : \ (a, m) = 1\}$.

Prueba. Inmediata. □

Proposición 1.5. *Sean n y m coprimos. Entonces*

(i) *El mapa $a \mapsto (a, a)$, de $\mathbb{Z}_{nm}$ en $\mathbb{Z}_n \times \mathbb{Z}_m$, es un isomorfismo de anillos.*

(ii) $U(\mathbb{Z}_{nm}) \simeq U(\mathbb{Z}_n) \times U(\mathbb{Z}_m)$.

Prueba. La suma y el producto en $\mathbb{Z}_n \times \mathbb{Z}_m$ está definido coordenada a coordenada, luego es claro que el mapa definido es un homomorfismo de anillos. El mapa es inyectivo pues si $(a, a) = (0, 0)$ en $\mathbb{Z}_n \times \mathbb{Z}_m$, entonces $n|a$ y $m|a$, pero como n y m son coprimos se sigue que $nm|a$ y luego $a = 0$ en $\mathbb{Z}_{nm}$. Como Z_{nm} y $\mathbb{Z}_n \times \mathbb{Z}_m$ tienen la misma cantidad de elementos, se sigue que el mapa es una biyección y luego es un isomorfismo.

Para la segunda parte basta observar que un b es coprimo con nm si y sólo si lo es con n y con m. Luego la restriccón del mapa definido es un isomorfismo. □

Definición 1.6 (La función ϕ de Euler). Sea m un entero positivo. Entonces definimos

$$\phi(m) = |U(\mathbb{Z}_m)| = \text{cardinal } \{1 \leq a \leq m : \ (a, m) = 1\}.$$

Esta función se llama *la función ϕ de Euler.*

Ejemplos 1.7.

(i) $\phi(1) = 1$; $\phi(2) = 1$; $\phi(3) = 2$; $\phi(4) = 2$; $\phi(5) = 4$.

(ii) Si p es primo, entonces $\phi(p) = p - 1$.

(iii) Si p es primo, entonces $\phi(p^l) = p^l - p^{l-1}$.

Proposición 1.8. *La función ϕ de Euler es multiplicativa, es decir $\phi(nm) = \phi(n)\phi(m)$, si $(n, m) = 1$. Además, para todo $n \geq 1$ vale*

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Prueba. La Proposición 1.5 implica que ϕ es multiplicativa. Este hecho y los cálculos en los ejemplos anteriores prueban la fórmula. □

Teorema 1.9. *Si p es un número primo, distinto de 2, entonces el grupo de unidades $U(\mathbb{Z}_{p^k})$ es cíclico de orden $p^k - p^{k-1}$; es decir existe un g tal que $U(\mathbb{Z}_{p^k}) = \{g^r : \ r = 1 \ldots p^k - p^{k-1}\}$.*

Ejemplo 1.10. Sea $p = 3$. El grupo de unidades de $\mathbb{Z}_9$ tiene 6 elementos; más aún

$$U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}.$$

Veamos, por ejemplo, que generamos con el 4. Tenemos $4^1 \equiv 4$, $4^2 \equiv 7$ y $4^3 \equiv 1$, luego con el 4 sólo generamos el subconjunto $\{1, 4, 7\}$ de unidades. Sin embargo si hacemos lo mismo con el 2, vemos que $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$ y $2^6 \equiv 1$. Es decir 2 es un generador del grupo de unidades en este caso.

1.2 Ecuaciones lineales y los Teoremas de Fermat y Euler

Nos proponemos entender y resolver la ecuación general de primer grado en $\mathbb{Z}_m$,

$$ax \equiv b \mod m, \qquad 0 \leq x \leq m - 1. \tag{1}$$

Si $a = 1$ se trata sólo de encontrar el resto de b en la división por m. En particular, con $a = 1$ la ecuación 1 siempre tiene solución. Para esto el algoritmo de Euclides que aprendimos en la escuela es adecuado. En algunos casos, por ejemplo cuando b no es muy grande, lo podemos aplicar directamente, pero en otros necesitaremos de mayor manipulación aritmética.

Por ejemplo, para resolver la ecuación

$$x \equiv 453 \mod 17, \qquad 0 \leq x \leq 16$$

el algoritmo de Euclides rapidamente nos dice que $453 = 26 \times 17 + 11$. Luego $x = 11$ es la solución buscada.

Un ejemplo algo más complicado es el siguiente.

Ejemplo 1.11. Encontrar los 2 últimos dígitos de 123^{456} es equivalente a encontrar un $0 \leq x \leq 99$ tal que $x \equiv 123^{456} \mod 100$.

Solución 1.

$$\begin{aligned} 123 &\equiv 23 \\ 123^2 &\equiv 23^2 \equiv 529 \equiv 29 \\ 123^3 &\equiv 23^3 \equiv 29 \times 23 \equiv 667 \equiv 67 \\ 123^5 &\equiv 29 \times 67 \equiv 43 \\ 123^6 &\equiv 23 \times 43 \equiv 89 \\ 123^{10} &\equiv 43 \times 43 \equiv 49 \\ 123^{20} &\equiv 49 \times 49 \equiv 1 \\ 123^{440} &\equiv 1 \\ 123^{456} &\equiv 123^{16}, \end{aligned}$$

además como $123^{16} \equiv 49 \times 89 \equiv 61$ resulta $123^{456} \equiv 61 \mod 100$. □

Solución 2. Escribimos 456 como suma de potencias de 2; es decir pensamos en el desarrollo bianrio de 456. Así tenemos que $456 = 256 + 128 + 64 + 8$. Ahora calculamos:

$$\begin{aligned} 123^2 &\equiv 23^2 \equiv 29 \\ 123^4 &\equiv 29^2 \equiv 41 \\ 123^8 &\equiv 41^2 \equiv 81 \\ 123^{16} &\equiv 81^2 \equiv 61 \\ 123^{32} &\equiv 61^2 \equiv 21 \\ 123^{64} &\equiv 21^2 \equiv 41 \\ 123^{128} &\equiv 41^2 \equiv 81 \\ 123^{256} &\equiv 81^2 \equiv 61; \end{aligned}$$

luego $123^456 \equiv 61 \times 81 \times 41 \times 81 \equiv 61 \mod 100$. □

Solución 3. La solución que buscamos satisface $x - 123^{456} = 100k$, para algún k. Pero como $100 = 4 \times 25$, entonces x también satisface $x - 123^{456} = 4k'$ y $x - 123^{456} = 25k''$; es decir

$$x \equiv 123^{456} \mod 4 \quad \text{y} \quad x \equiv 123^{456} \mod 25.$$

Por lo tanto comenzamos resolviendo estas dos ecuaciones más fáciles.

(i) Módulo 4 tenemos que, $123 \equiv 3 \Rightarrow 123^2 \equiv 1 \Rightarrow 123^{456} \equiv 1$.

(ii) Módulo 25 tenemos que,

$$\begin{aligned} 123 &\equiv -2 \\ 123^2 &\equiv 4 \\ 123^8 &\equiv 6 \\ 123^{10} &\equiv -1 \\ 123^{450} &\equiv -1 \end{aligned}$$

y también que $123^6 \equiv 4^3 \equiv 14$. Luego $123^{456} \equiv -14 \equiv 11$.

Ahora la solución x que buscamos satisface $x \equiv 1 \mod 4$ y $x \equiv 11 \mod 25$. Probamos con 11, 36, 61, bingo $x = 61$ es la solución.

□

Esta tercera solución muestra una estregia general para resolver no sólo ecuaciones de primer grado sino ecuaciones polinomiales generales: reducir la ecuación módulo m a ecuaciones módulo potencias de primos y luego a partir de soluciones de éstas reconstruir la solución de la ecuación original. La reconstrucción es siempre posible y está asegurada por el Teorema Chino del Resto. Al final de la clase describiremos los detalles.

Un paso más en esta dirección es reducir las ecuaciones módulo potencias de un primo a ecuaciones módulo un primo y luego a partir de las soluciones de estas reconstruir las soluciones de la ecuación original. En efecto esto funciona. Aunque no estudiaremos esta segunda reducción debe quedar clara la importancia del estudio de ecuaciones módulo un primo.

Probamos ahora dos de los teoremas fundamentales de la aritmética modular.

