TEMat

Ley de reciprocidad cuadrática y aplicaciones

Mario Pérez Maletzki
Universitat Jaume I
maletzki@uji.es

Resumen: El objetivo de este trabajo es introducir todos los conceptos y teoremas necesarios para poder dar una demostración rigurosa y autocontenida de la ley de reciprocidad cuadrática y ver cómo puede ser una herramienta útil para obtener resultados tales como el problema de los dos cuadrados, el problema de determinar cuándo una ecuación en congruencias de segundo grado tiene solución, probar ciertas propiedades sobre los números primos y hasta para obtener información sobre el conjunto de ceros de ciertas ecuaciones elípticas.

Acompañamos los resultados con ejemplos elegidos para mejorar la comprensión de los mismos, donde hemos usado el programa GAP por ser muy conveniente para este tipo de matemáticas, e incluimos los códigos para que el lector pueda fácilmente comprobarlos.

Abstract: The goal of this survey is to introduce all the necessary concepts and theorems to provide a rigorous and self-contained proof of the Quadratic Reciprocity Law and see how this is a useful tool to obtain results such as the problem of the two squares, the problem of determining when a second degree congruence equation has any solution, to prove some properties about prime numbers and even to obtain information about the zero set of an elliptic curve.

We include examples specifically chosen to improve the understanding of those theorems. These examples have been created with the program GAP due to its convenience for this topic of mathematics and we include the codes so the reader can readily test them.

Palabras clave: Ley de reciprocidad cuadrática, GAP, residuo cuadrático, símbolo de Legendre.

MSC2020: 11A07.

Recibido: 15 de octubre de 2021.
Aceptado: 7 de septiembre de 2022.

Referencia: Pérez Maletzki, Mario. «Ley de reciprocidad cuadrática y aplicaciones». En: *TEMat*, 7 (2023), págs. 51-66. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p51.

1. Introducción

El desarrollo y descubrimiento de la ley de reciprocidad cuadrática fue muy lento e involucró a muchos matemáticos tales como Gauss, Euler y Legendre entre otros. Sus orígenes se remontan a cuestiones sobre ecuaciones diofánticas y el problema que escribió Fermat a Mersenne en una carta en la cual afirmaba:

> Todo número primo, que supere por una unidad un múltiplo de 4, es una única vez la suma de dos cuadrados, y es una única vez la hipotenusa de un triángulo rectángulo.

Fermat, como era costumbre en él, no dio una demostración de este enunciado y hubo que esperar a Euler para que la proporcionara pasados unos años.

Euler se interesó pues en la teoría de números y, como veremos, formuló un criterio muy útil para determinar cuando un entero era un residuo cuadrático módulo un primo dado y conjeturó enunciados muy similares al que afirma la ley de reciprocidad cuadrática, pero no fue hasta que llegó Gauss, quien, a sus diecinueve años, enunció y probó este teorema. Mientras Euler se preguntaba si dado un número como módulo, otro número era residuo cuadrático de este, Gauss planteó el problema inverso: Dado un número entero, ¿módulo qué enteros es este un residuo cuadrático? Es por esto que se adoptó el nombre de ley de reciprocidad cuadrática, a la cual Gauss denominó el *Theorema Aureum*. Gauss dio ocho demostraciones distintas de este teorema a lo largo de su vida y, a día de hoy, este es uno de los teoremas con más demostraciones distintas de la historia de las matemáticas. Una gran variedad de pruebas distintas puede encontrarse en la obra recopilatoria de Oswald Baumgart [2].

La bibliografía principal será el clásico libro de Gauss, *Disquisitiones arithmeticae* [5]. Procuramos que este trabajo sea autocontenido, utilizando el mínimo número de resultados sin probar posibles, pero sí suponemos un conocimiento básico de aritmética modular y utilizamos el hecho de que el anillo $\mathbb{Z}_p$ de los enteros módulo p tiene estructura de cuerpo para cada primo p. Para una prueba de este último resultado el lector puede consultar, por ejemplo, el libro *Un curso de álgebra* [7].

Debido a la continua evolución del sistema GAP es posible que el código incluido en este trabajo quede desfasado cuando el lector pudiera ejecutarlo, por lo que recomendamos consultar el manual de referencia oficial [4] y comprobar la versión de GAP que se utilice.

2. Ley de reciprocidad cuadrática

Comenzamos definiendo qué es un residuo cuadrático.

Definición 1 (residuo cuadrático). Sea m un entero mayor o igual que 2. Diremos que un entero n es un residuo cuadrático módulo m si tiene solución la siguiente congruencia:

$$x^2 \equiv n \pmod{m}.$$

De la definición es claro que si n' es otro entero tal que $n \equiv n' \pmod{m}$, entonces n será un residuo cuadrático módulo m si y solo si lo es n'. También observamos que 0 y 1 son trivialmente residuos cuadráticos para cualquier m (basta con tomar $x = m$ para $n = 0$ y $x = 1$ para $n = 1$).

Ejemplo 2. Tenemos que $2^2 \equiv 1 \pmod{3}$, luego 1 es un residuo cuadrático módulo 3.

Observación **3.** Si x es una solución de la anterior ecuación, cualquier y congruente con x módulo m también lo será, pues si $x \equiv y \pmod{m}$ entonces $x^2 \equiv y^2 \pmod{m}$.

Esta observación es muy útil, pues nos indica que debemos buscar soluciones en el conjunto $\{1, \dots, m-1\}$. Así pues, para ver que 2 no puede ser un residuo cuadrático módulo 3 basta con observar que

$$\begin{aligned} 0^2 &\not\equiv 2 \pmod{3}, \\ 1^2 &\not\equiv 2 \pmod{3}, \\ 2^2 &\not\equiv 2 \pmod{3}. \end{aligned}$$

Proposición 4. *Dado un entero positivo m, en el conjunto $\{0, 1, \dots, m-1\}$ puede haber como máximo $\frac{m}{2}+1$ residuos cuadráticos si m es par y $\frac{m+1}{2}$ si m es impar.*

Demostración. Estudiamos de entre los números $\{1^2, 2^2, \dots, (m-1)^2\}$ cuántos son congruentes entre sí módulo m.

Supongamos que m es impar. En este caso $m-1$ es par y, como además $(m-1)^2 \equiv 1^2 \pmod{m}$, $(m-2)^2 \equiv 2^2 \pmod{m}$, etc., concluimos que como máximo puede haber $1 + \frac{m-1}{2} = \frac{m+1}{2}$ residuos cuadráticos distintos.

Si m es par, de forma análoga obtenemos que $(m-1)^2 \equiv 1^2 \pmod{m}$, $(m-2)^2 \equiv 2^2 \pmod{m}$, …, $\left(\frac{m}{2}+1\right)^2 \equiv \left(\frac{m}{2}-1\right)^2 \pmod{m}$ y tenemos que puede haber como máximo $1 + \frac{m-2}{2} + 1 = \frac{m}{2} + 1$ residuos cuadráticos. ∎

Nota 5. De ahora en adelante supondremos que el módulo es $m > 2$, pues todo entero es residuo cuadrático módulo 2 (lo cual se deduce fácilmente del comentario después de la definición 1) y por tanto el caso $m = 2$ carece de interés.

