La ley de reciprocidad cuadrática

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Noviembre de 2018

Estos apuntes acompañan una pequeña parte del curso de la teoría de números elemental. El objetivo es dar una prueba de la ley de reciprocidad cuadrática, revisando todo el material necesario. De manera implícita serán presentados algunos conceptos importantes de álgebra, pero voy a evitar las definiciones generales.

Índice

0 Restos módulo n

lección 1
15.11.18

Recordemos (fijemos) la notación y las definiciones básicas. Si para dos números enteros $m, n \in \mathbb{Z}$ se tiene $m = nc$ para algún $c \in \mathbb{Z}$, entonces se dice que n **divide** a m y se escribe $n \mid m$. Se dice que $a, b \in \mathbb{Z}$ son **congruentes** módulo n si $n \mid (a - b)$. En este caso se escribe $a \equiv b \pmod{n}$. Esto define una relación de equivalencia sobre los números enteros, y las clases de equivalencia se llaman los **restos módulo** n. Su conjunto se denota por

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Las operaciones

$$\overline{a} + \overline{b} := \overline{a+b}, \quad \overline{a} \cdot \overline{b} := \overline{ab}$$

están bien definidas y dan estructura de **anillo** sobre $\mathbb{Z}/n\mathbb{Z}$. Normalmente voy a denotar los elementos de $\mathbb{Z}/n\mathbb{Z}$ por las letras x, y, z, y en lugar de $\overline{0}$ y $\overline{1}$ escribiré 0 y 1.

1 Elementos invertibles módulo n

1.1. Definición. Se dice que un resto módulo n dado por $x = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** (o que $a \in \mathbb{Z}$ es **invertible módulo** n) si existe otro resto $y = \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$ (es decir, $ab \equiv 1 \pmod{n}$). En este caso también se dice que y es **inverso** a x (o que $b \in \mathbb{Z}$ es **inverso a** a **módulo** n).

Notamos que si tal y existe, este está definido de modo único como un elemento de $\mathbb{Z}/n\mathbb{Z}$. En efecto, asumamos que existen $y_1, y_2 \in \mathbb{Z}/n\mathbb{Z}$ tales que

$$xy_1 = xy_2 = 1.$$

Luego,

$$y_1 = y_1 \cdot 1 = y_1 x y_2 = 1 \cdot y_2 = y_2.$$

Por esto, si $x \in \mathbb{Z}/n\mathbb{Z}$ es invertible vamos a denotar su inverso por x^{-1}. Notamos que la relación "ser inverso" es simétrica: $x^{-1} = y \iff y^{-1} = x$; en otras palabras, si $x \in \mathbb{Z}/n\mathbb{Z}$ es invertible, entonces x^{-1} es también invertible y

$$(x^{-1})^{-1} = x.$$

1.2. Ejemplo. Trivialmente, 1 es invertible módulo n para cualquier n y es inverso a sí mismo. Notamos que si $n \mid a$, entonces a no es invertible módulo n: todos los múltiplos de a son congruentes a 0 módulo n. ▲

1.3. Ejemplo. Tenemos $5^2 = 25 \equiv 1 \pmod{6}$, así que 5 es inverso a sí mismo módulo 6. Al revisar la tabla de multiplicación módulo 6, se ve que $0, 2, 3, 4$ no son invertibles:

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

▲

1.4. Ejemplo. Todo número a tal que $7 \nmid a$ es invertible módulo 7:

$$2 \cdot 4 \equiv 1 \pmod 7, \quad 3 \cdot 5 \equiv 1 \pmod 7, \quad 6 \cdot 6 \equiv 1 \pmod 7,$$

así que

$$\overline{2}^{-1} = \overline{4}, \quad \overline{3}^{-1} = \overline{5}, \quad \overline{6}^{-1} = \overline{6}.$$

▲

El conjunto de los restos módulo n invertibles se denotará por

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{existe } \overline{b} = \overline{a}^{-1} \in \mathbb{Z}/n\mathbb{Z} \text{ tal que } \overline{a} \cdot \overline{b} = \overline{1}\}.$$

1.5. Observación. *El producto de dos restos módulo n invertibles es también invertible.*

Demostración. Supongamos que para $x, y \in \mathbb{Z}/n\mathbb{Z}$ existen $x^{-1}, y^{-1} \in \mathbb{Z}/n\mathbb{Z}$ tales que

$$xx^{-1} = yy^{-1} = 1.$$

Luego,

$$(xy)\,(y^{-1}x^{-1}) = x\,(yy^{-1})\,x^{-1} = x\,x^{-1} = 1,$$

así que $y^{-1}x^{-1}$ es el resto inverso a xy. ■

1.6. Digresión. Entonces, los restos invertibles $(\mathbb{Z}/n\mathbb{Z})^\times$ están cerrados respecto a la multiplicación. El conjunto $(\mathbb{Z}/n\mathbb{Z})^\times$ respecto a la multiplicación forma una estructura algebraica conocida como **grupo**. Nuestros resultados sobre $(\mathbb{Z}/n\mathbb{Z})^\times$ provienen de la **teoría de grupos** básica.

1.7. Observación (Cancelación). *Para cualesquiera $x, y, z \in \mathbb{Z}/n\mathbb{Z}$, si x es invertible, entonces*

$$xy = xz \Longrightarrow y = z.$$

Demostración. Al multiplicar la identidad $xy = xz$ por x^{-1}, nos queda

$$y = 1 \cdot y = x^{-1}\,xy = x^{-1}\,xz = 1 \cdot z = z.$$

■

1.8. Proposición. *Un número $a \in \mathbb{Z}$ es invertible módulo n si y solo sí es coprimo con n; es decir,* $\operatorname{mcd}(a, n) = 1$.

Demostración. Asumamos que $\operatorname{mcd}(a, n) = 1$. Luego, la **identidad de Bézout** nos dice que existen enteros $b, c \in \mathbb{Z}$ tales que $ab + nc = 1$. Reduciendo módulo n, se obtiene $ab \equiv 1 \pmod n$, así que a es invertible módulo n.

Viceversa, asumamos que existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod n$. Esto significa que $ab - 1 = nc$ para algún $c \in \mathbb{Z}$; es decir, que se tiene la identidad $ab + nc = 1$, lo que implica que $\operatorname{mcd}(a, n) = 1$. ■

1.9. Corolario. *El número de los restos módulo n invertibles es la función de Euler de n:*

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Demostración. Por lo que hemos visto,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid 0 \leq a \leq n-1, \quad \operatorname{mcd}(a, n) = 1\}.$$

■

1.10. Corolario. *Si p es primo, entonces $a \in \mathbb{Z}$ es invertible módulo p si y solo si $p \nmid a$. En otras palabras, todo resto módulo p no nulo es invertible:*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

Demostración. Se tiene $\mathrm{mcd}(a, p) = 1$ si y solo si $p \nmid a$. ■

1.11. Definición. Un anillo donde todo elemento no nulo es invertible, se llama un **cuerpo**[*].

Para subrayar que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, se usa la notación

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}.$$

Otro ejemplo de cuerpos bien conocido son los números racionales $\mathbb{Q}$.

1.12. Observación. *En todo cuerpo, si $xy = 0$, entonces $x = 0$ o $y = 0$. De modo equivalente, si $x, y \neq 0$, entonces $xy \neq 0$.*

Demostración. Si $xy = 0$ y $x \neq 0$, entonces x es invertible y luego $xy = 0 = x\,0$, y podemos cancelar x para obtener $y = 0$. ■

1.13. Corolario. *Los restos módulo n forman un cuerpo si y solo si $n = p$ es un número primo.*

Demostración. Ya hemos notado que si p es primo, entonces $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Ahora si n es un número compuesto, entonces $n = ab$ para algunos $1 < a, b < n$. Luego, los restos $\overline{a}$, $\overline{b}$ no son nulos, pero su producto $\overline{a} \cdot \overline{b} = \overline{ab}$ sí es nulo. Si $\mathbb{Z}/n\mathbb{Z}$ fuera un cuerpo, esto contradiría la observación anterior. ■

Podemos usar los restos invertibles $(\mathbb{Z}/n\mathbb{Z})^\times$ para dar una prueba directa del teorema de Euler.