Teorema 1.12 (Fermat). *Sea p primo. Entonces para cualquier a, $a^p \equiv a \mod p$. En particular si $p \nmid a$, entonces $a^{p-1} \equiv 1 \mod p$*

Prueba. Basta probar el teorema para a un entero positivo. Procedemos por inducción en a. El teorema es claro para $a = 1$. Supongamos que vale para $a = n$. Escribimos

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + 1.$$

Para $1 \leq k \leq p-1$, el coeficiente binomial $\binom{p}{k}$ es divisible por p. Luego $(n+1)^p \equiv n^p + 1 \mod p$. Por hipótesis inductiva $n^p \equiv n \mod p$, entonces resulta $(n+1)^p \equiv n+1 \mod p$. □

Teorema 1.13 (Euler). *Si $(a, m) = 1$, entonces $a^{\phi(m)} \equiv 1 \mod m$.*

Prueba. Sean $r_1, \ldots, r_{\phi(m)}$ todos los coprimos con m entre 1 y $m-1$. Ahora, $ar_1, \ldots, ar_{\phi(m)}$ son todos coprimos con m y cada ar_i es congruente a un único r_j. Luego

$$(ar_1) \ldots (ar_{\phi(m)}) \equiv r_1 \ldots r_{\phi(m)} \mod m,$$

es decir

$$a^{\phi(m)} r_1 \ldots r_{\phi(m)} \equiv r_1 \ldots r_{\phi(m)} \mod m$$

que solo es posible si $a^{\phi(m)} \equiv 1$, dado que m y $r_1 \ldots r_{\phi(m)}$ son coprimmos. □

El Teorema de Euler nos permite dar una cuarta solución al problema del Ejemplo 1.11.

Solución 4. Calculamos $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$; luego $123^{40} \equiv 1$. Como $456 = 11 \times 40 + 16$, entonces $123^{456} \equiv 123^{16} \equiv 61$. □

Volvemos ahora al problema original, la ecuación (1).

Teorema 1.14. *Si $(a, m) = 1$, entonces la ecuación $ax \equiv b \mod m$ tiene una única solución en $\mathbb{Z}_m$.*

Prueba. Sea $x_0 = a^{\phi(m)-1}b$, entonces

$$ax = a(a^{\phi(m)-1}b) = a^{\phi(m)}b \equiv b \mod m.$$

Es decir x_0 es solución.

Supongamos ahora que x e y son dos soluciones. Entonces

$$\begin{aligned} x \equiv a^{\phi(m)}x &\equiv a^{\phi(m)-1}(ax) \\ &\equiv a^{\phi(m)-1}b \\ &\equiv a^{\phi(m)-1}(ay) \equiv a^{\phi(m)}y \equiv y \mod m. \end{aligned}$$

□

Teorema 1.15. *Si $(a, m) = d$, entonces la ecuación $ax \equiv b \mod m$ tiene solución si y sólo si $d|b$. Cuando tiene solución, tiene exactamente d soluciones distintas en $\mathbb{Z}_m$.*

Prueba. El caso $d = 1$ es el teorema anterior. Luego suponemos que $d > 1$.

Si $ax \equiv b \mod m$, entonces existe y tal que $ax - my = b$ y luego $d|b$. Reciprocamente, si $d|b$ la ecuación $ax \equiv b \mod m$ es equivalente a la ecuación $a_1x \equiv b_1 \mod m_1$, donde $a = da_1$, $b = db_1$ y $m = dm_1$. Como ahora $(a_1, m_1) = 1$, la última ecuación tiene una (única) solución.

Sea t_1 la única solución de $a_1x \equiv b_1 \mod m_1$. Si x es una solución de $ax \equiv b \mod m$, entonces existe un y tal que $x = t_1 + ym_1$ (pues es también solución de la segunda ecuación). Ahora $t_1 + ym_1 \equiv t_1 + zm_1 \mod m$ si y sólo si $m|m_1(y-z)$ si y sólo si $d|(y-z)$. Por lo tanto hay exactamente d soluciones, dadas por

$$t_1, t_1 + m_1, t_1 + 2m_1, \ldots, t_1 + dm_1.$$

□

Ejemplo 1.16. La ecuación $6x \equiv 5 \mod 15$ no tiene solución, ya que $(6, 15) = 3$ y $3 \not| 5$.

En cambio la ecuación $6x \equiv 9 \mod 15$, si tiene; más aún sabemos que tiene $(6, 15) = 3$ soluciones distintas. Primero consideramos la ecuación $2x \equiv 3 \mod 5$ que obtenemos de la original dividiendo por $(6, 15) = 3$ y la resolvemos. Resulta que $x_0 = 4$ es su única solución. A partir de esta construimos las restantes de la ecuación original,

$$x_0 = 4, \quad x_1 = 9, \quad x_2 = 14, \quad \mod 15.$$

1.3 El Teorema Chino del Resto

Teorema 1.17. *Sean $m_1, \ldots m_r$ enteros positivos coprimos 2 a 2. El sistema de ecuaciones*

$$x \equiv a_1 \mod m_1 \quad ; \ldots ; \quad x \equiv a_r \mod m_r$$

tiene solución cualesquiera sean $a_1, \ldots a_r$. Esta solución es única módulo el producto $m_1 \cdots m_r$.

Prueba. Damos una prueba constructiva de este teroema.

Sea $M = m_1 \ldots m_r$. Entonces $m_j|M$ y $(M/m_j, m_j) = 1$, para $1 \leq j \leq r$. Luego, por el Teorema 1.14, existen enteros b_j para $1 \leq j \leq r$, tales que

$$(M/m_j)b_j \equiv 1 \mod m_j.$$

Además, para $i \neq j$,

$$(M/m_j)b_j \equiv 0 \mod m_i.$$

A partir de estos enteros b_j construimos

$$w = \sum_{j=1}^{r} (M/m_j)b_j a_j.$$

Si $1 \leq i \leq r$, entonces

$$w = \sum_{j=1}^{r} (M/m_j)b_j a_j \equiv (M/m_i)b_i a_i \equiv a_i \mod m_i$$

y w es una solución.

Finalmente, si x e y son dos soluciones, entonces

$$x \equiv a_i \equiv y \mod m_i, \qquad \text{para } 1 \leq i \leq r.$$

Luego si $1 \leq i \leq r$, $m_i | x - y$ y como los m_i son coprimos de a pares, entonces $M | x - y$; es decir $x \equiv y \mod M$. □

Ejemplo 1.18. Consideremos el sistema

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 4, \quad x \equiv 4 \mod 5.$$

Como 3,4 y 5 son coprimos 2 a 2, sabemos que el sistema tiene solución y que tiene una única solución x con $-29 \leq x \leq 30$. Para hallar esta solución comenzamos resolviendo las ecuaciones

$$20.y_1 \equiv 1 \mod 3, \quad 15.y_2 \equiv 1 \mod 4, \quad 12.y_3 \equiv 1 \mod 5.$$

Es fácil ver que $y_1 = 2$, $y_2 = 3$, $y_3 = 3$ son soluciones. Ahora $x = 20.2.2 + 15.3.3 + 12.3.4$ es una solución del sistema. Luego $x \equiv 20 + 15 + 24 \equiv 59 \equiv -1 \mod 60$ y $x = -1$ es la solución que buscábamos.

1.4 Ecuaciones polinomiales y el Teorema de Lagrange

Sea $f(x)$ un polinomio con coeficientes enteros de grado n y consideremos la ecuación

$$f(x) \equiv 0 \mod m. \tag{2}$$

Lamentablemente no podremos dar en general una respuesta contundente como en el caso de las ecuaciones de primer grado, es decir cuando $n = 1$. En la tercera clase abordaremos en detalle el caso $n = 2$.

Comenzamos con algunas observaciones elementales y algunos ejemplos. Como estamos interesados en las soluciones de (2) en $\mathbb{Z}_m$, es claro que a lo sumo hay m soluciones. Mas aún, en general, la cantidad de soluciones no está acotada por el grado de $f(x)$. Por ejemplo, la ecuación

$$2x^2 - 2x \equiv 0 \mod 4,$$

tiene 4 soluciones: 0, 1, 2 y 3.

Por otro lado hay ecuaciones como (2) sin ninguna solución, como por ejemplo

$$x^2 + x + 2 \equiv 0 \mod 3.$$

Teorema 1.19 (Lagrange). *Si $f(x)$ es un polinomio con coeficientes enteros de grado n y p es un número primo, entonces la ecuación*

$$f(x) \equiv 0 \mod p$$

tiene a lo sumo n soluciones distintas en $\mathbb{Z}_p$.

Enunciamos el teorema que permite reducir el estudio de una ecuación polinomial módulo m al estudio de la misma ecuación pero módulo las potencias de primos que dividen a m. La prueba se sigue del Teorema Chino del Resto.

Teorema 1.20. *Sea $m = p_1^{l_1} \dots p_r^{l_r}$ la factorización de m. Entonces la ecuación $f(x) \equiv 0 \mod m$ tiene solución si y sólo si $f(x) \equiv 0 \mod p_i^{l_i}$ tiene solución para todo $i = 1 \dots r$. Más aún, si $N(m)$ es el número de soluciones de $f(x) \equiv 0 \mod m$, entonces $N(m) = \prod_i N(p_i^{l_i})$.*

1.5 Ejercicios

1. **El grupo de unidades**

   (a) Encontrar la inversa del isomorfismo $\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$ dado en la Proposición 1.5.

   (b) Hallar todos los generadores de $U(\mathbb{Z}_{11})$, de $U(\mathbb{Z}_{13})$ y de $U(\mathbb{Z}_{25})$.