Cuando tratamos con congruencias módulo un número primo podemos refinar el anterior resultado:

Teorema 6. *Sea p un número primo. Entonces exactamente la mitad de los elementos de $\{1, 2, \dots, (p-1)\}$ son residuos cuadráticos módulo p.*

Demostración. Vamos a probar que ningún par de números en $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ pueden ser congruentes entre sí módulo p, y por tanto, todos ellos serán residuos cuadráticos distintos módulo p y como por la proposición anterior no pueden haber más de $\frac{p-1}{2}$ residuos distintos de 0, habremos terminado.

Si $1 \leq x < y \leq \frac{p-1}{2}$ son tales que $x^2 \equiv y^2 \pmod{p}$ entonces $p \mid (x-y)(x+y)$ pero, como $x + y < p$, esto solo puede ser posible si $x = y$. ∎

Ejemplo 7. Veamos cuántos residuos cuadráticos hay módulo 13 y 15, respectivamente.

```
gap> Z13:= Integers mod 13;
     GF(13)
gap> List(Elements(Z13),x_->Int(x^2));
     [ 0, 1, 4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10 ]
```

Observamos que hay seis residuos cuadráticos módulo 13 entre $\{1, 2, \dots, 12\}$, lo cual sabíamos que debía ocurrir por ser 13 primo.

```
gap> Z15:= Integers mod 15;
     (Integers mod 15)
gap> List( Elements (Z15) , x _> Int(x^2)  );
     [ 0, 1, 4, 9, 1, 10, 6, 4, 4, 6, 10, 1, 9, 4, 1 ]
```

En este caso (siendo 15 un número compuesto) nos encontramos con que solo hay cinco residuos cuadráticos módulo 15 en $\{1, 2, \dots, 14\}$.

Teorema 8. *Sean p un número primo y a y b enteros coprimos con p. Si ambos son residuos cuadráticos módulo p, su producto ab también es un residuo cuadrático módulo p; si uno de ellos lo es pero el otro no, entonces su producto tampoco lo es y si ninguno de ellos lo es, su producto sí lo es.*

Demostración. Si ambos lo son, deben existir enteros x e y tales que

$$x^2 \equiv a \pmod{p},$$
$$y^2 \equiv b \pmod{p},$$

y por tanto tenemos que

$$(xy)^2 \equiv x^2 y^2 \equiv ab \pmod{p},$$

de lo cual concluimos que ab es un residuo cuadrático módulo p.

Supongamos que a lo es pero b no. Por serlo a, existirá un x entero tal que $x^2 \equiv a \pmod{p}$, y si ab también lo fuera existiría otro entero z tal que $z^2 \equiv ab \pmod{p}$, pero entonces, teniendo en cuenta que, por ser x coprimo con p tiene inverso en $\mathbb{Z}_p$, tendríamos que

$$z^2 \equiv ab \equiv x^2 b \pmod{p}$$

y por tanto que

$$(zx^{-1})^2 \equiv z^2 (x^{-1})^2 \equiv b \pmod{p},$$

lo cual es una contradicción, pues habíamos supuesto que b no es residuo cuadrático.

Finalmente, si ni a ni b son residuos cuadráticos módulo p, multiplicamos a por cada elemento de $\{1, \dots, p-1\}$ que sí sea residuo cuadrático y obtenemos un total de $\frac{p-1}{2}$ residuos no cuadráticos. Pues en dicho conjunto sabemos que hay $\frac{p-1}{2}$ residuos cuadráticos y que al multiplicarlos por el residuo no cuadrático a obtenemos un residuo no cuadrático y, si $ax \equiv ay \pmod{p}$, entonces multiplicando en ambos lados por el inverso de a en $\mathbb{Z}_p$ llegamos a que $x \equiv y \pmod{p}$. Por tanto, como hay justamente $\frac{p-1}{2}$ residuos no cuadráticos, y todos ellos son el producto de a con un residuo cuadrático, necesariamente ab tiene que ser un residuo cuadrático, pues estamos suponiendo que b no lo es. ∎

El siguiente teorema será crucial para probar el criterio de Euler (teorema 10), el cual a su vez será la primera herramienta efectiva para determinar cuándo un entero es un residuo cuadrático módulo un número primo.

Teorema 9 (teorema de Wilson). *Sea p un entero mayor que 1. Entonces p es primo si y solo si*

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración. Para la implicación directa, supongamos que p es un número primo. Sabemos entonces que $\mathbb{Z}_p$ es cuerpo y, en particular, que todo elemento no nulo tiene inverso respecto a la multiplicación (y que es único). Además, solo hay dos números que sean inversos de sí mismos: En efecto, supongamos que $1 \leq x \leq p-1$ es tal que $x \equiv x^{-1} \pmod{p}$ o, lo que es lo mismo, que $x^2 \equiv 1 \pmod{p}$. Entonces, $(x-1)(x+1)$ es divisible por p y, como p es primo, esto solo puede ocurrir si o bien $x = 1$, o bien $x = p-1$. Por tanto, si multiplicamos todos los elementos de $\{1, 2, \dots, p-1\}$, agrupando dos a dos cada uno con su inverso tenemos que

$$(p-1)! \equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv (p-1) \equiv -1 \pmod{p}.$$

Para la implicación inversa, supongamos que p es un entero que cumple que $(p-1)! \equiv -1 \pmod{p}$. Supongamos que p no es primo y sea $1 < c < p$ un divisor propio de p. Obviamente c divide a $(p-1)!$ y, como por hipótesis $(p-1)! \equiv -1 \pmod{p}$, esto quiere decir que p divide a $(p-1)! + 1$ y, al ser c un divisor de p, c será también un divisor de $(p-1)! + 1$. Pero esto es imposible, pues el único entero que divide a dos números consecutivos es el 1 y habíamos supuesto que $1 < c < p$. ∎

Teorema 10 (criterio de Euler). *Sea p un primo impar y a un entero coprimo con p. Entonces*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{si } a \text{ es un residuo cuadrático módulo } p, \\ -1 \pmod{p} & \text{si } a \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Demostración. Consideramos los pares de elementos (x, y) tales que $x \leq y \leq p-1$ y $xy \equiv a \pmod{p}$. Observamos que para cada x existe un único $y \in \mathbb{Z}_p$ tal que $xy \equiv a \pmod{p}$ pues, al ser p primo y x coprimo con p, el inverso de x en $\mathbb{Z}_p$ existe y $x \cdot (x^{-1}a) \equiv a \pmod{p}$. Además, si $xz \equiv a \pmod{p}$ entonces $xy \equiv xz \pmod{p}$ y, multiplicando por x^{-1} en ambos lados, llegaríamos a $y \equiv z \pmod{p}$ que, al ser $1 \leq y, z \leq p-1$, solo puede ocurrir si $y = z$.