1.14. Teorema (Euler). *Si* $\mathrm{mcd}(a, n) = 1$, *entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Demostración. Tenemos

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{x_1, x_2, \ldots . x_{\phi(n)}\}.$$

Escribamos $y := \overline{a}$. Dado que $\mathrm{mcd}(a, n) = 1$, tenemos $y \in (\mathbb{Z}/n\mathbb{Z})^\times$. Consideremos la aplicación

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times,$$
$$x \mapsto xy.$$

Esta aplicación está bien definida: si $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$, entonces $xy \in (\mathbb{Z}/n\mathbb{Z})^\times$. Es inyectiva: si $x_1\, y = x_2\, y$, entonces podemos cancelar el elemento invertible y y concluir que $x_1 = x_2$. Siendo una aplicación inyectiva entre un conjunto finito y sí mismo, es también sobreyectiva[*] Esto nos permite concluir que

$$\{x_1, x_2, \ldots . x_{\phi(n)}\} = \{x_1 y, x_2 y, \ldots . x_{\phi(n)} y\}.$$

Luego,

$$\prod_{1 \leq i \leq \phi(n)} x_i = \prod_{1 \leq i \leq \phi(n)} x_i y = y^{\phi(n)} \prod_{1 \leq i \leq \phi(n)} x_i.$$

Cancelando el término $\prod_{1 \leq i \leq \phi(n)} x_i$, podemos concluir que $y^{\phi(n)} = 1$. ■

1.15. Corolario (El pequeño teorema de Fermat). *Para un número primo p, si $p \nmid a$, entonces*

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

[*] O también **campo**. Son sinónimos.

[*] De hecho, se ve que su inversa viene dada por $x \mapsto xy^{-1}$.

2 Digresión: polinomios

Denotemos por K cualquier **cuerpo**; es decir, un anillo donde todo elemento no nulo es invertible. Se puede pensar que $K = \mathbb{F}_p$, porque es el caso que nos va a interesar eventualmente, pero esto no será relevante para la teoría de esta sección.

2.1. Definición. Un **polinomio** en la variable X con coeficientes en K es una expresión formal

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

donde $a_0, a_1, \ldots, a_{n-1}, a_n \in K$. El conjunto de estos polinomios se denota por $K[X]$.

Es cómodo escribir en lugar de la expresión de arriba simplemente

$$f = \sum_{i \geq 0} a_i X^i,$$

donde $a_i \in K$ para todo $i \geq 0$ y $a_i = 0$ para i suficientemente grande (para $i > n$ en el caso de arriba).

Las palabras "expresión formal" significan que dos polinomios $\sum_{i\geq 0} a_i X^i$ y $\sum_{i\geq 0} b_i X^i$ son iguales si y solo si $a_i = b_i$ para todo i.

2.2. Definición. El **grado** de $f = \sum_{i\geq 0} a_i X^i$ se define mediante

$$\deg f := \text{máx}\{i \mid a_i \neq 0\}.$$

Si $a_i = 0$ para todo $i \geq 0$, se dice que $f = 0$ es **el polinomio nulo** y se pone

$$\deg f := -\infty.$$

2.3. Definición. Para dos polinomios

$$f = \sum_{i\geq 0} a_i X^i,\ g = \sum_{i\geq 0} b_i X^i \in K[X]$$

su suma se define término por término:

$$f + g := \sum_{i\geq 0} (a_i + b_i) X^i,$$

mientras que el producto se define mediante la distributividad y las identidades $a_i X^i \cdot b_j X^j = a_i b_j X^{i+j}$:

$$fg := \sum_{k\geq 0} c_k X^k, \quad \text{donde } c_k := \sum_{i+j=k} a_i b_j.$$

Ejercicio 1. *Comprueba que $K[X]$ es un anillo respecto a las operaciones de arriba. En particular, demuestre la asociatividad de la multiplicación y su distributividad respecto a la suma:*

$$(fg)\, h = f\, (gh), \quad (f + g)\, h = fh + gh.$$

2.4. Proposición. *Para cualesquiera $f, g \in K[X]$ se cumple*

$$\deg(fg) = \deg f + \deg g.$$

Demostración. Si $f = 0$ o $g = 0$, entonces $fg = 0$ y la identidad en cuestión se cumple por nuestra definición $\deg 0 := -\infty$. Podemos asumir entonces que $f \neq 0$ y $g \neq 0$. Escribamos

$$f = a_m X^m + \cdots + a_1 X + 1, \quad g = b_n X^n + \cdots + b_1 X + b_0,$$

donde $a_m, b_n \neq 0$. Luego,

$$fg = a_m b_n X^{m+n} + \cdots + (a_0 b_1 + a_1 b_0) X + a_0 b_0,$$

donde $a_m b_n \neq 0$. ■

2.5. Definición. Para un polinomio

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$$

y un elemento $c \in K$, el resultado de **evaluación** de f en c es

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 \in K.$$

Si $f(c) = 0$, se dice que c es una **raíz** de f.

Notamos que la evaluación está compatible con las sumas y productos de polinomios:

$$(f + g)(c) = f(c) + g(c), \quad (fg)(c) = f(c) \cdot g(c).$$

2.6. Comentario. No hay que confundir los polinomios con funciones polinomiales $K \to K$. Por ejemplo, si $K = \mathbb{F}_p$ es un cuerpo finito (y esto es el caso que nos va a interesar más adelante), entonces hay p^p diferentes aplicaciones $\mathbb{F}_p \to \mathbb{F}_p$, mientras que el conjunto $\mathbb{F}_p[X]$ es infinito: sus elementos son sumas formales de grado arbitrario. Por esto diferentes polinomios $f, g \in \mathbb{F}_p[X]$ pueden dan lugar a la misma aplicación $\mathbb{F}_p \to \mathbb{F}_p$. Por ejemplo, según el pequeño teorema de Fermat, el polinomio $X^p - X$ evaluado en cualquier $c \in \mathbb{F}_p$ nos da 0, aunque este polinomio no es nulo.

2.7. Lema. *Sean $f \in K[X]$ un polinomio de grado $n > 0$ y $c \in K$. Entonces, existe un polinomio $g \in K[X]$ de grado $n - 1$ tal que*

$$f = (X - c)\, g + r$$

para algún $r \in K$.

Demostración. Escribamos

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

El polinomio g que estamos buscando tiene que ser de la forma

$$g = b_{n-1} X^{n-1} + b_{n-2} X^{n-2} + \cdots + b_1 X + b_0.$$

Tenemos

$$(X - c)\, g + r = (X - c)\,(b_{n-1} X^{n-1} + b_{n-2} X^{n-2} + \cdots + b_1 X + b_0) + r = \\ b_{n-1} X^n + (b_{n-2} - c\, b_{n-1}) X^{n-1} + \cdots + (b_1 - c\, b_2) X^2 + (b_0 - c\, b_1) X + r - c\, b_0.$$

Para que este polinomio sea igual a f, deben cumplirse las identidades

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - c b_{n-1}, \\ a_{n-2} &= b_{n-3} - c b_{n-2}, \\ &\cdots \\ a_1 &= b_0 - c b_1, \\ a_0 &= r - c\, b_0 \end{aligned}$$

que nos llevan a las recurrencias

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + cb_{n-1}, \\ b_{n-3} &= a_{n-2} + cb_{n-2}, \\ &\cdots \\ b_i &= a_{i+1} + cb_{i+1}, \\ &\cdots \\ b_0 &= a_1 + cb_1, \\ r &= a_0 + cb_0 \end{aligned}$$

que definen de modo único los coeficientes del polinomio g y la constante r. ■

2.8. Proposición. *Para un polinomio $f \in K[X]$, un elemento $c \in K$ es una raíz de f si y solamente si*

$$f = (X - c) \cdot g$$

para algún polinomio $g \in K[X]$.