   (c) ¿Son $U(\mathbb{Z}_8)$ y $U(\mathbb{Z}_{10})$ cíclicos?

2. **La función ϕ de Euler**

   (a) Calcular $\phi(16)$, $\phi(37)$ y $\phi(420)$.

   (b) Probar que n es primo si y sólo si $\phi(n) = n - 1$.

   (c) Probar que si n es par, entonces $\phi(2n) = 2\phi(n)$ y que si n es impar, entonces $\phi(2n) = \phi(n)$.

3. **El Teorema de Wilson**

   Probar que si p es primo, entonces

   $$(p-1)! \equiv -1 \mod p.$$

   [Ayuda: considerar con cada elemento su inverso.]

4. **Ecuaciones de primer grado**

   (a) Sean a y m coprimos.

      i. Mostrar como se puede resolver la ecuación $ax \equiv b \mod m$ escribiendo $1 = \alpha a + \beta m$.

      ii. Resolver por este método las ecuaciones: $3x \equiv 4 \mod 8$ y $7x \equiv -4 \mod 22$.

   (b) Resolver las siguientes ecuaciones.

$$\begin{array}{llll} 5x \equiv 1 & \mod 7; & 187x \equiv 2 & \mod 503; \\ 14x \equiv 5 & \mod 45; & 179x \equiv 2 & \mod 153; \\ 9x \equiv 9 & \mod 12; & 182x \equiv 7 & \mod 203. \end{array}$$

(c) Probar que todo entero satisface al menos una de las siguientes ecuaciones:

$$x \equiv 0 \mod 2; \quad x \equiv 0 \mod 3; \quad x \equiv 1 \mod 4;$$
$$x \equiv 1 \mod 6; \quad x \equiv 11 \mod 12.$$

(d) Deducir el Teorema de Fermat como corolario del Teorema de Euler.

5. **Sistemas de ecuaciones de primer grado**

(a) Obtener todas las soluciones, módulo 210, del sistema de ecuaciones

$$2x \equiv 3 \mod 5; \quad 4x \equiv 2 \mod 6; \quad 3x \equiv 2 \mod 7.$$

(b) Resolver el sistema de ecuaciones

$$3x^2 + x \equiv 0 \mod 5; \qquad 2x + 3 \equiv 0 \mod 7.$$

(c) Encontrar el menor entero positivo cuyo resto en la división por 13 sea 5, en la división por 12 sea 3 y en la división por 35 sea 2.

6. **Ecuaciones con dos incógnitas**

(a) Si $(a, n) = 1$ y $(b, n) = 1$, entonces $ax + by \equiv c \mod n$ tiene exactamente n soluciones distintas.

(b) Resolver las siguientes ecuaciones:

$$6x + 15y \equiv 9 \mod 7; \quad 10x + 5y \equiv 9 \mod 15.$$

2 SEGUNDA CLASE
La Ley de Reciprocidad Cuadrática

2.1 Residuos cuadráticos

Definición 2.1. Sea p un primo impar. Un entero a, coprimo con p, es un *residuo cuadrático* módulo p, si existe un x tal que $x^2 \equiv a \mod p$. En caso contrario a es un *no-residuo cuadrático* módulo p.

Dados un primo p y un entero cualquiera a, el símbolo de Legendre está definido como

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{si } (p,a)=1 \text{ y } a \text{ es residuo cuadrático módulo } p; \\ 0, & \text{si } p|a; \\ -1, & \text{si } (p,a)=1 \text{ y } a \text{ es no-residuo cuadrático módulo } p. \end{cases}$$

Ejemplo 2.2. Calculemos los cuadrados en $\mathbb{Z}_p$, para $p = 5, 7, 11$.

		1	2	3	4	5	6	7	8	9	10
k^2	mod 5	1	4	4	1						
k^2	mod 7	1	4	2	2	4	1				
k^2	mod 11	1	4	9	5	3	3	5	9	4	1

Ahora listemos los residuos cuadráticos y los no-residuos cuadráticos para $p = 5, 7, 11$, menores que p.

	Residuos cuadráticos	Residuos no-cuadráticos
$p = 5$	$\{1, 4\}$	$\{2, 3\}$
$p = 7$	$\{1, 2, 4\}$	$\{3, 5, 6\}$
$p = 11$	$\{1, 3, 4, 5, 9\}$	$\{2, 6, 7, 8, 10\}$

Proposición 2.3. *Exactamente la mitad de los enteros a, con $1 \leq a \leq p-1$, son residuos cuadráticos módulo p.*

Prueba. En el conjunto $S = \{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ no hay ningún par de números congruentes entre si; luego hay por lo menos $\frac{p-1}{2}$ residuos cuadráticos.

Reciprocamente supongamos que a es un residuo cuadrático, es decir existe un z tal que $z^2 \equiv a$. Pero omo también $(p-z)^2 \equiv a$ y uno de los números z o $p-z$ es $\leq \frac{p-1}{2}$ resulta que $a \in S$. □

Teorema 2.4 (Criterio de Euler). *Sea p un número primo impar y a un entero cualquiera coprimo con p. Entonces*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Prueba. Sea g un generador de $U(\mathbb{Z}_p)$ y supongamos que a es residuo cuadrático módulo p, es decir

$$a \equiv x_0^2 \equiv (g^r)^2 \equiv g^{2r},$$

para algún x_0 y algún r. Entonces

$$a^{\frac{p-1}{2}} \equiv g^{2r\frac{p-1}{2}} \equiv (g^{p-1})^r \equiv 1.$$

Supongamos ahora que $a^{\frac{p-1}{2}} \equiv 1$. Como $a \equiv g^r$, para algún r. Entonces $g^{r\frac{p-1}{2}} \equiv 1$, luego $p-1|\frac{r(p-1)}{2}$ y $2|r$, por lo cual resulta $a \equiv (g^{\frac{r}{2}})^2$.

Finalmente, como $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1$, tenemos que $a^{\frac{p-1}{2}} \equiv \pm 1$. □

Ejemplos 2.5.

(i) Residuos cuadráticos módulo 11.

Calculemos $a^{\frac{11-1}{2}} = a^5$ para todo $a \in U(\mathbb{Z}_{11})$. Tenemos: $1^5 \equiv 1$, $2^5 \equiv -1$, $3^5 \equiv 1$, $4^5 \equiv 1$, $5^5 \equiv 1$, $6^5 \equiv -1$, $7^5 \equiv -1$, $8^5 \equiv -1$, $9^5 \equiv 1$ y $10^5 \equiv -1$. Luego los residuos cuadráticos módulo 11 son $\{1, 3, 4, 5, 9\}$.

(ii) ¿Es 2 residuo cuadrático módulo 13?

Como $2^6 = 64 = 13 \times 5 - 1$, entonces $2^6 \equiv -1 \mod 13$, por lo tanto 2 no es residuo cuadrático módulo 13 y la ecuación $x^2 \equiv 2 \mod 13$ no tiene solución.

Teorema 2.6. *Sea p un primo impar y sean a y b enteros coprimos con p. Entonces*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Prueba. Inmediata a partir del Criterio de Euler. □

De este teorema se sigue que para calcular $\left(\frac{a}{p}\right)$, para cualquier entero a, basta conocer $\left(\frac{1}{p}\right)$, $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ y $\left(\frac{q}{p}\right)$ para todos los primos q impares, positivos y menores que p.

Proposición 2.7.

(i) $\left(\frac{1}{p}\right) = 1$.

(ii) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \mod 4; \\ -1, & \text{si } p \equiv 3 \mod 4. \end{cases}$

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Ejemplo 2.8. Estudiemos el caso $\left(\frac{2}{p}\right)$. Lo ideal sería dar una condición para que $\left(\frac{2}{p}\right) = 1$. Comencemos por listar primos p para los cuales 2 es residuo cuadrático. Una forma de hacer esto es factorizar los números de la forma $x^2 - 2$. Si un $p|x^2 - 2$, entonces $\left(\frac{2}{p}\right) = 1$.

x	3	5	7	9	11	13	15	17	19	21
x^2-2	7	23	47	79	7×17	167	223	7×41	359	439

x	23	25	27	29	31	33	35	37
x^2-2	17×31	7×89	727	839	7×137	1087	1223	1367

De estas tablas se sigue que 2 es residuo cuadrático para los primos p en el conjunto $\{7, 17, 23, 31, 41, 47, 79, 89, \dots\}$. ¿Tienen algo en común estos primos? La respuesta es sí. Todos son congruentes a ± 1 módulo 8. Si miramos nuevamente las tablas veremos que no hay ningún primo que sea congruente a 3 o a 5 módulo 8. Por supuesto esto no alcanza para decir cuándo 2 es o no residuo cuadrático, pero podemos conjeturarlo.