Distinguimos pues dos casos. Si a no es residuo cuadrático, los elementos que forman cada uno de los pares posibles tienen que ser necesariamente distintos entre sí, y como hay $p-1$ elementos habrá $\frac{p-1}{2}$ pares. Si los multiplicamos todos ellos, por el teorema de Wilson (teorema 9) obtenemos que

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

En el caso en que a sí sea un residuo cuadrático, habrá exactamente dos enteros distintos en $\{1, \dots, p-1\}$ que sean solución de la ecuación $x^2 \equiv a \pmod{p}$. Esto es así debido a que, tal y como vimos en la demostración del teorema 6, ningún par de números en $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ pueden ser congruentes entre sí módulo p y, a su vez, estos números son congruentes respectivamente con $(p-1)^2, (p-2)^2, \dots, \left(\frac{p+1}{2}\right)^2$ módulo p. Luego existe una solución (y solo una) en el conjunto $\left\{1, \dots, \frac{p-1}{2}\right\}$, a la cual denotaremos por $\sqrt{a}$ y, por tanto, la otra solución será $p - \sqrt{a}$.

Tendremos así $\frac{p-3}{2}$ pares formados por elementos distintos y dos pares que son $(\sqrt{a}, \sqrt{a})$ y $(p-\sqrt{a}, p-\sqrt{a})$. Multiplicamos ahora todos los elementos de todos los pares para obtener que

$$a^{\frac{p+1}{2}} \equiv (p-1)! \cdot \sqrt{a} \cdot (p-\sqrt{a}) \equiv (-1) \cdot (-a) \equiv a \pmod{p},$$

y multiplicando en ambos lados por a^{-1} obtenemos que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$ ∎

Observación 11. Con el criterio de Euler podemos demostrar el teorema 8 de forma más directa teniendo en cuenta que

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$$

y que, por tanto, ab es residuo cuadrático si y solo si $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ si y solo si, o bien

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ y } b^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

o bien

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \text{ y } b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Definición 12 (símbolo de Legendre). Para cada número primo impar p y cada entero n coprimo con p, definimos el símbolo de Legendre de n respecto de p como

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{si } n \text{ es un residuo cuadrático módulo } p, \\ -1 & \text{si } n \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Con esta notación, el teorema 8 podría resumirse diciendo que el símbolo de Legendre es multiplicativo, *i.e.*,

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

El siguiente corolario será necesario cuando caractericemos qué números primos pueden expresarse como suma de dos números cuadrados (teorema 20).

Corolario 13. *Si p es un primo impar, entonces*

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

Demostración. En efecto, por el criterio de Euler $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ y ahora basta con tener en cuenta que $\frac{p-1}{2}$ es par si $p \equiv 1 \pmod{4}$ e impar si $p \equiv 3 \pmod{4}$. ∎

El siguiente lema técnico será clave para demostrar el resultado fundamental del trabajo.

Lema 14 (lema de Gauss). *Sean p un primo impar y n un entero coprimo con p. Definimos los conjuntos*

$$S := \left\{n, 2n, \dots, \frac{p-1}{2}n\right\}$$

y S' como los representantes de las clases de equivalencia de los elementos de S en $\mathbb{Z}_p$.

Si denotamos por k el número de elementos de S' que son mayores que $\frac{p}{2}$ entonces

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

Demostración. Primero observamos que en S no hay ningún múltiplo de p y que en S' no hay ningún par de elementos congruentes entre sí módulo p. Pues, si $nx \equiv ny \pmod{p}$, multiplicamos en ambos lados por el inverso de n en $\mathbb{Z}_p$ y obtenemos que $x \equiv y \pmod{p}$, lo cual, siendo $1 \leq x, y \leq \frac{p-1}{2}$, solo es posible si $x = y$. Por tanto, en S' hay exactamente $\frac{p-1}{2}$ elementos.

Si denotamos por $r_1, \dots, r_l$ a los elementos de S' menores que $\frac{p}{2}$ y por $s_1, \dots, s_k$ a los mayores que $\frac{p}{2}$, se tiene que

$$\left\{1, 2, \dots, \frac{p-1}{2}\right\} = \{r_1, \dots, r_l, p - s_1, \dots, p - s_k\}.$$

Para probar la anterior igualdad, observamos que $1 \leq r_i,\ p - s_j \leq \frac{p-1}{2}$ y que, por tanto, basta con comprobar que todos ellos son incongruentes entre sí. Ya hemos visto que si $i \neq j$, r_i no puede ser congruente con r_j. Análogamente, s_i no puede ser congruente con s_j y, por tanto, $p - s_i$ no puede ser congruente con $p - s_j$. Si existieran elementos tales que $r_i \equiv p - s_j \pmod{p}$, llegaríamos a que p divide a un número de la forma $n(x + y)$ con $1 \leq x, y \leq \frac{p-1}{2}$, lo cual es imposible.

Ahora, si multiplicamos todos los elementos de cada conjunto llegamos a que

$$\left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{l} r_i \prod_{j=1}^{k} (p - s_j) \equiv (-1)^k \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \pmod{p}.$$

Por otro lado, como los elementos de S son congruentes uno a uno con los de S', multiplicándolos todos entre sí obtenemos que

$$n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \pmod{p}.$$

Juntándolo todo y multiplicando por el inverso de $\left(\frac{p-1}{2}\right)!$ (el cual existe por ser coprimo con p) concluimos que

$$n^{\frac{p-1}{2}} (-1)^k \equiv 1 \pmod{p}$$

o, equivalentemente,

$$n^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}.$$

El resultado se sigue ahora de aplicar el criterio de Euler (véase teorema 10). ∎

Veamos en el siguiente corolario cómo el lema de Gauss proporciona una manera más rápida de determinar cuándo $n = 2$ es un residuo cuadrático módulo un número primo.

Corolario 15. *Si p es un primo impar entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Demostración. Usaremos el lema de Gauss y para ello bastará con estudiar la paridad del conjunto de números mayores que $\frac{p}{2}$ entre el conjunto $\{2, 4, \dots, p-1\}$. Como hay $\left[\frac{p}{4}\right]$ números pares menores que $\frac{p}{2}$ (siendo $\left[\frac{p}{4}\right]$ la parte entera de $\frac{p}{4}$, *i.e.*, el cociente de la división entera de p entre 4), habrá $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ mayores.

Distinguiremos 4 casos posibles:

1. Si $p \equiv 1 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n - 2n$ para algún entero n. Por tanto, k será par.
2. Si $p \equiv 3 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 1 - 2n$ para algún entero n. Por tanto, k será impar.
3. Si $p \equiv 5 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 2 - (2n + 1)$ para algún entero n. Por tanto, k será impar.
4. Si $p \equiv 7 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 3 - (2n + 1)$ para algún entero n. Por tanto, k será par.

Todo esto lo expresamos de una forma más compacta diciendo que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

pues $\frac{p^2-1}{8}$ es par si $p \equiv 1, 7 \pmod 8$ y es impar si $p \equiv 3, 5 \pmod 8$. ∎

Ejemplo 16. Comprobemos si 2 es un residuo cuadrático para ciertos números primos usando el lema de Gauss y el criterio de Euler, respectivamente, y veamos cómo llegamos al mismo resultado.

```
gap> IsPrime(41);
    true
gap> 41 mod 8;
    1
gap> 2^20 mod 41;
    1
```

Como $\frac{p^2-1}{8}$ es par si $p \equiv 1 \pmod 8$, el lema de Gauss indica que 2 es residuo cuadrático módulo 41; concluimos lo mismo aplicando el criterio de Euler.

```
gap> IsPrime(101);
    true
gap> 101 mod 8;
    5
gap> 2^50 mod 101;
    100
```

Puesto que $\frac{p^2-1}{8}$ es impar si $p \equiv 5 \pmod 8$, el lema de Gauss indica que 2 no es residuo cuadrático módulo 101. Observamos que deducimos lo mismo con el criterio de Euler, pero el lema de Gauss es computacionalmente más eficiente en este caso.