Demostración. En una dirección, esto es obvio: si podemos escribir

$$f = (X - c) \cdot g,$$

entonces la evaluación en c nos da

$$f(c) = (c - c) \cdot g(c) = 0.$$

En la otra dirección, el lema anterior nos dice que un polinomio no constante f siempre puede ser escrito como

$$f = (X - c)\, g + r$$

para algunos $g \in K[X]$ y $r \in K$. Ahora si c es una raíz de f, entonces

$$0 = f(c) = \underbrace{(c - c)}_{=0}\, g(c) + r,$$

de donde podemos concluir que $r = 0$. ■

lección 2
16.11.18

2.9. Corolario (Lagrange, 1768). *Si $f \in K[X]$ es un polinomio no nulo, entonces f tiene $\leq \deg f$ raíces distintas en K.*

Demostración. Inducción sobre $n = \deg f$. Si $n = 0$, entonces f, siendo un polinomio constante no nulo, no tiene raíces. Para el paso inductivo, notamos que si $c \in K$ es una raíz de f, entonces

$$f = (X - c)\, g$$

para algún polinomio $g \in K[X]$. Luego,

$$\deg f = \deg(X - c) \cdot \deg g,$$

así que $\deg g = n - 1$ y por la hipótesis de inducción sabemos que g tiene $\leq n - 1$ raíces. Toda raíz de g es una raíz de f, y si $c' \neq c$ es una raíz de f, entonces la identidad en K

$$0 = f(c') = (c - c') \cdot g(c')$$

implica que $g(c') = 0$ y c' es una raíz de g. Podemos concluir que f tiene $\leq n$ diferentes raíces. ■

2.10. Ejemplo. Consideremos el polinomio $f := X^3 - 1 \in K[X]$.

1) Si $K = \mathbb{F}_5$, entonces f tiene solo una raíz $X = 1$. Luego,

$$(X-1)(X^2+X+1) = X^3 - 1 \quad \text{en } \mathbb{F}_5[X],$$

donde el polinomio $X^2 + X + 1$ no tiene ninguna raíz en $\mathbb{F}_5$.

2) Si $K = \mathbb{F}_7$, entonces f tiene tres raíces $X = 1, 2, 4$ y

$$(X-1)(X-2)(X-4) = X^3 - 7X^2 + 14X - 8 = X^3 - 1 \quad \text{en } \mathbb{F}_7[X].$$

3) Si $K = \mathbb{F}_3$, entonces f tiene solo una raíz $X = 1$, pero es una "raíz de multiplicidad 3" porque

$$(X-1)^3 = X^3 - 3X^2 + 3X - 1 = X^3 - 1 \quad \text{en } \mathbb{F}_3[X].$$

▲

Ejercicio 2. *Encuentre las raíces de polinomios*

$$f = X^2 + 1, \quad X^3 + 1, \quad X^4 + 1$$

en $K = \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$. *Cuando hay una raíz, escriba* f *como* $f = (X - c)\, g$ *para* $g \in K[X]$. *Si* g *también tiene raíces, repita este proceso para* g.

Ejercicio 3. *Demuestre que para todo polinomio* $f = \sum_{i \geq 0} a_i X^i \in \mathbb{F}_p[X]$ *se cumple*

$$f(X^p) := \sum_{i \geq 0} a_i X^{pi} = \left(\sum_{i \geq 0} a_i X^i \right)^p =: f^p.$$

Ejercicio 4. *Consideremos un polinomio cuadrático* $f = a X^2 + b X + c \in \mathbb{F}_p[X]$ *donde* p *es un primo impar*[*] *y* $a \neq 0$ *en* $\mathbb{F}_p$. *Consideremos el elemento*

$$D := b^2 - 4ac \in \mathbb{F}_p.$$

Demuestre que

1) *si en* $\mathbb{F}_p$ *no existe un elemento* $\sqrt{D}$ *tal que* $\sqrt{D}^2 = D$, *entonces* f *no tiene raíces;*

2) *si tal* $\sqrt{D}$ *existe, entonces* f *tiene raíces dadas por*

$$x = \frac{-b \pm \sqrt{D}}{2a} =: (-b \pm \sqrt{D}) \cdot (2a)^{-1}.$$

2.11. Digresión. El lector puede notar que en ninguna parte de esta sección hemos tomado los elementos inversos a_i^{-1} para $a_i \in K$. De hecho, lo único que hemos usado es la propiedad 1.12.

Aunque se pueden considerar los polinomios con coeficientes en $\mathbb{Z}/n\mathbb{Z}$ donde n, en este caso 1.12 no se cumple y puede pasar que $\deg(fg) < \deg f + \deg g$. Por ejemplo, en $\mathbb{Z}/8\mathbb{Z}[X]$ tenemos trivialmente $2X \cdot 4X = 0$. Por esto la prueba de 2.9 no funciona y un polinomio $f \in \mathbb{Z}/n\mathbb{Z}[X]$ con n compuesto puede tener más de $\deg f$ raíces. Por ejemplo, el polinomio cuadrático $f = X^2 - 1$ tiene cuatro raíces en $\mathbb{Z}/n\mathbb{Z}$: son $1, 3, 5, 7$. Tenemos

$$(X-1)(X+1)(X-3)(X+3) = (X^2-1)(X^2-3^2) = (X^2-1)^2 \quad \text{en } \mathbb{Z}/8\mathbb{Z}[X].$$

[*]Por supuesto, "primo impar" significa nada más que $p \neq 2$. Esta expresión es muy común y aparecerá muy a menudo en estos apuntes porque el primo 2 es muy especial en varios aspectos.

3 Orden multiplicativo módulo n

Sea $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ un resto módulo n invertible. Consideremos sus potencias:

$$1, x, x^2, x^3, \ldots \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

El conjunto $(\mathbb{Z}/n\mathbb{Z})^\times$ es finito, y por ende en esta lista hay repeticiones: existen $1 \leq k < \ell$ tales que $x^k = x^\ell$. Luego, al multiplicar esta identidad por $(x^k)^{-1}$, nos queda $x^{\ell-k} = 1$. Entonces, para todo $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ existe $k = 1, 2, 3, \ldots$ tal que $x^k = 1$.

3.1. Definición. Para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ el mínimo número positivo k tal que $x^k = 1$ se llama el **orden** de x. En este caso se escribe

$$\operatorname{ord} x = k.$$

Notamos que la discusión de arriba demuestra que los elementos

$$1, x, x^2, x^3, \ldots, x^{\operatorname{ord} x - 1}$$

deben ser distintos.

3.2. Ejemplo. En $\mathbb{F}_7^\times = (\mathbb{Z}/7\mathbb{Z})^\times$ tenemos

$$\begin{aligned}
&\operatorname{ord} \overline{1} = 1, \\
&\operatorname{ord} \overline{2} = 3, \quad (2^2 = 4,\ 2^3 \equiv 1) \\
&\operatorname{ord} \overline{3} = 6, \quad (3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1) \\
&\operatorname{ord} \overline{4} = 3, \quad (4^2 \equiv 2,\ 4^3 \equiv 1) \\
&\operatorname{ord} \overline{5} = 6, \quad (5^2 \equiv 4,\ 5^3 \equiv 6,\ 5^4 \equiv 2,\ 5^6 \equiv 1) \\
&\operatorname{ord} \overline{6} = 2. \quad (6^2 \equiv 1)
\end{aligned}$$

▲

Ejercicio 5. *Encuentre los órdenes de los elementos de* $(\mathbb{Z}/8\mathbb{Z})^\times$ *y* $(\mathbb{Z}/10\mathbb{Z})^\times$.

3.3. Observación. *Para* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ *se tiene* $x^k = 1$ *si y solo si* $\operatorname{ord} x \mid k$.