Ejemplo 2.9. Analicemos ahora para que primos p, son 3 y 5 residuos cuadráticos módulo p.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\left(\frac{3}{p}\right)$	1	-1	-1	1	1	-1	-1	1	-1	-1	1	-1	-1	1
$\left(\frac{5}{p}\right)$	-1	1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1

Si miramos con cuidado esta tabla parece que $\left(\frac{3}{p}\right)$ depende sólo de la clase de congruencia de p módulo 3, fenómeno que se repite para $\left(\frac{5}{p}\right)$. Sin embargo con lo que sabemos hasta ahora no es claro como probaríamos esto. Por ejemplo, no parece evidente que $5^{\frac{p-1}{2}} \equiv R \mod p$ para todos los primos p con un mismo resto módulo 5.

Euler y Legendre descubrieron la razón del fenómeno observado en el ejemplo, que más tarde Gauss probó.

2.2 La Ley de Reciprocidad Cuadrática

Cada uno de los primeros matemáticos que se ocuparon de este fenómeno formuló el resultado a su manera. Quiza la versión más difundida hoy sea la Legendre. Sin embargo en ciertos contextos otras pueden resultar más útiles.

Versión de Legendre *Sea p y q primos impares. Entonces*

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

Este teorema nos da un método muy eficiente para calcular $\left(\frac{a}{p}\right)$.

Ejemplo 2.10. Calculemos $\left(\frac{11}{43}\right)$.

$$\left(\frac{11}{43}\right) = \left(\frac{43}{11}\right)(-1)^{5\times 21} = -\left(\frac{-1}{11}\right) = 1.$$

Es decir, no existe ningún entero a tal que $a^2 \equiv 11 \mod 43$.

Ejemplo 2.11. Calculemos $\left(\frac{17}{97}\right)$.

$$\begin{aligned}\left(\frac{17}{97}\right) &= \left(\frac{97}{17}\right)(-1)^{8\times 48} \\ &= \left(\frac{12}{17}\right) = \left(\frac{2}{17}\right)^2\left(\frac{3}{17}\right) \\ &= \left(\frac{17}{3}\right)(-1)^8 = \left(\frac{2}{3}\right) \\ &= -1.\end{aligned}$$

Es decir, existe al menos un entero a tal que $a^2 \equiv 17 \mod 97$.

Versión de Euler *Si p y q son primos impares distintos, entonces $\left(\frac{q}{p}\right) = 1$ si y sólo si $p \equiv \pm b^2 \mod 4q$ para algún entero impar b.*

Versión de Gauss *Sea p y q primos impares. Entonces*

(i) *Si p es de la forma $4n+1$, entonces q es un residuo cuadrático módulo p si y sólo si p es un residuo cuadrático módulo q.*

(ii) *Si p es de la forma $4n+3$, entonces q es un residuo cuadrático módulo p si y sólo si $-p$ es un residuo cuadrático módulo q.*

2.3 El Lema de Gauss

Teorema 2.12 (Lema de Gauss). *Sea p un primo impar, a un entero coprimo con p y $R = \{k : -\frac{p-1}{2} \leq k \leq \frac{p-1}{2}\}$. Sea*

$$S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$$

y sea $S' \subseteq R$ el correspondiente conjunto de representantes módulo p. Si la cantidad de enteros negativos en S' es n, entonces

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Prueba. Primero probamos que los elementos de S son distintos módulo p y que salvo signo son $\{1, 2, \ldots, \frac{p-1}{2}\}$ (posiblemente en otro orden). Si $0 < i, j \leq \frac{p-1}{2}$ y $ai \equiv aj \mod p$, entonces $i \equiv j$ y luego $i = j$; por lo tanto los elementos de S son todos distintos. Ahora, $ai \equiv -aj \mod p$ implica que $i \equiv -j$, pero tampoco es posible si $i \neq j$. Como en S' hay $\frac{p-1}{2}$ elementos, en valor absoluto deben ser $\{1, 2, \ldots, \frac{p-1}{2}\}$.

Entonces,

$$a(2a)\ldots\big(\frac{p-1}{2}\big) \equiv (-1)^n \frac{p-1}{2}! \mod p;$$

luego

$$a^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv (-1)^n \frac{p-1}{2}! \mod p.$$

Como $\frac{p-1}{2}!$ es invertible módulo p, obtenemos que $a^{\frac{p-1}{2}} \equiv (-1)^n \mod p$, o $\left(\frac{a}{p}\right) = (-1)^n$. $\square$

Corolario 2.13. *Sea p un primo impar. Entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\omega(p)}, \text{ donde } \omega(p) \equiv \frac{p-1}{2} \mod 2 = \begin{cases} 0, & \text{si } p \equiv 1 \mod 4; \\ 1, & \text{si } p \equiv -1 \mod 4. \end{cases}$$

Es decir, 2 es un cuadrado módulo p si y sólo si $p \equiv 1, 7 \mod 8$.

2.4 Ejercicios

1. Listar todos los residuos cuadráticos y los no-residuos cuadráticos módulo p, para $p = 13, 17$.

2. Decir si las siguientes ecuaciones tienen o no solución.

$$x^2 \equiv -7 \mod 13; \quad 24x^2 \equiv 3 \mod 12; \quad x^2 \equiv 9 \mod 23.$$

3. ¿Existe sólo un número finito de primos p tales que $p|n^2 + 1$ para algún entero n?

4. Sea p un primo impar. Mostrar que el conjunto $\{2, 5, 10\}$ siempre contiene al menos un residuo cuadrático módulo p. Mostrar con un ejemplo que, sin embargo, todos pueden ser residuos cuadráticos.

5. Mostrar que las versiones de Gauss y Legendre son en efecto equivalentes.

6. Evaluar los siguientes símbolos de Legendre:

$$\left(\frac{11}{29}\right), \quad \left(\frac{23}{61}\right), \quad \left(\frac{7}{31}\right), \quad \left(\frac{60}{79}\right) \quad \text{y} \quad \left(\frac{133}{17}\right)$$

7. Decidir si las siguientes ecuaciones tienen o no solución y en caso afirmativo hallar alguna. (Ayuda: completar cuadrado)

$$x^2 + 4x + 3 \equiv 7 \mod 11; \qquad x^2 + 6x - 19 \equiv 24 \mod 101.$$

8. Determinar $\left(\frac{5}{p}\right)$ para todo primo p con $p \neq 5$.

9. Mostrar que un primo p tiene a lo sumo una representación de la forma $p = ax^2 + by^2$, con $x, y > 0$, para cada par de enteros a y b dados. ¿Qué primos p se pueden representar de la forma $p = x^2 + 7y^2$?

3 TERCERA CLASE
APLICACIONES

En esta tercera clase haremos 2 cosas. Una, resolver ecuaciones cuadráticas en $\mathbb{Z}_m$ y otra describir un algoritmo muy eficiente para decidir si un natural dado es primo o no.

3.1 Resolución de ecuaciones cuadráticas

Consideremos la ecuación general de segundo grado en $\mathbb{Z}_m$

$$ax^2 + bx + c \equiv 0 \mod m. \tag{3}$$

Nos proponemos resolver esta ecuación. Esto es, queremos decidir si tiene o no solución y en caso afirmativo decir cuántas tiene y finalmente encontrarlas.

Comenzamos como la hacemos sobre los números reales, completando el cuadrado. Recordemos que, en el caso real, las soluciones son de la forma $\frac{-b \pm \sqrt{b^2 - 4ac}}{2}$. Luego hay solución cuando el discriminante $b^2 - 4ac$ tiene raíz cuadrada. Una observación más es que $2a$ aparece en el denominador, es decir hace falta que $2a$ tenga inverso multiplicativo.

Multiplicando (3) por $4a$ obtenemos la ecuación

$$4a^2x^2 + 4ab + 4ac \equiv 0 \mod m, \tag{4}$$

que es equivalente a

$$(2ax + b)^2 + 4ac - b^2 \equiv 0 \mod m. \tag{5}$$

Si ponemos $y = 2ax + b$, ésta es equivalente al sistema de ecuaciones

$$\begin{aligned} y^2 &\equiv b^2 - 4ac \mod m \\ y &\equiv 2ax + b \mod m. \end{aligned} \tag{6}$$

Ya sabemos resolver con toda generalidad la ecuación lineal. En particular notamos que si $2a \in U(\mathbb{Z}_m)$, es decir si $(2a, m) = 1$, hay solución cualquiera sea y.

Sobre la ecuación cuadrática sabemos que tiene solución si y solo si las ecuaciones

$$y^2 \equiv b^2 - 4ac \mod p^k$$

tienen solución para todos los primos $p|m$ con k adecuado. Luego, si hay solución $b^2 - 4ac$ es residuo cudrático módulo p.

Por lo tanto nos concentramos en calcular *raices cuadradas* módulo p y módulo p^k, esto es resolver la ecuación

$$x^2 \equiv D \mod p^k.$$

Antes de continuar hacemos una observación importante.