Ejemplo 17. Antes de probar el resultado principal, veamos otros ejemplos con GAP en los cuales comprobamos si ciertos números primos son residuos cuadráticos módulo otros números primos dados mediante el criterio de Euler. Observamos qué relación hay entre $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$ según la naturaleza de los primos p y q.

```
gap> IsPrime(911);
    true
gap> 911 mod 4;
    3
gap> IsPrime(919);
    true
gap> 919 mod 4;
    3
gap> IsPrime(929);
    true
gap> 929 mod 4;
    1
gap> IsPrime(937);
    true
gap> 937 mod 4;
    1
gap> 911^459 mod 919;
    918
gap> 919^455 mod 911;
    1
```

Observamos que 911 no es residuo cuadrático módulo 919, pero 919 sí que es residuo cuadrático módulo 911.

```
gap> 929^455 mod 911;
    1
gap> 911^464 mod 929;
    1
```

En este caso tenemos que 929 es residuo cuadrático módulo 911 y también 911 es residuo cuadrático módulo 929.

```
gap> 929^459 mod 919;
    1
gap> 919^464 mod 929;
    1
```

Otra vez tenemos que 929 es residuo cuadrático módulo 919 y también 919 es residuo cuadrático módulo 929.

Vayamos pues con el teorema fundamental de este trabajo:

Teorema 18 (ley de reciprocidad cuadrática). *Si p y q son números primos impares distintos se tiene que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Primero vamos a probar que si n es un número impar coprimo con p entonces

$$\left(\frac{n}{p}\right) = (-1)^{\rho_{n,p}},$$

donde $\rho_{n,p} := \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right]$. Definimos S' como en el lema 14 y volvemos a denotar por $r_1, \dots, r_l$ los elementos de S' menores que $\frac{p}{2}$ y por $s_1, \dots, s_k$ los mayores que $\frac{p}{2}$. Para cada $1 \leq j \leq \frac{p-1}{2}$ está claro que $jn = \left[\frac{jn}{p}\right]p + t$ para cierto $t \in S'$ que, además, es único (como deducimos en el primer párrafo de la demostración del lema 14) y, por tanto,

$$\sum_{j=1}^{\frac{p-1}{2}} jn = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right]p + \sum_{j=1}^{l} r_j + \sum_{j=1}^{k} s_j.$$

Por otra parte, como ya probamos en el lema 14, se tiene que

$$\left\{1, 2, \dots, \frac{p-1}{2}\right\} = \{r_1, \dots, r_l, p - s_1, \dots, p - s_k\},$$

por lo que,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{l} r_j + \sum_{j=1}^{k} (p - s_j) = \sum_{j=1}^{l} r_j + kp - \sum_{j=1}^{k} s_j$$

y, restando estas dos expresiones, obtenemos que

$$(n-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right] - k\right) + 2\left(\sum_{j=1}^{k} s_j\right) = p(\rho_{n,p} - k) + 2\left(\sum_{j=1}^{k} s_j\right).$$

Observamos que k y $\rho_{n,p}$ tienen que tener la misma paridad pues, al ser n impar, la expresión de la izquierda es par y, por ser p un primo impar, $p(\rho_{n,p} - k)$ es par si y solo si k y $\rho_{n,p}$ tienen la misma paridad. Por tanto, por el lema de Gauss (véase lema 14), tenemos que $\left(\frac{n}{p}\right) = (-1)^k = (-1)^{\rho_{n,p}}$.

Supongamos sin pérdida de generalidad que $q < p$ y calculemos el valor $\rho_{q,p}$. Para $j = 1$ tenemos que $\left[\frac{jq}{p}\right] = 0$, y para $j = \frac{p-1}{2}$ tenemos que

$$\left[\frac{\frac{p-1}{2}q}{p}\right] = \left[\frac{\frac{q-1}{2}p + \frac{p-q}{2}}{p}\right] = \left[\frac{q-1}{2} + \frac{1}{2}\left(1 - \frac{q}{p}\right)\right] = \frac{q-1}{2},$$

pues $\frac{q}{p} < 1$. Por tanto, todos los sumandos toman valores de forma creciente entre 0 y $\frac{q-1}{2}$. Puesto que $p > q$ y ambos son impares, tenemos que $\frac{p-1}{2} \geq \frac{q+1}{2}$ y, como los términos $\frac{jq}{p}$ están igualmente espaciados, para cada n tal que $0 \leq n \leq \frac{q-1}{2}$ habrá algún sumando que tome dicho valor. Para calcular $\rho_{q,p}$ solo nos hará falta ver cuántos sumandos hay que tomen el mismo valor para cada n. Para ver esto, si consideramos dos sumandos consecutivos de forma que $\left[\frac{jq}{p}\right] = n-1$ y $\left[\frac{(j+1)q}{p}\right] = n$ se tiene que $\frac{jq}{p} < n < \frac{(j+1)q}{p}$, por lo que $j < \frac{np}{q} < j+1$ y, así, $\left[\frac{np}{q}\right] = j$.

Por tanto, el número exacto de sumandos en $\rho_{q,p}$ que toman valores estrictamente menores que n será $\left[\frac{np}{q}\right]$, de lo cual se deduce que el número de sumandos en $\rho_{q,p}$ que toman el valor n es exactamente $\left[\frac{(n+1)p}{q}\right] - \left[\frac{np}{q}\right]$. Así,

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] &= 1\left(\left[\frac{2p}{q}\right] - \left[\frac{p}{q}\right]\right) + 2\left(\left[\frac{3p}{q}\right] - \left[\frac{2p}{q}\right]\right) + \cdots + \frac{q-1}{2}\left(\frac{p-1}{2} - \left[\frac{\frac{q-1}{2}p}{q}\right]\right) \\ &= -\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] + \frac{(p-1)(q-1)}{4}\end{aligned}$$

y obtenemos $\rho_{q,p} + \rho_{p,q} = \frac{(p-1)(q-1)}{4}$. Finalmente, concluimos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\rho_{q,p}}(-1)^{\rho_{p,q}} = (-1)^{\rho_{q,p}+\rho_{p,q}} = (-1)^{\frac{(p-1)(q-1)}{4}},$$

como queríamos probar. ∎

Otra forma equivalente de expresar el anterior teorema es la siguiente:

Teorema 18.b. *Sean p y q dos números primos impares distintos entre sí. Entonces:*

1. *Si bien $p \equiv 1 \pmod 4$ o $q \equiv 1 \pmod 4$, entonces q es un residuo cuadrático módulo p si y solo si p es un residuo cuadrático módulo q.*
2. *Si $p \equiv 3 \pmod 4$ y también $q \equiv 3 \pmod 4$, entonces q es un residuo cuadrático módulo p si y solo si $-p$ es un residuo cuadrático módulo q.*

El criterio de Euler es excelente a nivel teórico, pero computacionalmente no es muy óptimo ya que para determinar si un número es un residuo cuadrático módulo un número primo que sea «grande» tenemos que calcular potencias de un orden muy alto.