Demostración. Si $k = m \cdot \operatorname{ord} x$, entonces

$$x^k = (x^{\operatorname{ord} x})^m = 1^m = 1.$$

Viceversa, supongamos que $x^k = 1$. La división con resto nos da $k = q \cdot \operatorname{ord} x + r$, donde $0 \leq r < \operatorname{ord} x$. Tenemos

$$1 = x^k = x^{q \cdot \operatorname{ord} x + r} = x^{x \cdot \operatorname{ord} x}\, x^r = x^r.$$

Pero $\operatorname{ord} x$ es el mínimo número positivo tal que $x^{\operatorname{ord} x} = 1$. Entonces, necesariamente $r = 0$, y por ende $\operatorname{ord} x \mid k$. ■

3.4. Corolario. *Para todo* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ *se tiene* $\operatorname{ord} x \mid \phi(n)$.

Demostración. Se sigue del teorema de Euler 1.14. ■

3.5. Corolario. *Para* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ *se tiene* $x^k = x^\ell$ *si y solo si* $k \equiv \ell \pmod{\operatorname{ord} x}$.

Demostración. Sin pérdida de generalidad, $k \leq \ell$. Luego, $x^k = x^\ell$ si y solo si $x^{\ell-k} = 1$, lo que sucede si y solo si $\operatorname{ord} x \mid (\ell - k)$. ■

3.6. Ejemplo. Tenemos $2^2 \equiv 2^5 \equiv 4 \pmod 7$, dado que $2 \equiv 5 \pmod 3$, donde 3 es el orden de 2 módulo 7. ▲

3.7. Proposición. *Para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ se tiene*

$$\operatorname{ord} x^k = \frac{\operatorname{ord} x}{\operatorname{mcd}(\operatorname{ord} x, k)}.$$

Demostración. Denotemos $m := \operatorname{ord} x$. Si $\operatorname{mcd}(m,k) = d$, entonces podemos escribir

$$m = dm', \quad k = dk', \quad \text{donde } \operatorname{mcd}(m',k') = 1.$$

Luego,

$$m \mid k\ell \iff dm' \mid dk'\ell \iff m' \mid k'\ell \iff m' \mid \ell.$$

Tenemos entonces

$$\operatorname{ord} x^k = \min\{\ell \mid (x^k)^\ell = 1\} = \min\{\ell \mid m \mid k\ell\} = \min\{\ell \mid m' \mid \ell\} = m' = m/d.$$

■

3.8. Ejemplo. Módulo 7, se tiene

$$\operatorname{ord} 2^2 = \frac{\operatorname{ord} 2}{\operatorname{mcd}(\operatorname{ord} 2, 2)} = \frac{3}{\operatorname{mcd}(3,2)} = 3.$$

▲

3.9. Proposición. *Para $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$, si $\operatorname{mcd}(\operatorname{ord} x, \operatorname{ord} y) = 1$, entonces $\operatorname{ord}(xy) = \operatorname{ord} x \cdot \operatorname{ord} y$.*

Demostración. Primero,

$$(xy)^{\operatorname{ord} x \cdot \operatorname{ord} y} = (x^{\operatorname{ord} x})^{\operatorname{ord} y} (y^{\operatorname{ord} y})^{\operatorname{ord} x} = 1,$$

lo que implica

$$\operatorname{ord}(xy) \mid \operatorname{ord} x \cdot \operatorname{ord} y.$$

Además,

$$x^{\operatorname{ord} y \cdot \operatorname{ord}(xy)} = (y^{\operatorname{ord} y})^{\operatorname{ord}(xy)}\, x^{\operatorname{ord} y \cdot \operatorname{ord}(xy)} = ((xy)^{\operatorname{ord}(xy)})^{\operatorname{ord} y},$$

de donde

$$\operatorname{ord} x \mid \operatorname{ord} y \cdot \operatorname{ord}(xy).$$

De modo similar, intercambiando x e y, se obtiene

$$\operatorname{ord} y \mid \operatorname{ord} x \cdot \operatorname{ord}(xy).$$

Pero $\operatorname{mcd}(\operatorname{ord} x, \operatorname{ord} y) = 1$ por nuestra hipótesis, así que

$$\operatorname{ord} x \cdot \operatorname{ord} y \mid \operatorname{ord}(xy).$$

■

3.10. Ejemplo. Los números 7 y 8 son invertibles módulo 9. Tenemos

$$7^2 \equiv 4,\ 7^3 \equiv 1, \quad 8^2 \equiv 1 \pmod 9,$$

así que 7 y 8 tienen orden 3 y 2 módulo 9. Los números 2 y 3 son coprimos, así que, $7 \cdot 8 \equiv 2 \pmod 9$ debe tener orden 6. En efecto,

$$2^2 = 4,\ 2^3 = 8,\ 2^4 \equiv 7,\ 2^5 \equiv 5,\ 2^6 \equiv 1 \pmod 9.$$

▲

Ejercicio 6. *Demuestre que para todo $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ se tiene $\operatorname{ord} x = \operatorname{ord}(x^{-1})$.*

4 Raíces primitivas módulo p

El objetivo de esta sección es probar el siguiente resultado.

4.1. Teorema. *Si p es un número primo, entonces para todo $d \mid (p-1)$ en $\mathbb{F}_p^\times$ hay $\phi(d)$ elementos de orden d.*

En particular, nos va a interesar el siguiente caso particular.

4.2. Corolario. *Para un primo p, en $\mathbb{F}_p^\times$ existe un elemento de orden $p-1$; en otras palabras, existe $x \in \mathbb{F}_p^\times$ tal que sus potencias nos dan todos los restos invertibles módulo p:*

$$\mathbb{F}_p^\times = \{1, x, x^2, x^3, \ldots, x^{p-2}\}.$$

Demostración. Basta tomar $d = p-1$ en el teorema y notar que $\phi(p-1) \geq 1$. ■

4.3. Definición. Un elemento x del corolario se llama una **raíz primitiva módulo** p, o un **generador** de $\mathbb{F}_p^\times$.

Las raíces primitivas simplifican mucho la vida: escribiendo todos los elementos de $\mathbb{F}_p^\times$ como las potencias x^k de algún x fijo, es fácil entender las propiedades multiplicativas, ya que $x^k \cdot x^\ell = x^{k+\ell}$. La existencia de raíces primitivas se usa de modo implícito en los trabajos de Euler, pero fue probada por primera vez por Gauss en su tratado "Disquisitiones arithmeticae" ("Investigaciones aritméticas") publicado en 1801.

4.4. Ejemplo. Módulo $p = 5$, las potencias de 2 nos dan

$$2, \quad 2^2 = 4, \quad 2^3 \equiv 3, \quad 2^4 \equiv 1.$$

De modo similar, calculando las potencias de 3, se obtiene

$$3, \quad 3^2 \equiv 4, \quad 3^3 \equiv 2, \quad 3^4 \equiv 1.$$

Esto significa que 2 y 3 son raíces primitivas módulo 5. ▲

4.5. Ejemplo. He aquí una pequeña tabla de las raíces primitivas módulo p para diferentes p.

$p = 2$:	$\overline{1}$;	
$p = 3$:	$\overline{2}$;	$(\phi(2) = 1)$
$p = 5$:	$\overline{2}, \overline{3}$;	$(\phi(4) = 2)$
$p = 7$:	$\overline{3}, \overline{5}$;	$(\phi(6) = 2)$
$p = 11$:	$\overline{2}, \overline{6}, \overline{7}, \overline{8}$;	$(\phi(10) = 4)$
$p = 13$:	$\overline{2}, \overline{6}, \overline{7}, \overline{11}$;	$(\phi(12) = 4)$
$p = 17$:	$\overline{3}, \overline{5}, \overline{6}, \overline{7}, \overline{10}, \overline{11}, \overline{12}, \overline{14}$;	$(\phi(16) = \phi(2^4) = (2-1) \cdot 2^3 = 8)$
$p = 19$:	$\overline{2}, \overline{3}, \overline{10}, \overline{13}, \overline{14}, \overline{15}$;	$(\phi(18) = \phi(2)\,\phi(9) = (3-1) \cdot 3 = 6)$
	$\ldots$	

▲

Ejercicio 7. *Compruebe que 3 y 5 son raíces primitivas módulo 7.*

4.6. Ejemplo. Si n no es primo, entonces $(\mathbb{Z}/n\mathbb{Z})^\times$ no necesariamente tiene una raíz primitiva (que sería un elemento de orden $\phi(n)$). Por ejemplo, si $n = 8$, los restos invertibles módulo 8 son $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Luego, tenemos $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, así que

$$\operatorname{ord} \overline{1} = 1, \quad \operatorname{ord} \overline{3} = \operatorname{ord} \overline{5} = \operatorname{ord} \overline{7} = 2.$$

En general, $(\mathbb{Z}/n\mathbb{Z})^\times$ tiene una raíz primitiva (un resto módulo n cuyas potencias nos dan todos los elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$) solo si n es de la forma $2, 4, p^k$, o $2p^k$ donde p es un primo impar y $k = 1, 2, 3, \ldots$ No es muy difícil probarlo, pero no vamos a necesitar este resultado.