Observación. Las ecuaciones (3) y (4) no son en genral equivalentes. Si $(4a, m) = 1$, entonces si lo son. Toda solución de (3) es solución de (4); es decir (4) tiene más soluciones que la original (3). ¿Que hacemos entonces? Una cosa obvia es simplemente resolver (4) y luego chequear cuáles soluciones son solución de (3). Otra cosa es considerar la ecuación

$$4a^2x^2 + 4abx + 4ac \equiv 0 \mod 4am, \tag{7}$$

que sí es equivalente a la original (3). Si, por ejemplo, $(4a, m) \neq 1$ pero $(a, m) = 1$ podemos también considerar la ecuación

$$4a^2x^2 + 4abx + 4ac \equiv 0 \mod 4m,$$

también equivalente a (3).

3.1.1 Raices cuadradas módulo p

Una vez que sabemos que la ecuación $x^2 \equiv a \mod p$ tiene solución (y entonces en general tiene 2), nos planteamos naturalmente cómo econtrar una. Una opción, aunque en general impráctica, es probar con $x = 1$, ..., $x = p - 1$.

Por ejemplo, resolvamos probando las siguientes ecuaciones e imaginemos que haríamos con otras más difíciles. ¿Porqué estamos seguros de que tienen solución?

Ejemplos 3.1.

1. $x^2 \equiv 5 \mod 19$. A probar.

x	1	2	3	4	5	6	7	8	9
x^2	1	4	9	16	6	17	11	7	5

2. $x^2 \equiv 2 \mod 41$. De nuevo a probar.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	...
x^2	1	4	9	16	25	36	7	22	39	18	39	21	5	...

Mostramos a continuación cómo calcular raices cuadradas módulo p. Consideramos por separado 2 casos, según sea $p \equiv 3 \mod 4$ o $p \equiv 1 \mod 4$.

Caso $p \equiv 3 \mod 4$.

Si $p = 4n + 3$, escribimos $p - 1 = 2s$ con $s = 2n + 1$ y elegimos $x = a^{(s+1)/2} = a^{n+1} = a^{(p+1)/4}$. Verifiquemos que $x^2 \equiv a \mod p$. En efecto

$$x^2 \equiv a^{2n+2} \equiv a^{2n+1}a \equiv a^{(p-1)/2}a \equiv a.$$

La última identidad se sigue del Criterio de Euler.

Caso $p \equiv 1 \mod 4$.

Si $p = 4n + 3$, escribimos $p - 1 = 2^r s$ con s impar y elegimos $y = a^{(s+1)/2}$. Como $y^2 \equiv a^{s+1} \equiv a^s a$, necesitamos encontrar un z tal que $z^2 \equiv a^s$, pues entonces $x = yz^{-1}$ será la solución buscada. Notemos que z existe pues a^s es un residuo cuadrático.

La ecuación $z^2 \equiv a^s$ la resolvemos probando, pero solamente con los números del conjunto

$$S = \{m^s, m^{2s}, \ldots, m^{2^r s}\},$$

donde m es cualquier no residuo módulo p. Notemos que el conjunto S tiene 2^r elementos, que en general es mucho más chico que p.

¿Porqué estamos seguros que z está en el conjunto S? En primer lugar, como a es un residuo cuadrático, entonces $1 \equiv a^{(p-1)/2} \equiv a^{2^{r-1}s}$ y luego el orden de a^s divide a 2^{r-1}. Como $z^2 \equiv a^s$, entonces el orden de z divide a 2^r. El Teorema de Lagrange implica que hay a lo sumo 2^r de estos elementos. Por otro lado, si m es un no residuo cuadrático, entonces el orden de m^s es exactamente 2^r ya que por el Criterio de Euler $(n^s)^{2^{r-1}} \equiv n^{(p-1)/2} \equiv -1$. De esto se sigue que los elementos del conjunto S son todos distintos y como son exactamente 2^r, son todos.

Veamos como funciona este método en algunos ejemplos.

Ejemplo 3.2. Hallar la raíz cuadrada de 5 módulo 101, si la tiene.

Como $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right)(-1)^{50\times 2} = \left(\frac{1}{5}\right) = 1$, entonces 5 si tiene raíz cuadrada módulo 101.

Dado que $101 \equiv 1 \mod 4$ estamos en el caso difícil. Ahora $100 = 2^2 \times 25$. Luego por un lado tomamos $y = 5^{13} \equiv 24^4 \times 5 \equiv 92 \times 5 \equiv 56 \mod 101$. Por el otro tomamos un residuo no cuadrático cualquiera, por ejemplo $m = 3$ y consideramos el conjunto

$$S = \{3^{25}, 3^{50}, 3^{75}, 3^{100}\}.$$

En este conjunto hay un número z que satisface $z^2 \equiv 5^{25}$.

Aprovechando los cálculos anteriores sabemos que $5^{25} \equiv 56 \times 92 \equiv 1 \mod 101$. Pero Fermat nos dice que $3^{100} \equiv 1 \mod 101$, es decir $(3^{50})^2 \equiv 1$. Entonces resulta que $x = \pm 56$ son las 2 raices cuadras de 5 módulo 101.

3.1.2 Raices cuadradas módulo p^k

Proposición 3.3. *Sea p un primo impar y a un entero no divisible por p. La ecuación $x^2 \equiv a \mod p^k$ tiene exactamente 2 soluciones si la ecuación $x^2 \equiv a \mod p$ tiene 2 soluciones, y no tiene ninguna solución si $x^2 \equiv a \mod p$ no tiene solución.*

Prueba. Supongamos primero que $x^2 \equiv a \mod p^k$ tiene solución, entonces es inmediato que $x^2 \equiv a \mod p$ también tiene solución. Veamos que en este caso son exactamente 2. Sea x_0 una solución y sea x cualquier otra. Notemos que $-x_0$ es también solución. Luego $p^k | x_0^2 - x^2$. Como no es posible que $p|x_0 - x$ y que $p|x_0 + x$, pues en ese caso $p|2x_0$, $p|x_0$ y $p|a$, entonces se sigue que $p^k|x_0 - x$ o $p^k|x_0 + x$. Es decir $x \equiv x_0 \mod p^k$ o $x \equiv -x_0 \mod p^k$. Luego no hay más que 2 soluciones.

Reciprocamente si $x^2 \equiv a \mod p^k$ no tiene solución, entonces $x^2 \equiv a \mod p$ tampoco. Esto se sigue del algortimo que mostramos a continuación que construye a partir de una solución de $x^2 \equiv a \mod p$ una de $x^2 \equiv a \mod p^k$. □

Describimos a continuación un algortimo para encontrar efectivamente las soluciones de $x^2 \equiv a \mod p^k$.

Sea α una solución de la ecuación $x^2 \equiv a \mod p$. Sean P_i y Q_i los enteros definidos por

$$P_i + Q_i\sqrt{a} = (\alpha + \sqrt{a})^i$$
$$P_i - Q_i\sqrt{a} = (\alpha - \sqrt{a})^i,$$

para $i \geq 1$. Notar que $P_1 = \alpha$ y $Q_1 = 1$. Como

$$P_i \pm Q_i = (P_{i-1} \pm Q_{i-1})(\alpha \pm \sqrt{a}),$$

se sigue que

$$P_i = \alpha P_{i-1} + aQ_{i-1} \quad \text{y} \quad Q_i = P_{i-1} + \alpha Q_{i-1}. \tag{8}$$

Ahora tenemos que

$$\begin{aligned} P_i + \alpha Q_i &= 2\alpha P_{i-1} + Q_{i-1}(a + \alpha^2) \\ &\equiv 2\alpha(P_{i-1} + \alpha Q_{i-1}) \mod p. \end{aligned}$$

Luego, por inducción, resulta que

$$P_i + \alpha Q_i \equiv (2\alpha)^2 \mod p$$

y así $p \nmid P_i + \alpha Q_i$. Por otro lado como $P_i - \alpha Q_i = Q_{i-1}(a - \alpha^2)$ si es divisible por p se sigue que $(Q_i, p) = (2\alpha Q_i, p) = 1$. De (8) se sigue por inducción que

$$P_i^2 - aQ_i^2 = (\alpha^2 - a)^i \equiv 0 \mod p^i.$$

Como $(Q_i, p) = 1$, existe $\overline{Q_i}$ con

$$Q_i\overline{Q_i} \equiv 1 \mod p^i;$$

multiplicando por $\overline{Q_i}$ la ecuación anterior a ésta se sigue que $\beta = P_i\overline{Q_i}$ satisface

$$\beta^2 \equiv a \mod p^i.$$

Ejemplo 3.4. Encontrar la raiz cuadrada de 14 módulo $625 = 5^4$.