Por ejemplo, para determinar si 19 es un residuo cuadrático módulo 859 tendríamos que calcular el valor de $19^{429} \pmod{859}$. Sin embargo, con la ley de reciprocidad cuadrática, puesto que tanto 19 como 859 son congruentes con 3 módulo 4, podríamos determinar si 19 es un residuo cuadrático módulo 859 de forma mucho más sencilla; basta con ver si 859 es un residuo cuadrático módulo 19 y, como se cumple $859 \equiv 4 \equiv 2^2 \pmod{19}$, podemos afirmar que 19 no es residuo cuadrático módulo 859.

Ejemplo 19. Veamos en este ejemplo cómo usando la ley de reciprocidad cuadrática podemos evitar ciertos cálculos para determinar si un número primo es un residuo cuadrático módulo otro número primo.

```
gap> IsPrime(881);
    true
gap> IsPrime(877);
    true
gap> 877 mod 4;
    1
gap> 877^440 mod 881;
    1
```

Según la ley de reciprocidad cuadrática, en este caso debe darse que 881 es un residuo cuadrático módulo 877. Lo comprobamos con el criterio de Euler y

```
gap> 881^438 mod 877;
    1
```

como queríamos probar.

3. Aplicaciones

Veamos algunas aplicaciones de la ley de reciprocidad cuadrática y los resultados sobre residuos cuadráticos que hemos desarrollado a lo largo del trabajo en teoría de números.

3.1. Enteros que son suma de dos cuadrados

Ya hacia el año 250 d.C. se hace referencia en la *Arithmetica* de Diofanto al problema de determinar si un número dado se puede descomponer como suma de dos cuadrados. Vamos a dar una caracterización completa de los enteros positivos que tienen esta propiedad de descomposición utilizando resultados sobre residuos cuadráticos. Para una prueba distinta basada en las propiedades del anillo de los enteros de Gauss véase el libro *Introducción al Álgebra* [3].

Comenzamos observando que el conjunto de enteros que son suma de dos cuadrados es cerrado por multiplicación, esto es, dados dos números cada uno de los cuales es suma de dos cuadrados, su producto también podrá ser expresado como suma de dos cuadrados, como muestra la siguiente fórmula:

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

para cualesquiera enteros a, b, c y d.

Parece lógico pues comenzar caracterizando los números primos que pueden escribirse como suma de dos cuadrados y, como trivialmente $2 = 1^2 + 1^2$, nos centramos en los primos impares.

Teorema 20. *Si p es un primo impar, entonces p es suma de dos cuadrados si y solo si $p \equiv 1 \pmod 4$.*

Demostración. Dado un número entero, su cuadrado siempre es congruente con 0 o 1 módulo 4 (de comprobación inmediata) y, por tanto, si un entero es suma de dos cuadrados, será congruente con 0, 1 o 2 módulo 4. Ahora, si p es un primo impar, entonces no puede ser congruente con 0 ni 2 módulo 4 (pues si no sería par) y, por tanto, si p es un primo impar que es además suma de dos cuadrados, necesariamente debe ser $p \equiv 1 \pmod 4$.

Supongamos ahora que $p \equiv 1 \pmod 4$. Por el corolario 13 tenemos que $\left(\frac{-1}{p}\right) = 1$ y, por tanto, existe un entero $u \in \mathbb{Z}$ tal que $u^2 \equiv -1 \pmod p$. Consideremos el conjunto de enteros de la forma $x + uy$ tales que $x, y \in \mathbb{Z}$ y $0 \leq x, y < \sqrt{p}$. Como hay $([\sqrt{p}]+1)^2 > p$ posibles pares (x, y) distintos en estas condiciones, por el principio del palomar (también llamado principio del casillero), necesariamente debe haber $(x_1, y_1) \neq (x_2, y_2)$ tales que

$$x_1 + uy_1 \equiv x_2 + uy_2 \pmod p,$$

lo cual equivale a que

$$x_1 - x_2 \equiv u(y_2 - y_1) \pmod p.$$

Definimos $a \coloneqq x_1 - x_2$ y $b \coloneqq y_2 - y_1$. Se tiene que $|a| < \sqrt{p}$, $|b| < \sqrt{p}$ y $a \equiv ub \pmod p$. Por tanto, teniendo en cuenta que $u^2 + 1 \equiv 0 \pmod p$ y operando, obtenemos

$$a^2 + b^2 \equiv (u^2+1)b^2 \equiv 0 \pmod p.$$

Finalmente, nos damos cuenta de que, por un lado $a^2 + b^2 < 2p$ y, por otro, al ser $(x_1, y_1) \neq (x_2, y_2)$, debe ser $0 < a^2 + b^2$ y solo queda una posibilidad:

$$a^2 + b^2 = p.$$ ∎

Recordamos que, como consecuencia del teorema fundamental de la aritmética, todo entero positivo se puede escribir como producto de un número cuadrado y un entero libre de cuadrados. En efecto, si $n = \prod_{i=1}^{k} p_i^{e_i}$ es la factorización de n como producto de primos y reordenamos los primos p_i de forma que los l primeros estén elevados a una potencia impar y los demás estén elevados a una potencia par, y si escribimos $e_i = 2f_i + 1$ para $1 \leq i \leq l$ y $e_i = 2f_i$ para $l+1 \leq i \leq k$, tendremos que

$$n = \prod_{i=1}^{l} p_i^{2f_i+1} \prod_{i=l+1}^{k} p_i^{2f_i} = \prod_{i=1}^{l} p_i \prod_{i=1}^{k} p_i^{2f_i} = n_1 n_2^2,$$

siendo $n_1 \coloneqq \prod_{i=1}^{l} p_i$ y $n_2 \coloneqq \prod_{i=1}^{k} p_i^{f_i}$.

Teorema 21. *Sea n un entero positivo, que se escribe como $n = n_1 n_2^2$ con n_1 libre de cuadrados (lo cual queda justificado por el párrafo anterior). Entonces n es suma de dos cuadrados si y solo si n_1 no tiene ningún factor primo de la forma $p \equiv 3 \pmod 4$.*

Demostración. Supongamos que n es suma de dos cuadrados y probemos que si cierto número primo p divisor de n es de la forma $p \equiv 3 \pmod 4$, entonces la máxima potencia de p que divide a n es par, lo cual implica que p no será factor de n_1.

Primero, tenemos que si un número primo de la forma $p \equiv 3 \pmod 4$ es tal que $p \mid n = a^2 + b^2$ entonces $p \mid a$ y $p \mid b$. Pues si p no dividiese a b, por ejemplo, b sería coprimo con p y, por ser p primo, existiría el inverso de b en $\mathbb{Z}_p$. Entonces, como $a^2 + b^2 \equiv 0 \pmod p$, esto implica que

$$(ab^{-1})^2 + 1 \equiv 0 \pmod p,$$

es decir, $\left(\frac{-1}{p}\right) = 1$, lo cual contradice el corolario 13.