Por ejemplo, $(\mathbb{Z}/10\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ y $\overline{3}$ y $\overline{7}$ son raíces primitivas módulo 10, ya que

$$3^2 = 9,\ 3^3 \equiv 7 \pmod{10}, \quad 7^2 \equiv 9,\ 7^3 \equiv 3 \pmod{10}.$$

▲

lección 3
22.11.18

4.7. Lema. *La función de Euler satisface*

$$\sum_{d|n} \phi(d) = n.$$

Demostración. Consideremos las fracciones

$$\frac{1}{n},\ \frac{2}{n},\ \frac{3}{n},\ \ldots,\ \frac{n-1}{n}.$$

Podemos reducirlas a la forma $\frac{a}{b}$, donde $a < b$ y $\operatorname{mcd}(a, b) = 1$. Al hacerlo, en los denominadores estarán los divisores $d \mid n$. El número de tales fracciones con d en el denominador es precisamente $\phi(d)$. ■

4.8. Ejemplo. Para $n = 10$ tenemos

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10.$$

▲

Demostración del teorema. Para $x \in \mathbb{F}_p^\times$ se tiene $\operatorname{ord} x \mid \phi(p) = p - 1$. Para todo $d \mid (p-1)$, definamos

$$\psi(d) := \#\{x \in \mathbb{F}_p^\times \mid \operatorname{ord} x = d\}.$$

Tenemos entonces

$$\sum_{d|(p-1)} \psi(d) = p - 1.$$

Sea d un divisor de $p-1$ tal que $\psi(d) > 0$ y sea $x \in \mathbb{F}_p^\times$ un residuo de orden d. En este caso

$$1, x, x^2, \ldots, x^{d-1}$$

son elementos distintos de $\mathbb{F}_p^\times$ que cumplen $(x^k)^d = (x^d)^k = 1$; es decir, son d raíces del polinomio $X^d - 1 \in \mathbb{F}_p[X]$. Pero según 2.9, este polinomio tiene a lo sumo d raíces, así que $z = 1, x, x^2, \ldots, x^{d-1}$ son *todos* los elementos en $\mathbb{F}_p^\times$ que cumplen $z^d = 1$. En particular, todos los elementos de orden d están en esta lista.

Luego, la fórmula

$$\operatorname{ord}(x^k) = \frac{\operatorname{ord} x}{\operatorname{mcd}(\operatorname{ord} x, k)} = \frac{d}{\operatorname{mcd}(d, k)}$$

nos dice que

$$\operatorname{ord}(x^k) = d \iff \operatorname{mcd}(d, k) = 1,$$

y por lo tanto,

$$\psi(d) = \#\{x^k \mid 0 \le k \le d-1,\ \operatorname{mcd}(d, k) = 1\} = \phi(d).$$

Hemos probado entonces que para todo $d \mid (p-1)$, si $\psi(d) > 0$, entonces $\psi(d) = \phi(d)$. Pero según el lema anterior,

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \phi(d) = p - 1,$$

y por ende *para todo* $d \mid (p-1)$ se cumple $\psi(d) = \phi(d)$. ■

4.9. Comentario. Note que aunque hemos establecido la existencia de una raíz primitiva módulo p y sabemos que hay $\phi(p-1)$ de ellas, nuestra prueba no produce una raíz primitiva de manera explícita. En efecto, no existe una fórmula general para una raíz primitiva módulo p.

5 El símbolo de Legendre y los cuadrados módulo p

5.1. Definición. Sea p un número primo. Se dice que un entero $a \in \mathbb{Z}$ es un **cuadrado** (o **residuo cuadrático**) **módulo** p si existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a \pmod{p}$. De modo equivalente, $x \in \mathbb{F}_p$ es un cuadrado si existe $y \in \mathbb{F}_p$ tal que $x = y^2$.

5.2. Ejemplo. Los cuadrados en $\mathbb{Z}/7\mathbb{Z}$ son $\overline{0}, \overline{1}, \overline{2}, \overline{4}$:

$$0^2 = 0, \quad 1^2 \equiv 6^2 \equiv 1, \quad 3^2 \equiv 4^2 \equiv 2, \quad 2^2 \equiv 5^2 \equiv 4 \pmod{7}.$$

He aquí una lista de cuadrados en $\mathbb{Z}/p\mathbb{Z}$ para diferentes p:

$$\begin{aligned}
p = 2&: \overline{0}, \overline{1};\\
p = 3&: \overline{0}, \overline{1};\\
p = 5&: \overline{0}, \overline{1}, \overline{4};\\
p = 7&: \overline{0}, \overline{1}, \overline{2}, \overline{4};\\
p = 11&: \overline{0}, \overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9};\\
p = 13&: \overline{0}, \overline{1}, \overline{3}, \overline{4}, \overline{9}, \overline{10}, \overline{12};\\
p = 17&: \overline{0}, \overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{9}, \overline{13}, \overline{15}, \overline{16};\\
p = 19&: \overline{0}, \overline{1}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{9}, \overline{11}, \overline{16}, \overline{17};\\
p = 23&: \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{12}, \overline{13}, \overline{16}, \overline{18};\\
p = 29&: \overline{0}, \overline{1}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{9}, \overline{13}, \overline{16}, \overline{20}, \overline{22}, \overline{23}, \overline{24}, \overline{25}, \overline{28}.
\end{aligned}$$

▲

Notamos que para x fijo la ecuación $y^2 - x = 0$ siempre tiene ≤ 2 soluciones $y \in \mathbb{F}_p$. Si p es un primo impar, entonces esta ecuación o no tiene soluciones, o tiene dos diferentes soluciones $+y$ e $-y$. Por ejemplo, $5 \equiv 4^2 \equiv 7^2 \pmod{11}$.

5.3. Comentario. Módulo 2, cualquier número es un cuadrado. Para excluir este caso trivial, en varios resultados vamos a asumir que p es un primo impar.

Nuestro objetivo es desarrollar un método eficaz de ver si un número es un cuadrado módulo p, sin calcular explícitamente su "raíz cuadrada" módulo p. Para esto sirve el símbolo de Legendre.

5.4. Definición. Para un número entero a y un primo p el **símbolo de Legendre** se define mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un cuadrado módulo } p,\\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p,\\ 0, & \text{si } p \mid a. \end{cases}$$

5.5. Observación. *El símbolo de Legendre $\left(\frac{a}{p}\right)$ depende solamente del resto de a módulo p: si $a' \equiv a \pmod{p}$, entonces*

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

Demostración. La propiedad de ser un cuadrado módulo p depende solo del resto de a módulo p. ■

5.6. Proposición. *El símbolo de Legendre es multiplicativo: para cualesquiera $a, b \in \mathbb{Z}$ se cumple*

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

Notamos que si a y b son cuadrados, por ejemplo $a \equiv c^2$ y $b \equiv d^2 \pmod{p}$, entonces $ab \equiv (cd)^2$ es un cuadrado. Lo que no está claro es por qué el producto de dos no-cuadrados debe ser un cuadrado.