Primero calculamos una raiz cuadrada de 14 módulo 5; $\alpha = 3$ satisface $\alpha^2 \equiv 9 \equiv 14 \mod 5$. Ahora comenzando con $P_1 = 3$ y $Q_1 = 1$ calculamos

$$P_2 = 23, Q_2 = 6, \quad P_3 = 153, Q_3 = 41, \quad P_4 = 1033, Q_4 = 276.$$

Luego la raiz que buscamos es $P_4\overline{Q_4} = 408 \times 351 \equiv 83$.

Falta aún considerar el caso $p^k = 2^k$. Sólo enunciamos la siguiente proposición.

Proposición 3.5. *Sea a un entero impar. Entonces*

(i) $x^2 \equiv a \mod 2$ *tiene exactamente una solución cualquiera sea a.*

(ii) $x^2 \equiv a \mod 4$ *tiene dos soluciones distintas si y sólo si $a \equiv 1 \mod 4$ y no tiene ninguna solución en caso contrario.*

(ii) $x^2 \equiv a \mod 2^n$, *con $n \geq 3$, tiene solución si y sólo si $a \equiv 1 \mod 8$. En este caso tiene cuatro soluciones. Si x_0 es una, $\pm x_0$ y $\pm x_0 + 2^{n-1}$ son las cuatro.*

3.2 Ejercicios

1. Determinar si las siguientes ecuaciones tiene solución y en caso afirmativo hallar todas.

   (a) $x^2 \equiv 61 \mod 169$

   (b) $x^2 \equiv 869 \mod 961$

   (c) $x^2 \equiv 191 \mod 529$

   (d) $x^2 \equiv 696 \mod 943$

(e) $x^2 \equiv 153 \mod 236$

(f) $x^2 \equiv 1225 \mod 1552$

2. Determinar si las siguientes ecuaciones tiene solución y en caso afirmativo hallar todas.

   (a) $7x^2 + 13x + 26 \equiv 0 \mod 97$

   (b) $5x^2 + 7x + 78 \equiv 0 \mod 136$

   (c) $6x^2 + 14x + 8 \equiv 0 \mod 21$

3. Estudiar para que valores de a la ecuación

$$6x^2 + 14x + a \equiv 0 \mod 1890$$

   tiene solución. Determinar además el número de soluciones.

3.3 Test de primalidad

El problema de entender los números primos está en el centro de la teoría de números desde hace muchos años. Una de las conjeturas abiertas más famosa de la matemática, la Conjetura de Riemann, predice como están distribuidos.

Mucho más recientemente la teoría de números y los números primos han encontrado aplicaciones fundamentales a la tecnología de las comunicaciones, en particular a la criptografía. Hoy en día cada transacción bancaria que viaja por la red está a salvo gracias a números primos muy grandes conocidos por muy pocos.

Quién tenga interés puede mirar la página web

`www.utm.edu/research/primes`

donde hay todo tipo de información sobre los números primos conocidos. En 2003 se descubrió el más grande que se conocce hasta ahora; tiene 6.320.430 dígitos.

Es así que el producir números primos o factorizar números que se creen primos puede ser un negocio más que lucrativo. El siguiente texto fue pegado de la página web de la compañía RSA Security (www.rsasecurity.com, The RSA Challenge Numbers).

RSA-2048

Prize: $ 200,000

Status: Not Factored

Decimal Digits: 617

25195908475657893494027183240048398571429282126204

03202777713783604366202070759555626401852588078440

69182906412495150821892985591491761845028084891200

72844992687392807287776735971418347270261896375014

97182469116507761337985909570009733045974880842840

17974291006424586918171951187461215151726546322822

16869987549182422433637259085141865462043576798423

38718477444792073993423658482382428119816381501067

48104516603773060562016196762561338441436038339044

14952634432190114657544454178424020924616515723350

77870774981712577246796292638635637328991215483143

81678998850404453640235273819513786365643912120103

97122822120720357

Decimal Digit Sum: 2738

Download Text

Comencemos haciendo algún esfuerzo. ¿Es el número 35 primo? Seguramente todos conocemo la respuestas y justamente por eso no recibiremos ni un centavo. De todos modos hagamos el siguente cálculo.

$$3^{17} \equiv (3^4 \times 3^4)^2 \times 3 \equiv (11 \times 11)^2 \times 3 \equiv 51^2 \times 3 \equiv 11 \times 3 \equiv 33 \mod 35.$$

Listo! No es primo.

En efecto, el criterio de Euler nos dice que si 35 fuera primo, entonces valdría que $3^{(35-1)/2} \equiv \pm 1 \mod 35$. En esta simple observación está basado uno de los algortimos más eficientes conocidos para decidir si un número dado es primo o no.

El siguiente resultado es un ingrediente fundamental del algoritmo que describiremos.

Proposición 3.6 (Ankeny). *Supongamos que la conjetura de Riemann es verdadera. Entonces, para cada primo impar p, hay un no-residuo cuadrático a tal que*

$$a \leq 2(\log p)^2.$$

Lema 3.7. *Sea $d \in \mathbb{N}$ impar. Si $a^{d-1} \equiv 1 \mod d$ para todo $a \in U(\mathbb{Z}_d)$, entonces d es libre de cuadrados.*

Prueba. Sea p un factor primo de d y sea p^t la mayor potencia de p que divide a d. Sea g un generador del grupo cíclico $U(\mathbb{Z}_{p^t})$ (Teorema 1.9). Sea x un natural tal que $x \equiv g \mod p^t$ y $x \equiv 1 \mod d/p^t$ (Teorema Chino del Resto). Entonces, por hipótesis $x^{d-1} \equiv 1 \mod d$ y luego $x^{d-1} \equiv 1 \mod p^t$; además como $x \equiv g \mod p^t$, entonces $g^{d-1} \equiv x^{d-1} \equiv 1 \mod p^t$. Como el orden de g es $p^t(p-1)$, entonces $p^t(p-1)|d-1$, que sólo es posible si $t = 1$. Por lo tanto d es libre de cuadrados. □

El síbolo de Legendre $\left(\frac{a}{p}\right)$ está definido sólo cuando p es primo, sin embrago resulta útil extender su definición.

Definición 3.8. Sea a un entero y d un entero impar positivo. Si d se factoriza como $d = p_1 \dots p_k$ en producto de primo, entonces el síbolo de Jacobi $\left(\frac{a}{d}\right)$ está definido por

$$\left(\frac{a}{d}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right),$$

donde los síbolos de la derecha son símbolos de Legendre.

Aunque el símbolo de Jacobi $\left(\frac{a}{d}\right)$ no está directamente relacionado al hecho de ser o no a un residuo cuadrático módulo d, tiene las mismas propiedades formales que el símbolo de Legendre; en particular vale la Ley de Reciprocidad Cuadrática.

Si $m, n > 0$ son enteros impares, entonces

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

Proposición 3.9. *Supongamos que la conjetura de Riemann es verdadera. Entonces, para un entero impar d son equivalentes:*

(i) *d es primo;*

(ii) *Para todo $a \in \mathbb{N}$ con $a \in U(\mathbb{Z}_d)$ y $a \leq 2(\log p)^2$ vale:*

$$a^{\frac{d-1}{2}} \equiv \left(\frac{a}{d}\right) \mod d.$$

Prueba. El Criterio de Euler prueba que (i)implica (ii).

Del lema anterior se sigue que $d = p_1 \dots p_r$ es producto de primos distintos. Sea $\alpha \in U(\mathbb{Z}_{p_1})$ tal que $\left(\frac{\alpha}{p_1}\right) = -1$ (que existe pues p_1 es impar). Ahora sea $a \in \mathbb{N}$ tal que $a \equiv \alpha(p_1)$ y $a \equiv 1(p_i)$ para $i = 2 \dots r$. Así tenemos que $a \in U(\mathbb{Z}_d)$ y

$$\left(\frac{a}{d}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right) = -1,$$

luego $a^{\frac{d-1}{2}} \equiv -1(d)$ y finalmente $a^{\frac{d-1}{2}} \equiv -1(p_2)$, que es una contradiccón. Por lo tanto p_2 no existe y d es primo. □

De esta proposición surge el siguiente algoritmo para decidir si un número natural dado es primo o no.

Test de primalidad de Solovay y Strassen

Sea d un natural impar y sea $a = 3$.

1. Calcular (a, d). Si $(a, d) \neq 1$, terminar. NO ES PRIMO.
2. Calular $a^{\frac{d-1}{2}}$ y $\left(\frac{a}{d}\right)$ módulo d. Si son distintos, terminar. NO ES PRIMO.
3. Incrementar a en 1. Si $a > 2(\log d)^2$, terminar. **ES PRIMO**.
4. Volver a 1.

Este algoritmo decide si d es primo o no en tiempo poliomial (en el número de dígitos).

La Criba de Eratóstenes, que se aprende en la escuela, es otro algoritmo para testear la primalidad de un natural. Este requiere tiempo exponencial (en el número de dígitos).

Criba de Eratóstenes

Sea d un natural impar y sea $a = 3$.