Por tanto, si p^{e_1} y p^{e_2} son las máximas potencias de p que dividen a a y b respectivamente, tendremos que $e := \min\{e_1, e_2\} \geq 1$, luego $a = p^e a_1$ y $b = p^e b_1$ para ciertos enteros a_1 y b_1, al menos uno de los cuales no es divisible por p. Entonces $n = a^2 + b^2 = p^{2e}a_1^2 + p^{2e}b_1^2 = p^{2e}(a_1^2 + b_1^2)$ y, además, no puede ser que $p^{2e+1} \mid n$, pues entonces $p \mid (a_1^2 + b_1^2)$ y, por la primera parte, tendríamos que $p \mid a_1$ y $p \mid b_1$, lo cual es una contradicción.

Supongamos ahora que n es tal que n_1 no contiene ningún factor primo de la forma $p \equiv 3 \pmod 4$ y veamos que n es suma de dos cuadrados. Por el teorema 20 cada factor primo de n_1 es suma de dos cuadrados y, como vimos al principio de la sección, el producto de dos números que son suma de dos cuadrados es también suma de dos cuadrados. Podemos por tanto asegurar que existen $a, b \in \mathbb{N}$ tales que $a^2 + b^2 = n_1$ y, multiplicando a ambos lados por n_2^2, tendremos que

$$n = n_1 n_2^2 = (a^2 + b^2)n_2^2 = (an_2)^2 + (bn_2)^2.$$ ∎

Ejemplo 22. Veamos, usando GAP, cómo determinar si los enteros 123 456 789 y 987 654 321 son suma de dos cuadrados.

```
gap> PrintFactorsInt(123456789);
    3^2*3607*3803
gap> 3607 mod 4;
    3
```

Vemos que, como el entero libre de cuadrados de 123 456 789 contiene el número primo 3607 de la forma $p \equiv 3 \pmod 4$, este no puede expresarse como suma de dos cuadrados.

```
gap> PrintFactorsInt(987654321);
    3^2*17^2*379721
gap> 379721 mod 4;
    1
```

Puesto que el único primo que divide a 987 654 321 con exponente un número impar es 379 721 y este es de la forma $p \equiv 1 \pmod 4$, se puede expresar como suma de dos cuadrados.

3.2. Ecuaciones en congruencias de segundo grado

Dada una ecuación en congruencia lineal del tipo $ax + b \equiv 0 \pmod m$, es muy sencillo determinar cuándo tiene solución. Sin embargo, la situación se vuelve más compleja cuando estudiamos la ecuación

$$ax^2 + bx + c \equiv 0 \pmod m.$$

Para determinar si esta ecuación tiene o no solución, primero la transformamos en una ecuación más sencilla de la siguiente forma:

$$\begin{aligned} ax^2 + bx + c \equiv 0 \pmod m &\iff 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}, \\ &\iff (2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}. \end{aligned}$$

Por tanto, considerando la ecuación

$$y^2 \equiv b^2 - 4ac \pmod{4am},$$

el problema de determinar si una ecuación de segundo grado tiene solución queda reducido al problema de determinar si un número es un residuo cuadrático módulo un número compuesto y, en caso de tener que cierto y es una solución, resolver la ecuación lineal

$$2ax + b \equiv y \pmod{4am}.$$

Por tanto, nos planteamos el problema de determinar cuándo un número dado es un residuo cuadrático módulo un número compuesto, teniendo en cuenta que las herramientas de la sección anterior nos permiten abordar el problema de forma eficiente cuando tratamos con un número primo como módulo.

El siguiente teorema, junto al teorema fundamental de la aritmética, reducen el problema a considerar únicamente potencias de números primos como módulos.

Teorema 23. *Sean m y n enteros coprimos y sea a coprimo tanto con m como con n. Entonces, a es un residuo cuadrático módulo mn si y solo si a es un residuo cuadrático módulo m y también es un residuo cuadrático módulo n.*

Demostración. Si existe x tal que $x^2 \equiv a \pmod{mn}$, en particular se tiene que $x^2 \equiv a \pmod{m}$ y también $x^2 \equiv a \pmod{n}$.

Recíprocamente, supongamos que existen enteros r y s tales que

$$\begin{cases} r^2 \equiv a \pmod{m}, \\ s^2 \equiv a \pmod{n}. \end{cases}$$

Como m y n son coprimos, el teorema chino del resto nos asegura que el sistema

$$\begin{cases} x \equiv r \pmod{m}, \\ x \equiv s \pmod{n}, \end{cases}$$

tiene una solución t que, además, es única módulo mn. Por tanto, obtenemos que $t^2 \equiv r^2 \equiv a \pmod{m}$ y $t^2 \equiv s^2 \equiv a \pmod{n}$, lo cual implica que tanto m como n dividen a $t^2 - a$ y, por ser estos coprimos, mn divide a $t^2 - a$, *i.e.*, $t^2 \equiv a \pmod{mn}$. ∎

Distinguimos ahora cuando el módulo es una potencia de un número primo par e impar. Cuando tratamos con número primos impares, el siguiente lema generaliza el teorema 6.

Lema 24. *Si p es un primo impar y n un entero positivo, entonces exactamente la mitad de los elementos de $\{1, 2, \dots, (p^n - 1)\}$ que sean coprimos con p son residuos cuadráticos módulo p^n.*

Demostración. Si existieran dos enteros x, y coprimos con p tales que $1 \leq x < y \leq \frac{p^n-1}{2}$ y, además, $y^2 \equiv x^2 \pmod{p^n}$, entonces $p^n \mid (y - x)(y + x)$. Pero, como $y + x < p^n$, tiene que existir algún $k \geq 1$ tal que $p^k \mid y - x$ y, en particular, $y = x + mp$ para cierto entero no nulo m. Por otro lado, como también $y - x < p^n$, tendremos que $k < n$ y, por tanto, $p \mid y + x = 2x + mp$. Pero entonces tendríamos que $p \mid x$, y esto contradice la hipótesis de que x sea coprimo con p.

Por tanto, al menos la mitad de los enteros coprimos con p son residuos cuadráticos módulo p^n pero, como para cada $1 \leq r \leq \frac{p^n-1}{2}$ se tiene $r^2 \equiv (p^n - r)^2 \pmod{p^n}$, y r es coprimo con p si y solo si $(p^n - r)$ es coprimo con p, se sigue el resultado. ∎

Proposición 25. *Sean p un primo impar y a un entero coprimo con p. Dado un entero positivo n, se tiene que a es un residuo cuadrático módulo p si y solo si a es un residuo cuadrático módulo p^n.*

Demostración. Está claro que si a es un residuo cuadrático módulo p^n entonces también es un residuo cuadrático módulo p.