Demostración. Si $p \mid a$ o $p \mid b$, entonces $p \mid ab$, y la identidad se cumple. dado que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$. Podemos asumir entonces que $p \nmid a$ y $p \nmid b$, así que ambos símbolos $\left(\frac{a}{p}\right)$ y $\left(\frac{b}{p}\right)$ son iguales a ± 1.

En este caso los números a y b corresponden a elementos no nulos de $\mathbb{F}_p$. Hemos probado que existe un elemento (raíz primitiva) $x \in \mathbb{F}_p^\times$ tal que

$$\mathbb{F}_p = \{0, 1, x, x^2, \ldots, x^{p-2}\}.$$

Entonces, $\overline{a} = x^k$ y $\overline{b} = x^\ell$ para algunos k, ℓ. Notamos que x^k es un cuadrado si y solo si k es un número par. Luego, $x^k\, x^\ell = x^{k+\ell}$ y tenemos

$$\left(\frac{a}{p}\right) = (-1)^k, \quad \left(\frac{b}{p}\right) = (-1)^\ell, \quad \left(\frac{ab}{p}\right) = (-1)^{k+\ell}.$$

■

5.7. Ejemplo. Los números 3 y 5 no son cuadrados módulo 7, pero $15 \equiv 1$ es claramente un cuadrado. ▲

5.8. Comentario. Para nuestras pruebas es importante que p sea primo. Los cuadrados módulo un número compuesto n no se comportan bien. Por ejemplo, módulo 8 los cuadrados son

$$0 = 0^2 \equiv 4^2, \quad 1 = 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2, \quad 4 = 2^2 \equiv 6^2$$

y los números $2, 3, 5, 6, 7$ no son cuadrados. Note que 1 tiene cuatro "raíces cuadradas" módulo 8: son ± 1 y ± 3.

5.9. Proposición. *Sea p un primo impar. Entonces, entre los números $1, 2, 3, \ldots, p-1$ precisamente la mitad son cuadrados módulo p y la mitad no son cuadrados.*

Demostración. Tenemos

$$\mathbb{F}_p^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{1, x, x^2, \ldots, x^{p-2}\},$$

donde x es una raíz primitiva y x^k es un cuadrado si y solo si k es par. ■

5.10. Ejemplo. Consideremos los restos módulo 7. Podemos escoger una raíz primitiva $x = \overline{3}$. Tenemos

$$\mathbb{F}_7^\times = \{1 \equiv 3^6,\ 2 \equiv 3^2,\ 3,\ 4 \equiv 3^4,\ 5 \equiv 3^5,\ 6 \equiv 3^3\}.$$

Luego, los cuadrados no nulos módulo 7 son $1, 2, 4$. ▲

Ejercicio 8. *Demuestre que si p es un primo impar, entonces*

$$\sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) = 0.$$

Ejercicio 9. *Para $n = 2, 3, 4, \ldots$ sea p un primo tal que $p \equiv 1 \pmod{n}$.*

1) *Demuestre que para todo $x \in \mathbb{F}_p^\times$ o $x \neq y^n$ para ningún n, o $x = y^n$ para n diferentes $y \in \mathbb{F}_p^\times$.*

2) *Demuestre que el conjunto*
$$\{x \in \mathbb{F}_p^\times \mid x = y^n \text{ para algún } y \in \mathbb{F}_p^\times\}$$
tiene $\frac{p-1}{n}$ elementos.

3) *En particular, encuentre todos los cubos en $\mathbb{F}_{13}^\times$.*

6 El criterio de Euler

Nos va a servir la siguiente interpretación del símbolo de Legendre.

6.1. Proposición (Criterio de Euler). *Si p es un primo impar, entonces*
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Demostración. Si $p \mid a$, entonces $\left(\frac{a}{p}\right) = 0$ y $a^{\frac{p-1}{2}} = 0 \pmod{p}$, así que el resultado es obvio. Asumamos entonces que $p \nmid a$. En este caso de nuevo, podemos escoger una raíz primitiva $x \in \mathbb{F}_p^\times$ tal que
$$\mathbb{F}_p^\times = \{1, x, x^2, \ldots, x^{p-2}\}.$$
Luego, $\overline{a}_p = x^k$ para algún k y $\left(\frac{a}{p}\right) = (-1)^k$. Si k es un número par, entonces $\operatorname{ord} x = (p-1) \mid k\,\frac{p-1}{2}$, y luego
$$\overline{a^{\frac{p-1}{2}}} = x^{k\frac{p-1}{2}} = 1.$$
Si k es un número impar, entonces
$$x^{k\frac{p-1}{2}} \neq 1.$$
Sin embargo,
$$\left(x^{k\frac{p-1}{2}}\right)^2 = x^{k(p-1)} = 1,$$
lo que nos permite concluir que
$$x^{k\frac{p-1}{2}} = -1.$$
—en efecto, el polinomio $X^2 - 1 \in \mathbb{F}_p[X]$ tiene dos raíces y son $+1$ y -1. ■

6.2. Ejemplo. El criterio de Euler es de interés teórico y no ayuda mucho con los cálculos del símbolo de Legendre. Podemos revisar un ejemplo sencillo: para $p = 7$ tenemos $\frac{p-1}{2} = 3$. Luego, $2^3 \equiv 1 \pmod{7}$ y en efecto, $2 \equiv 3^2$ es un cuadrado módulo 7. Por otro lado, $3^3 \equiv 6 \equiv -1 \pmod{7}$, así que 3 no es un cuadrado módulo 7. ▲

7 La primera ley de reciprocidad suplementaria

Sustituyendo $a = -1$ en el criterio de Euler, se obtiene que para p impar

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p};$$

es decir,

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

7.1. Observación. *Sea p un número impar. Entonces, $\frac{p-1}{2}$ es par si $p \equiv 1 \pmod 4$ y es impar si $p \equiv 3 \pmod 4$.*

Demostración. Si $p = 4k+1$, entonces $\frac{p-1}{2} = 2k$. Si $p = 4k+3$, entonces $\frac{p-1}{2} = 2k+1$. ■

Entonces, como una consecuencia del criterio de Euler, hemos obtenido el siguiente resultado.

7.2. Proposición (La primera ley de reciprocidad suplementaria). *Si p es un primo impar, entonces*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

7.3. Ejemplo. Consideremos los restos módulo 4 de los primeros primos impares:

p:	3	5	7	11	13	17	19	23	29	31	37	$\cdots$
$p \bmod 4$:	3	1	3	3	1	1	3	3	1	3	1	$\cdots$

Entonces, -1 es un cuadrado módulo $p = 5, 13, 17, 29, 37, \ldots$

$$-1 \equiv 2^2 \pmod 5, \quad -1 \equiv 5^2 \pmod{13}, \quad -1 \equiv 4^2 \pmod{17},$$
$$-1 \equiv 12^2 \pmod{29}, \quad -1 \equiv 6^2 \pmod{37}.$$

▲

8 Un lema de Gauss

lección 4
23.11.18

El siguiente lema pertenece a Gauss y da otra interpretación útil del símbolo de Legendre.

8.1. Lema. *Sea p un primo impar y $a \in \mathbb{Z}$ un entero tal que $p \nmid a$. Pongamos $n := \frac{p-1}{2}$.*

1) Consideremos los números

$$a, 2a, 3a, \ldots, na.$$

Sea s el número de elementos de arriba cuyo resto de división por p es mayor que $\frac{p}{2}$. Entonces,

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

2) Si $a \geq 3$ es un número impar, entonces

$$\left(\frac{a}{p}\right) = (-1)^t, \quad \textit{donde } t := \sum_{1 \leq i \leq n} \left\lfloor \frac{ai}{p} \right\rfloor.$$

Demostración. Puesto que $p \nmid a$ y $p \nmid i$ para ningún $1 \leq i \leq n$, ningún número entre

$$a, 2a, 3a, \ldots, na.$$

es divisible por p. Además, estos números no son congruentes entre sí: en efecto, si $ia \equiv ja \pmod{p}$, entonces $i \equiv j \pmod{p}$, lo que sucede si y solo si $i = j$, dado que $1 \leq i, j \leq n$.