1. Calcular (a, d). Si $(a, d) \neq 1$, terminar. NO ES PRIMO.
2. Incrementar a en 1. Si $a > sqrt(d)$, terminar. **ES PRIMO**.
3. Volver a 1.

Comparemos la cantidad de casos que es necesario tester en uno y otro algortimos cuando queremos decidir si un número grande, digamos de entre 10 y 200 dígitos, es primo o no.

d	10^{10}	10^{20}	10^{40}	10^{80}	10^{200}
$\sqrt{d}$	10^5	10^{10}	10^{20}	10^{40}	10^{100}
$2(\log d)^2 \sim$	1060	4241	16966	67864	424151

Ambos algoritmos son muy fáciles de implementar. La siguientes tablas muestran el tiempo en segundos requerido por ambos algortimos para decidir que ciertos números son o no primos. La primera tabla contiene sólo números primos, mientras que la segunda contiene sólo números compuestos. Los algortimos fueron implementados usando Magma en una misma computadora.

Tabla de números primos

Dígitos	Primo	Solovay Strassen	Eratóstenes
10	5915587277	0.03	0.15
11	76778329031	0.05	0.54
12	387965390731	0.05	1.21
13	3647948372479	0.07	3.96
14	69308723175841	0.08	21.05
15	873749123394023	0.11	76.84
16	7367789546931337	0.13	307.34
17	99153275743439773	0.17	2046.41
18	346597323152177437	0.17	
19	4637889300435020321	0.19	
20	48112959837082048697	0.36	

Tabla de números compuestos

Dígitos	Número Descomposición	Solovay Strassen	Eratóstenes
15	239811859939591 15485863×15485857	0.01	64.22
16	7400836914565673 86028121×86028113	0.01	369.58
16	3458452900645327 $13 \times 61 \times 4361226860839$	0.01	0.01
20	34726098733214543007 $3 \times 9090203 \times 1273389191023$	0.01	0.01

4 Apéndice

La Ley de Reciprocidad Cuadrática fue probada por primera vez por Gauss en 1801, luego de que Legendre diera una prueba incompleta en 1788. Desde entonces y hasta nuestros dias se publican nuevas pruebas; muchas de ellas son pequeñas variaciones de otras. El mismo Gauss dió 6 pruebas distintas.

En la página `http://www.rzuser.uni-heidelberg.de/ hb3`, se han recopilado pruebas y referencias a la Ley de Reciprocidad y sus generalizaciones; se pueden ver más de 1.000 referencias. A continuación mostramos la tabla que compila cronológicamente las pruebas conocidas.

Author	Year	Method	Author	Year	Method
1. Legendre	1788	Quadratic forms †	2. Gauss 1	1801	Induction
3. Gauss 2	1801	Quadratic forms	4. Gauss 3	1808	Gauss' Lemma
5. Gauss 4	1811	Cyclotomy	6. Gauss 5	1818	Gauss' Lemma
7. Gauss 6	1818	Gauss' sums	8. Cauchy	1829	Gauss 6
9. Jacobi	1830	Gauss 6	10. Dirichlet 1	1835	Gauss 4
11. Lebesgue 1	1838		12. Schönemann	1839	Quad. period eq.
13. Cauchy	1840	Gauss 4	14. Eisenstein 1	1844	Gen. Jacobi sums
15. Eisenstein 2	1844	Gauss 6	16. Eisenstein 3	1844	Gauss' Lemma
17. Eisenstein 4	1845	Sine	18. Eisenstein 5	1845	Infinite products
19. Liouville	1847	Cyclotomy	20. Lebesgue 2	1847	Lebesgue 1
21. Schaar	1847	Gauss' Lemma	22. Plana 1	1852	
23. Genocchi 1	1852	Gauss' Lemma	24. Dirichlet 2	1854	Gauss 1
25. Lebesgue 3	1860	Gauss 7, 8	26. Kummer 1	1862	Quadratic forms
27. Kummer 2	1862	Quadratic forms	28. Dedekind 1	1863	Quadratic forms
29. Gauss 7	1863	Quadratic periods	30. Gauss 8	1863	Quadratic periods
31. Mathieu	1867	Cyclotomy	32. von Staudt	1867	Cyclotomy
33. Bouniakowski	1869	Gauss' Lemma	34. Stern	1870	Gauss' Lemma
35. Zeller	1872	Gauss' Lemma	36. Zolotarev	1872	Permutations
37. Kronecker 1	1872	Zeller	38. Schering 1	1875	Gauss 3
39. Kronecker 2	1876	Induction	40. Mansion 1	1876	Gauss' Lemma
41. Dedekind 2	1877	Gauss 6	42. Dedekind 3	1877	Dedekind Sums
43. Pellet 1	1878	Stickelberger-Voronoi	44. Pépin 1	1878	Cyclotomy
45. Sochocki	1878	Theta functions	46. Schering 2	1879	Gauss' Lemma
47. Petersen	1879	Gauss' Lemma	48. Genocchi 2	1880	Gauss' Lemma
49. Kronecker 3	1880	Gauss 4	50. Kronecker 4	1880	Quadratic period
51. Voigt	1881	Gauss' Lemma	52. Pellet 2	1882	Mathieu 1867
53. Busche 1	1883	Gauss' Lemma	54. Gegenbauer 1	1884	Gauss' Lemma
55. Kronecker 5	1884	Gauss Lemma	56. Kronecker 6	1885	Gauss 3
57. Kronecker 7	1885	Gauss' Lemma	58. Bock	1886	Gauss Lemma
59. Lerch 1	1887	Gauss 3	60. Busche 2	1888	Gauss' Lemma
61. Hacks	1889	Schering	62. Hermes	1889	Induction
63. Kronecker 8	1889	Gauss' Lemma	64. Tafelmacher 1	1889	Stern
65. Tafelmacher 2	1889	Stern/Schering	66. Tafelmacher 3	1889	Schering
67. Busche 3	1890	Gauss' Lemma	68. Franklin	1890	Gauss' Lemma
69. Lucas	1890	Gauss Lemma	70. Pépin 2	1890	Gauss 2
71. Fields	1891	Gauss' Lemma	72. Gegenbauer 2	1891	Gauss' Lemma
73. Gegenbauer 3	1893	Gauss' Lemma	74. Schmidt 1	1893	Gauss' Lemma
75. Schmidt 2	1893	Gauss' Lemma	76. Schmidt 3	1893	Induction
77. Gegenbauer 4	1894	Gauss' Lemma	78. Bang	1894	Induction
79. Mertens 1	1894	Gauss' Lemma	80. Mertens 2	1894	Gauss sums
81. Busche 4	1896	Gauss Lemma	82. Lange 1	1896	Gauss' Lemma
83. Mansion 2	1896	Gauss 2	84. de la Vallée Poussin	1896	Gauss 2
85. Lange 2	1897	Gauss' Lemma	86. Hilbert	1897	Cyclotomy
87. Alexejewsky	1898	Schering	88. Pépin 3	1898	Legendre
89. Pépin 4	1898	Gauss 5	90. König	1899	Induction
91. Fischer	1900	Resultants	92. Takagi	1903	Zeller
93. Lerch 2	1903	Gauss 5	94. Mertens 3	1904	Eisenstein 4
95. Mirimanoff & Hensel	1905	Stickelberger-Voronoi	96. Cornacchia 5	1909	
97. Busche 5	1909	Zeller	98. Busche 6	1909	Eisenstein
99. Aubry	1910	= Eisenstein 3	100. Aubry	1910	= Voigt

†Esta prueba es incompleta.