Recíprocamente, tenemos, por el lema 24, que en el conjunto

$$\{1, 2, \dots, p - 1, p + 1, p + 2, \dots, 2p - 1, 2p + 1, 2p + 2, \dots, p^n - 1\}$$

la mitad de los elementos son residuos cuadráticos módulo p^n, mientras que el resto son residuos no cuadráticos. Además, todos esos residuos cuadráticos módulo p^n lo son también módulo p, luego bastará con probar que en dicho conjunto también son residuos cuadráticos módulo p exactamente la mitad de sus elementos. Por el teorema 6 tenemos que exactamente la mitad de los elementos de $\{1, 2, \dots, (p-1)\}$ son residuos cuadráticos módulo p y, por tanto, también lo son la mitad de cada uno de los conjuntos $\{pk+1, pk+2, \dots, pk+(p-1)\}$ para $0 \leq k \leq p^{n-1}-1$. Luego tendremos que exactamente la mitad de los elementos de

$$\{1, 2, \dots, p-1, p+1, p+2, \dots, 2p-1, 2p+1, 2p+2, \dots, p^n-1\}$$

son residuos cuadráticos módulo p. ∎

Cuando tratamos con potencias de 2 como módulo, tenemos que, trivialmente, todos los enteros impares son residuos cuadráticos módulo 2, y se comprueba fácilmente que los únicos enteros impares que son residuos cuadráticos módulo 4 con aquellos congruentes con 1 módulo 4. De forma más general, tenemos el siguiente resultado.

Proposición 26. *Sean $n \geq 3$ y a un entero impar. Entonces a es un residuo cuadrático módulo 2^n si y solo si $a \equiv 1 \pmod 8$.*

Demostración. Para $n = 3$, puesto que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, se tiene que solo los enteros congruentes con 1 módulo 8 serán residuos cuadráticos.

Veamos que, para cada $n \geq 3$ y cada entero impar a, se tiene que a es un residuo cuadrático módulo 2^n si y solo si lo es módulo 2^{n+1}, de donde se deducirá (junto con el caso que acabamos de probar) el resultado general por inducción.

Está claro que si a es un residuo cuadrático módulo 2^{n+1} también lo será módulo 2^n.

Recíprocamente, si existiera un r tal que $r^2 \equiv a \pmod{2^n}$, necesariamente r tendría que ser impar y, además, existiría un entero no nulo t tal que $a = r^2 + t2^n$. Entonces, $s \coloneqq r + t2^{n-1}$ cumple que

$$s^2 = x^2 + xt2^n + t^2 2^{2n-2} = a - t2^n + xt2^n + t^2 2^{2n-2} = a + 2^n(x-1)t + t^2 2^{2n-2},$$

y, como x tiene que ser impar, será $s^2 \equiv a \pmod{2^{n+1}}$. ∎

Para más información véase, por ejemplo, *An introduction to the theory of numbers* de Niven, Zuckerman y Montgomery [8].

3.3. Números Primos

En esta sección vamos a ver cómo, usando la ley de reciprocidad cuadrática, podemos demostrar la existencia de infinitos números primos congruentes con 4 módulo 5. Comenzamos recordando este clásico teorema debido a Euclides.

Teorema 27 (Euclides). *Existen infinitos números primos.*

Demostración. Supongamos que solo hay un conjunto finito de números primos $\{p_1, \dots, p_n\}$. Consideremos $p \coloneqq p_1 p_2 \cdots p_n + 1$. Tenemos que p no es divisible por p_i para ningún p_i pues, de lo contrario, $p_i \mid (p - p_1 p_2 \cdots p_n) = 1$. Por tanto, p es un entero mayor estricto que p_i para $1 \leq i \leq n$ que no es divisible por ningún número distinto de sí mismo y de 1, lo cual equivale a decir que p es un número primo tal que $p \notin \{p_1, \dots, p_n\}$ y esto supone una contradicción. ∎

La siguiente proposición generaliza el teorema de Euclides:

Proposición 28. *Sea $f \in \mathbb{Z}[x]$ un polinomio no constante y*

$$P_f \coloneqq \{p \mid \ p \text{ es primo y } p \mid f(n) \text{ para algún } n \in \mathbb{N}\}.$$

Entonces P_f contiene infinitos números primos.

Demostración. Si $f(0) = 0$ entonces f no tiene término independiente y para cada primo p se tiene que $p \mid f(p)$.

Supongamos pues que $f(0) \neq 0$. Entonces $f(x) = f(0) + a_1 x + \cdots + a_n x^n$ y si solo hubiera una cantidad finita $P_f = \{p_1, \dots, p_m\}$, tendríamos que para cualquier entero k, si $Q \coloneqq p_1 \cdots p_m$,

$$l_k \coloneqq \frac{1}{f(0)} f\big(kf(0)Q\big) = 1 + a_1 kQ + a_2 k^2 Q^2 f(0) + \cdots + a_n k^n Q^n f(0)^{n-1} = 1 + rQ$$

para cierto $r \in \mathbb{Z}$. Está claro que l_k no es divisible por ningún p_i, y que si consideramos k lo suficientemente grande tendrá que ser $|l_k| > 1$. Luego l_k será divisible por algún número primo p_{m+1} distinto de p_i para $1 \leq i \leq m$, lo cual es una contradicción. ∎

Como consecuencia de esta proposición, si consideramos un número primo p y el polinomio $f(x) = x^2 - p$, tendremos que existen infinitos números primos q tales que $q \mid n^2 - p$ para algún $n \in \mathbb{N}$; es decir, existen infinitos números primos q para los cuales p es un residuo cuadrático.

Vamos ahora con el teorema principal de esta sección:

Teorema 29. *Existen infinitos números primos de la forma* $p \equiv 4 \pmod 5$.

Demostración. Si definimos $f(x) = 5x^2 - 1 \in \mathbb{Z}[x]$, tenemos por la proposición 28 que existen infinitos números primos que dividen a algún número de la forma $5n^2 - 1$ con $n \in \mathbb{N}$. Si p es un primo impar tal que $p \mid 5n^2 - 1$, observamos primero que, necesariamente, $p \neq 5$ y, además, $1^2 \equiv 1 \equiv 5n^2 \pmod p$. Por tanto, $5n^2$ es un residuo cuadrático módulo p, es decir, $\left(\frac{5n^2}{p}\right) = 1$. Como, obviamente, $\left(\frac{n^2}{p}\right) = 1$, por el teorema 8 tenemos que $\left(\frac{5}{p}\right) = 1$ y, como consecuencia de la ley de reciprocidad cuadrática, $\left(\frac{p}{5}\right) = 1$. Por tanto, existe un entero $u \in \mathbb{Z}$ tal que $u^2 \equiv p \pmod 5$ y, como los números cuadrados no divisibles por 5 son congruentes, o bien a 1, o bien a 4 módulo 5, $p \equiv 1$ o $4 \pmod 5$. Para terminar la prueba solo falta comprobar que no puede haber solo una cantidad finita tal que $p \equiv 4 \pmod 5$.

Supongamos que hay una cantidad finita $\{p_1, \dots, p_m\}$ de primos tales que $p \equiv 4 \pmod 5$ y consideremos $n \coloneqq 2p_1 \cdots p_m$. Entonces, puesto que $5n^2 - 1$ es impar, se deduce de la primera parte de la demostración que cualquier divisor primo suyo será congruente con 1 o 4 módulo 5 y, como $5n^2 - 1$ es coprimo con p_i para $1 \leq i \leq m$, todos sus divisores primos tienen que ser congruentes con 1 módulo 5. Pero esto es imposible porque, en ese caso, tendría que ser $5n^2 - 1 \equiv 1 \pmod 5$ y, por tanto, llegaríamos a que $0 \equiv 2 \pmod 5$, lo cual no es posible. Así quedaría probado que tiene que haber algún divisor q de $5n^2 - 1$ congruente con 4 módulo 5 y distinto de p_i para $i = 1, \dots, m$, lo cual es una contradicción. ∎

Teniendo en cuenta que todos los primos de la forma $p \equiv 4 \pmod 5$ tienen por último dígito 9, este teorema equivale al enunciado más «visual» que afirma que existen infinitos números primos cuyo último dígito es 9.