Reemplazando los números de arriba por sus restos de división por p y poniéndolos en el orden creciente, se obtiene

$$b_1, b_2, \ldots, b_r, c_1, c_2, \ldots, c_s,$$

donde $r + s = n$ y

$$1 \leq b_1 < b_2 < \cdots < b_r < \frac{p}{2} < c_1 < c_2 < \cdots < c_s \leq p - 1.$$

Pasemos ahora a los números

$$b_1, b_2, \ldots, b_r, p - c_1, p - c_2, \ldots, p - c_s. \tag{1}$$

Notamos que todos los elementos de esta lista están entre 1 y $n := \frac{p-1}{2}$. De nuevo, estos números no son congruentes entre sí. Está claro que $b_i \not\equiv b_j$ y $p - c_i \not\equiv p - c_j$ para $i \neq j$. Para ver que $b_i \not\equiv p - c_j$, notamos que en este caso tendríamos $b_i + c_j \equiv 0$. Sin embargo, $b_i \equiv k\,a$ y $c_j \equiv \ell\,a$ para algunos $1 \leq k, \ell \leq n$. Puesto que $p \nmid a$, esto implicaría $k + \ell \equiv 0 \pmod{p}$, lo que no es posible dado que $k + \ell \leq 2n = p - 1$.

Entonces, en la lista (1) están n números distintos entre 1 y n, así que son precisamente $1, 2, \ldots, n$ en algún orden. Luego,

$$n! = b_1 \cdots b_r\,(p - c_1) \cdots (p - c_s) \equiv (-1)^s\, b_1 \cdots b_r\, c_1 \cdots c_r \pmod{p}$$

Para la parte derecha, tenemos

$$b_1 \cdots b_r\, c_1 \cdots c_r \equiv a \cdot 2a \cdots na = n!\, a^n \pmod{p}.$$

Entonces,

$$n! \equiv (-1)^s\, n!\, a^n \pmod{p}.$$

Dado que $p \nmid n!$, esto implica

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

Por el criterio de Euler, la parte izquierda es congruente a $\left(\frac{a}{p}\right)$. Esto demuestra la parte 1) del lema.

Para probar la parte 2), hay que ver que los números s y t tienen la misma paridad. Dividiendo ai con resto por p, se obtiene

$$ai = p\,\left\lfloor \frac{ai}{p} \right\rfloor + r, \quad \text{donde } 0 \leq r < p.$$

Entonces,

$$\sum_{1 \leq i \leq n} ai = \sum_{1 \leq i \leq n} p\,\left\lfloor \frac{ai}{p} \right\rfloor + b_1 + \cdots + b_r + c_1 + \cdots + c_s. \tag{2}$$

Recordamos que en la lista

$$b_1, b_2, \ldots, b_r, p - c_1, p - c_2, \ldots, p - c_s$$

están nada más los números $1, \ldots, n$, así que

$$\sum_{1 \leq i \leq n} i = b_1 + \cdots + b_r + (p - c_1) + \cdots + (p - c_s). \tag{3}$$

Ahora restando (3) de (2), se obtiene

$$(a-1)\sum_{1\le i\le n} i = \sum_{1\le i\le n} p\left\lfloor \frac{ai}{p}\right\rfloor - ps + 2\,(c_1+\cdots+c_s).$$

Puesto que p y a son impares por nuestra hipótesis, rediciendo la última ecuación módulo 2, se obtiene

$$s \equiv \sum_{1\le i\le n}\left\lfloor \frac{ai}{p}\right\rfloor \pmod 2.$$

■

8.2. Ejemplo. Para $p = 11$, tenemos $n = 5$.

1) Para $a = 3$, consideremos los números

$$3, 6, 9, 12, 15.$$

Los correspondientes restos de división por 11 son

$$3, 6, 9, 1, 4.$$

Entre estos 6 y 9 son mayores que $11/2$ y por ende $s = 2$. También usando la segunda parte del lema, podemos calcular

$$t = \left\lfloor \frac{3}{11}\right\rfloor + \left\lfloor \frac{6}{11}\right\rfloor + \left\lfloor \frac{9}{11}\right\rfloor + \left\lfloor \frac{12}{11}\right\rfloor + \left\lfloor \frac{15}{11}\right\rfloor = 0+0+0+1+1 = 2.$$

Ambos cálculos nos dan

$$\left(\frac{3}{11}\right) = (-1)^2 = +1.$$

(De hecho, $3 \equiv 5^2 \pmod{11}$.)

2) Para $a = 7$ hay que considerar los números

$$7, 14, 21, 28, 35.$$

Los restos de división por 11 correspondientes son

$$7, 3, 10, 6, 2.$$

Entre estos $7, 6, 10$ son mayores que $11/2$, así que $s = 3$. Por otro lado,

$$t = \left\lfloor \frac{7}{11}\right\rfloor + \left\lfloor \frac{14}{11}\right\rfloor + \left\lfloor \frac{21}{11}\right\rfloor + \left\lfloor \frac{28}{11}\right\rfloor + \left\lfloor \frac{35}{11}\right\rfloor = 0+1+1+2+3 = 7.$$

Estos cálculos nos dan

$$\left(\frac{7}{11}\right) = (-1)^3 = (-1)^7 = -1.$$

En efecto, 7 no es un cuadrado módulo 11; los cuadrados módulo 11 son $\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}$.

▲

8.3. Ejemplo. Notamos que la prueba de la segunda parte del lema usa el hecho de que a sea impar. Por ejemplo, para $p = 11$ y $a = 6$ podríamos calcular

$$t = \left\lfloor \frac{6}{11}\right\rfloor + \left\lfloor \frac{12}{11}\right\rfloor + \left\lfloor \frac{18}{11}\right\rfloor + \left\lfloor \frac{24}{11}\right\rfloor + \left\lfloor \frac{30}{11}\right\rfloor = 0+1+1+2+2 = 6.$$

Esto es un número par, pero 6 *no es* un cuadrado módulo 11. ▲

9 La segunda ley de reciprocidad suplementaria

9.1. Observación. *Sea p un número impar. Entonces, $\frac{p^2-1}{8}$ es par si y solo si $p \equiv \pm 1 \pmod 8$ y es impar si y solo si $p \equiv \pm 3 \pmod 8$.*

Demostración. Los posibles restos de p módulo 8 son $1, 3, 5, 7$. Notamos que $5 \equiv -3$ y $7 \equiv -1 \pmod 8$. Si $p = 8k \pm 1$, entonces

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k \quad \text{es par.}$$

Si $p = 8k \pm 3$, entonces

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1 \quad \text{es impar.}$$

■

9.2. Proposición. *Si p es un primo impar, entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostración. Según el lema de Gauss, hay que considerar los números

$$2, 4, 6, \ldots p-1$$

y contar cuántos de estos son mayores que $p/2$. Notamos que $2k > \frac{p}{2}$ si y solo si $k > \frac{p}{4}$. Entonces, los primeros $\lfloor \frac{p}{4} \rfloor$ números de la lista son menores o iguales que $\frac{p}{2}$, y el resto son mayores que $\frac{p}{2}$. Tenemos entonces

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Nos interesa la paridad de s. Consideremos todos los casos posibles.