Author	Year	Method	Author	Year	Method
101. Aubry	1910	= Kronecker	102. Pépin 5	1911	Gauss 2
103. Petr 1	1911	Mertens 3	104. Pocklington	1911	Gauss 3
105. Dedekind 3	1912	Zeller	106. Heawood	1913	Geometric
107. Frobenius 1	1914	Zeller	108. Frobenius 2	1914	Geom. (Eisenstein)
109. Lasker	1916	Stickelberger-Voronoi	110. Cerone	1917	Eisenstein 4
111. Bartelds-Schuh	1918	Gauss' Lemma	112. Stieltjes	1918	Lattice points
113. Teege 1	1920	Legendre	114. Teege 2	1921	Cyclotomy
115. Arwin	1924	Quadratic forms	116. Rédei 1	1925	Gauss' Lemma
117. Rédei 2	1926	Gauss' Lemma	118. Whitehead	1927	Genus (Kummer)
119. Petr 2	1927	Theta functions	120. Skolem 1	1928	Genus theory
121. Petr 3	1934	Kronecker (signs)	122. van Veen	1934	Geom. (Eisenstein)
123. Fueter	1935	Quaternion algebras	124. Whiteman	1935	Gauss' Lemma
125. Dockeray	1938	Eisenstein 3	126. Dörge	1942	Gauss' Lemma
127. Rédei 3	1944	Gauss 5	128. Lewy	1946	Cyclotomy
129. Petr 4	1946	Cyclotomy	130. Skolem 2	1948	Gauss 2
131. Barbilian	1950	Eisenstein 1	132. Rédei 4	1951	Gauss 3
133. Brandt 1	1951	Gauss 2	134. Brandt 2	1951	Gauss sums
135. Brewer	1951	Mathieu, Pellet	136. F. de Almeida	1951	Finite fields
137. Zassenhaus	1952	Finite fields	138. Riesz	1953	Permutations
139. Fröhlich	1954	Class Field Theory	140. Ankeny	1955	Cyclotomy
141. D.H. Lehmer	1957	Gauss' Lemma	142. C. Meyer	1957	Dedekind sums
143. Holzer	1958	Gauss sums	144. Rédei 5	1958	Cyclotomic polynom.
145. Reichardt	1958	Gauss 3	146. Carlitz	1960	Gauss 1
147. Kubota 1	1961	Cyclotomy	148. Kubota 2	1961	Gauss sums (sign)
149. Skolem 3	1961	Cyclotomy	150. Skolem 4	1961	Finite fields
151. Hausner	1961	Gauss sums	152. Swan 1	1962	Stickelberger-Voronoi
153. Gerstenhaber	1963	Eisenstein, sine	154. Koschmieder	1963	Eisenstein, sine
155. Rademacher	1964	Finite Fourier anal.	156. Weil	1964	Theta functions
157. Kloosterman	1965	Holzer	158. Chowla	1966	Finite fields
159. Burde	1967	Gauss' Lemma	160. Kaplan 1	1969	Eisenstein
161. Kaplan 2	1969	Quad. congruences	162. Birch	1971	K-groups (Tate)
163. Reshetukha	1971	Gauss sums	164. Agou	1972	Finite fields
165. Brenner	1973	Zolotarev	166. Honda	1973	Gauss sums
167. Milnor-Husemöller	1973	Weil 1964	168. Allander	1974	Gauss' Lemma
169. Berndt-Evans	1974	Gauss' Lemma	170. Hirzebruch-Zagier	1974	Dedekind Sums
171. Rogers	1974	Legendre	172. Castaldo	1976	Gauss' Lemma
173. Frame	1978	Kronecker (signs)	174. Hurrelbrink	1978	K-theory
175. Auslander-Tolimieri	1979	Fourier transform	176. Brown	1981	Gauss 1
177. Goldschmidt	1981	cyclotomy	178. Kac	1981	Eisenstein, sine
179. Barcanescu	1981	Zolotarev	180. Zantema	1983	Brauer groups
181. Ely	1984	Lebesgue 1	182. Eichler	1985	Theta function
183. Barrucand-Laubie	1987	Stickelberger-Voronoi	184. Peklar	1989	Gauss' Lemma
185. Barnes	1990	Zolotarev	186. Swan 2	1990	Cyclotomy
187. Rousseau 1	1990	Exterior algebras	188. Rousseau 2	1991	Permutations
189. Keune	1991	Finite fields	190. Kubota 3	1992	Geometry
191. Russinoff	1992	Gauss' Lemma	192. Garrett	1992	Weil 1964
193. Motose	1993	Group algebras	194. Rousseau 3	1994	Zolotarev
195. Young	1995	Gauss' sums	196. Brylinski	1997	Group actions
197. Merindol	1997	Eisenstein, sine	198. Watanabe	1997	Zolotarev
199. Ishii	1998	Gauss 4	200. Motose	1999	Group algebras
201. Zahidi	2000	Stickelberger-Voronoi	202. Lemmermeyer	2000	Lebesgue 1, Ely
203. Meyer	2000	Dedekind sums	204. Tangedal	2000	Eisenstein, geometric
205. Chapman	2001	Recurring sequences	206. Hammick	2001	Rousseau 2
207. Girstmair	2001	Eichler	208. Sey Yoon Kim	2003	Rousseau 2

4.1 Una prueba de la Ley de Reciprocidad Cuadrática

Está claro que no resulta fácil elegir una prueba de la Ley de Reciprocidad Cuadrática. Algunas de ellas son más conceptuales que otras, pero requieren algunas herramientas más sofisticadas. Algunas son más accesibles, pero más largas y técnicas. Ante tal diversidad decidimos incluir la última prueba, recientemente aparecida en el primer número de 2004 de "The American Mathematical Monthly".

Una prueba elemental de la Ley de Reciprocidad Cuadrática, por Sey Y. Kim.

Definamos el conjunto Φ por

$$\Phi = \{a:\ 1 \leq a \leq \frac{pq-1}{2},\ (a,pq) = 1\},$$

y sea $A = \prod_{a\in\Phi} a$.

Lema. $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \mod p$ *y* $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \mod q$.

Prueba. Sean S y T definidos por

$$S = \{a:\ 1 \leq a \leq \frac{pq-1}{2},\ (a,p) = 1\}, \qquad T = \{q, 2q, \ldots, \frac{p-1}{2}q\}.$$

Es claro que T es un subconjunto de S y como

$$\frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2},$$

se sigue fácilmente que $\Phi = S - T$. Luego, por el criterio de Euler,

$$\prod_{a\in S} a = \prod_{a\in T} a \prod_{a\in\Phi} a = q^{\frac{p-1}{2}} \left[\frac{p-1}{2}\right]! \ A \equiv \left(\frac{q}{p}\right) \left[\frac{p-1}{2}\right]! \ A \mod p.$$

Por otro lado, como

$$\frac{pq-1}{2} = \frac{q-1}{2}p + \frac{p-1}{2},$$

tenemos que

$$\prod_{a\in S} a \equiv [(p-1)!]^{\frac{q-1}{2}} \left[\frac{p-1}{2}\right]! \equiv (-1)^{\frac{q-1}{2}} \left[\frac{p-1}{2}\right]! \mod p;$$

notar que hemos usado el teorema de Wilson: $(p-1)! \equiv -1 \mod p$. Deducimos entonces que

$$\left(\frac{q}{p}\right) \left[\frac{p-1}{2}\right]! \ A \equiv (-1)^{\frac{q-1}{2}} \left[\frac{p-1}{2}\right]! \mod p,$$

y así $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \mod p$. La otra parte del enunciado se sigue por simetría. □

De este Lema se sigue inmediatamente que $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ si y sólo si $A \equiv \pm 1 \mod pq$.

Lema. *$A \equiv \pm 1 \mod pq$ si y sólo si $p \equiv q \equiv 1 \mod 4$.*

Prueba. Sea $d = pq$. Por el Teorema Chino del Resto, la ecuación $X^2 \equiv 1 \mod d$ tiene precisamente cuatro soluciones, $X \equiv 1, -1, N, -N \mod d$. La ecuación $X^2 \equiv -1$ tiene una solución $X \equiv I \mod d$ si y sólo si $p \equiv q \equiv 1 \mod 4$, en cuyo caso hay cuatro soluciones, $X \equiv I, -I, NI, -NI \mod d$.

Ahora para cada $a \in \Phi$ hay únicos a' en Φ y $\delta_a \in \{-1, 1\}$ tales que $aa' \equiv \delta_a \mod d$. (La correspondencia $a \mapsto a'$ es una permutación de Φ.) Escribiendo

$$\Psi = \{a \in \Phi : \ a = a'\} = \{a \in \Phi : \ a^2 \equiv \pm 1 \mod d\}$$

observamos que

$$A = \prod_{a \in \Phi} a \equiv \pm \prod_{a \in \Psi} a \mod d.$$

Si $p \equiv q \equiv 1 \mod 4$, tenemos que

$$\prod_{a \in \Psi} a \equiv \pm(1 \cdot N \cdot I \cdot IN) \equiv \pm(N^2 \cdot I^2) \equiv \mp 1 \mod d,$$

y en caso contrario

$$\prod_{a \in \Psi} a \equiv \pm(1 \cdot N) \not\equiv \pm 1 \mod d.$$

Ahora el lema se sigue directamente. □

Combinando ambos Lemas concluimos que

$$(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \quad \text{si y sólo si} \quad p \equiv q \equiv 1 \mod 4.$$

La Ley de Reciprocidad Cuadrática se sigue ahora considerando los cuatro casos $(p, q) \equiv (1, 1), (1, -1), (-1, 1), (-1, -1) \mod 4$. O dicho con fórmulas, como $p \equiv q \equiv 1 \mod 4$ si y sólo si $(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = -1$,

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

Pero

$$\begin{aligned}\frac{p-1}{2}\frac{q-1}{2} &= \frac{pq-p-q+1}{4} = \frac{pq+p+q+1}{4} - \frac{p+q}{2} \\ &= \frac{p+1}{2}\frac{q+1}{2} - \left(\frac{p-1}{2} + \frac{q-1}{2} + 1\right) \\ &= \frac{p+1}{2}\frac{q+1}{2} + \left(\frac{p-1}{2} + \frac{q-1}{2} + 1\right) \mod 2,\end{aligned}$$

mostrando que $-(-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.