Antes de terminar la sección, cabría comentar que este es un caso particular del teorema de Dirichlet de progresiones aritméticas, el cual afirma que, dados dos enteros positivos y coprimos $a, d \in \mathbb{N}$, existen infinitos números naturales $n \in \mathbb{N}$ para los cuales $a + nd$ es primo. La demostración del teorema de Dirichlet queda fuera de nuestro alcance, pero muchos casos particulares pueden demostrarse gracias a la ley de reciprocidad cuadrática imitando la demostración del teorema 29. Para más información sobre el teorema de Dirichlet, véase *Introduction to analytic number theory* de Apostol [1].

3.4. Soluciones enteras de ecuaciones elípticas

Recordamos que una curva elíptica sobre un cuerpo de característica distinta de 2 y de 3 es (en su forma simplificada) el conjunto de soluciones de la ecuación

$$y^2 = x^3 + ax + b$$

siendo a y b elementos de dicho cuerpo (*i.e.*, la curva algebraica definida por dicha ecuación).

Una cuestión interesante sobre las curvas elípticas con coeficientes racionales (u otro cuerpo de característica 0) consiste en determinar si tiene soluciones (x, y) formadas por números enteros y, en caso de

tenerlas, determinar cuántas pueden haber. Sin ahondar demasiado en este asunto, mencionamos que el matemático C. L. Siegel probó que, sobre el cuerpo de los números racionales, el conjunto de soluciones formadas por números enteros de una curva elíptica dada tiene que ser finito [9].

Damos a continuación un ejemplo ilustrativo de cómo puede usarse la ley de reciprocidad cuadrática para determinar si una curva no tiene soluciones enteras.

Proposición 30. *La ecuación elíptica $y^2 + 3 = x^3 - x$ no tiene soluciones enteras.*

Demostración. Supongamos que (x, y) es una solución con $x, y \in \mathbb{Z}$. Puesto que $x^3 - x$ es siempre par, $y^2 + 3$ tiene que ser par y, por tanto, y tiene que ser impar. Supongamos que $y = 2k + 1$ para cierto $k \in \mathbb{Z}$. Entonces, $y^2 + 3 = (4k^2 + 4k + 1) + 3 = 4(k^2 + k + 1)$ y, puesto que $k^2 + k$ siempre es par, deducimos que $4 \mid y^2 + 3$ pero $8 \nmid y^2 + 3$.

Si x fuera impar, $x^2 - 1$ sería divisible por 8 y, por tanto, $8 \mid x(x^2 - 1) = y^2 + 3$. Pero acabamos de ver que esto no es posible, luego x tiene que ser par.

Si x es par, tanto $x - 1$ como $x + 1$ son impares y, puesto que $y^2 + 3 = (x - 1)x(x + 1)$, deducimos que $4 \mid x$ pero $8 \nmid x$.

Como $x - 1, x, x + 1$ son tres enteros consecutivos, uno de ellos tiene que ser congruente con 2 módulo 3. Puesto que $(x - 1)x(x + 1) = 4(x - 1)\frac{x}{4}(x + 1)$ y, además, por ser x múltiplo de 4 es $x \equiv \frac{x}{4} \pmod 3$, tendrá que darse que $(x - 1)$, $\frac{x}{4}$ o $(x + 1)$ sea congruente con 2 módulo 3. Aquel que sea congruente con 2 módulo 3 tendrá que tener como factor algún primo congruente con 2 módulo 3 y, puesto que $(x - 1)$, $\frac{x}{4}$ y $(x + 1)$ son todos impares, ese primo p también tendrá que ser impar.

Hemos probado pues que existe un primo impar $p \equiv 2 \pmod 3$ tal que $p \mid y^2 + 3$, lo cual equivale a afirmar que $\left(\frac{-3}{p}\right) = 1$. Por la ley de reciprocidad cuadrática y el criterio de Euler, tenemos que

$$\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}}(-1)^{\frac{(p-1)}{2}} = 1,$$

luego existe un $u \in \mathbb{Z}$ tal que $u^2 \equiv p \pmod 3$. Pero como, para cualquier entero u, $u^2 \equiv 0$ o $1 \pmod 3$, esto implicaría que $p \equiv 0$ o $1 \pmod 3$, lo cual es una contradicción. ∎

4. Generalizaciones

A lo largo del siglo XIX matemáticos como Dirichlet, Hilbert, Kummer, Eisenstein y Dedekind se dedicaron a encontrar resultados semejantes de orden superior; criterios que permitieran determinar cuándo un entero dado es un residuo cúbico o cuártico módulo un entero dado, por ejemplo. También se descubrieron leyes de reciprocidad cuadrática cuando el anillo que se considera es el de los enteros Gaussianos $\mathbb{Z}[i]$ o el de los enteros de Eisenstein $\mathbb{Z}[\omega]$.

Todos estos trabajos motivaron a considerar el problema de hallar la ley más general del teorema de reciprocidad en cualquier cuerpo numérico algebraico, llegando David Hilbert a considerar este problema como el noveno de su famosa lista de veintitrés problemas, que mencionó en la conferencia en París de 1900. A día de hoy, la ley de reciprocidad más general es el teorema de reciprocidad de Artin, debido a Emil Artin. Para una lectura más precisa y amplia sobre este tema véase *Reciprocity laws* [6].

Referencias

[1] Apostol, Tom M. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Baumgart, Oswald. *The quadratic reciprocity law*. A collection of classical proofs, Edited, translated from the German, and with contributions by Franz Lemmermeyer. Birkhäuser/Springer, Cham, 2015. https://doi.org/10.1007/978-3-319-16283-6.

[3] Delgado de la Mata, Félix; Fuertes Fraile, María Concepción, y Xambó Descamps, Sebastiá. *Introducción al Álgebra*. First. Editorial Complutense, 1993. isbn: 978-84-7491-428-3.

[4] *GAP - Reference Manual*.

[5] Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. ISBN: 978-0-387-96254-2.

[6] Lemmermeyer, Franz. *Reciprocity laws*. Springer Monographs in Mathematics. From Euler to Eisenstein. Springer-Verlag, Berlin, 2000. https://doi.org/10.1007/978-3-662-12893-0.

[7] Navarro Ortega, Gabriel. *Un curso de álgebra*. Second. Vol. 56. Educació. Sèrie Materials. Publicacions de la Universitat de València, 2016. ISBN: 978-84-370-9713-8.

[8] Niven, Ivan; Zuckerman, Herbert S., y Montgomery, Hugh L. *An introduction to the theory of numbers*. Fifth. John Wiley & Sons, Inc., New York, 1991. ISBN: 978-0-471-62546-9.

[9] Silverman, Joseph H. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009. https://doi.org/10.1007/978-0-387-09494-6.