- Si $p = 8k + 1$, entonces
$$s = \frac{8k}{2} - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k \quad \text{es par.}$$
- Si $p = 8k + 3$, entonces
$$s = \frac{8k+2}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = 4k + 1 - 2k = 2k + 1 \quad \text{es impar.}$$
- Si $p = 8k + 5$, entonces
$$s = \frac{8k+4}{2} - \left\lfloor \frac{8k+5}{4} \right\rfloor = 4k + 2 - (2k + 1) = 2k + 1 \quad \text{es impar.}$$
- Si $p = 8k + 7$, entonces
$$s = \frac{8k+6}{2} - \left\lfloor \frac{8k+7}{4} \right\rfloor = 4k + 3 - (2k + 1) = 2k + 2 \quad \text{es par.}$$

■

9.3. Ejemplo. Revisemos los restos módulo 8 de los primeros números primos:

p:	3	5	7	11	13	17	19	23	29	31	37	41	$\cdots$
p mód 8:	$+3$	-3	-1	$+3$	-3	$+1$	$+3$	-1	-3	-1	-3	$+1$	$\cdots$

Entonces, los primeros primos módulo cuales 2 es un cuadrado son $7, 17, 23, 31, 41, \ldots$

$$2 \equiv 3^2 \pmod 7, \quad 2 \equiv 6^2 \pmod{17}, \quad 2 \equiv 5^2 \pmod{23},$$
$$2 \equiv 8^2 \pmod{31}, \quad 2 \equiv 17^2 \pmod{41}.$$

▲

Ejercicio 10. *Sea p un primo impar. Demuestre que -2 es un cuadrado módulo p si y solamente si $p \equiv 1$ o $3 \pmod 8$.*

10 La ley de reciprocidad cuadrática

lección 5
29.11.18

La segunda parte del lema de Gauss nos permite deducir el siguiente resultado, que es uno de los más importantes en la teoría de números.

10.1. Teorema (La ley de reciprocidad cuadrática). *Si p y q son diferentes primos impares, entonces*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}$$

Demostración. Del lema de Gauss se sigue que

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

donde

$$t = \sum_{1 \le i \le \frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{1 \le i \le \frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor.$$

Para calcular esta suma, consideremos el conjunto

$$S := \left\{ (i,j) \;\middle|\; 1 \le i \le \frac{p-1}{2},\ 1 \le j \le \frac{q-1}{2} \right\}$$

y sus subconjuntos

$$S_1 := \{(i,j) \in S \mid qi > pj\},$$
$$S_2 := \{(i,j) \in S \mid qi < pj\}.$$

Notamos que $qi \neq pj$, dado que p y q son primos distintos. Entonces, S es la unión disjunta de S_1 y S_2:

$$S = S_1 \cup S_2, \quad S_1 \cap S_2 = \emptyset, \quad |S| = |S_1| + |S_2|.$$

Tenemos claramente

$$|S| = \frac{p-1}{2}\,\frac{q-1}{2}.$$

Por otra parte,

$$|S_1| = \#\left\{(i,j) \in S \;\middle|\; 1 \le i \le \frac{p-1}{2},\ 1 \le j < \frac{qi}{p}\right\} = \sum_{1 \le i \le \frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor,$$

$$|S_2| = \#\left\{(i,j) \in S \;\middle|\; 1 \le j \le \frac{q-1}{2},\ 1 \le i < \frac{pj}{q}\right\} = \sum_{1 \le j \le \frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor,$$

de donde podemos concluir que

$$\sum_{1 \le i \le \frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{1 \le i \le \frac{q-1}{2}} \left\lfloor \frac{pi}{q} \right\rfloor = \frac{p-1}{2}\,\frac{q-1}{2},$$

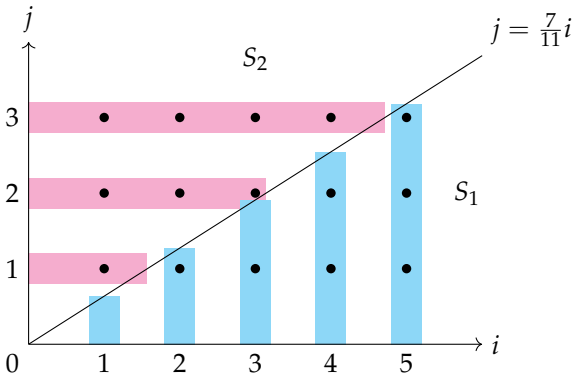
y entonces,

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

■

En "Disquisitiones Arithmeticae" de Gauss se encuentran ocho diferentes pruebas de reciprocidad cuadrática y hoy en día se conocen alrededor de 250 (por supuesto, algunas de estas pruebas usan ideas parecidas).

10.2. Ejemplo. Visualicemos el argumento combinatorio de la última prueba. Por ejemplo, si $p = 11$ y $q = 7$, los conjuntos S_1 y S_2 son los siguientes:



$$|S_1| = \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor = 0+1+1+2+3 = 7,$$

$$|S_2| = \left\lfloor \frac{11}{7} \right\rfloor + \left\lfloor \frac{22}{7} \right\rfloor + \left\lfloor \frac{33}{7} \right\rfloor = 1+3+4 = 8.$$

▲

10.3. Ejemplo. Los cuadrados módulo 7 son $\overline{1}, \overline{2}, \overline{4}$ y los cuadrados módulo 11 son $\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}$. Tenemos entonces

$$\left(\frac{11}{7}\right) = +1, \quad \left(\frac{7}{11}\right) = -1.$$

Tenemos $7 \equiv 11 \equiv 3 \pmod 4$, lo cual concuerda con la ley de reciprocidad cuadrática. ▲

10.4. Ejemplo. Encontremos todos los primos p tales que 3 es un cuadrado módulo p. Excluyendo los casos triviales $p = 2, 3$, tenemos gracias a la ley de reciprocidad cuadrática

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

donde

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4; \end{cases} \quad \left(\frac{p}{3}\right) = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 3, \\ -1, & \text{si } p \equiv 2 \pmod 3. \end{cases}$$

Entonces, el resultado depende del resto de p módulo 12. Si $p \neq 2, 3$, tenemos los siguientes casos:

p mód 12:	1	5	7	11
p mód 4:	1	1	3	3
p mód 3:	1	2	1	2

Luego,

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod{12}, \\ -1, & p \equiv \pm 5 \pmod{12}. \end{cases}$$

He aquí una lista de los restos módulo 12 de los primeros números primos.

p:	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
p mód 12:	5	7	11	1	5	7	11	5	7	1	5	7	11	5	11	1	7	11

Entonces, los primeros primos $p > 3$ tales que 3 es un cuadrado módulo p son $11, 13, 23, 37, 47, 59, 61, 71, \ldots$ Por ejemplo,

$$3 \equiv 5^2 \pmod{11}, \quad 3 \equiv 4^2 \pmod{13}, \quad 3 \equiv 7^2 \pmod{23}.$$

▲

Ejercicio 11. *Demuestre que el polinomio $X^2 + X + 1$ tiene una raíz módulo p si y solo si $p = 3$ o $p \equiv 1 \pmod 3$. (Indicación: use el ejercicio 4.)*

Ejercicio 12. *Sea p un primo impar diferente de 5. Demuestre que 5 es un cuadrado módulo p si y solo si $p \equiv \pm 1, \pm 9 \pmod{20}$. Compruebe este resultado para $p = 11, 19, 29$.*

Ejercicio 13. *Sean p y q dos primos impares. Demuestre que*

1) *si $p \equiv q \pmod{4a}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$;*

2) *si $p \equiv -q \pmod{4a}$, entonces $\left(\frac{a}{p}\right) = \operatorname{sgn} a \cdot \left(\frac{a}{q}\right)$, donde $\operatorname{sgn} a = \pm 1$ es el signo de a.*

(Este resultado es equivalente *a la ley de reciprocidad cuadrática y fue descubierto por Euler en 1744, pero sin prueba.)*

10.5. Ejemplo. He aquí una pequeña tabla de los valores de $\left(\frac{p}{q}\right)$.

p \ q	3	5	7	11	13	17	19	23	29	31
3	0	−	−	+	+	−	−	+	−	−
5	−	0	−	+	−	−	+	−	+	+
7	+	−	0	−	−	−	+	−	+	+
11	−	+	+	0	−	−	+	−	−	−
13	+	−	−	−	0	+	−	+	+	−
17	−	−	−	−	+	0	+	−	−	−
19	+	+	−	−	−	+	0	−	−	+
23	−	−	+	+	+	−	+	0	+	−
29	−	+	+	−	+	−	−	+	0	−
31	+	+	−	+	−	−	−	+	−	0

▲

11 El cálculo del símbolo de Legendre

Resumamos las propiedades del símbolo de Legendre que hemos probado.

0) Si $a' \equiv a \pmod{p}$, entonces
$$\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right).$$

1) El símbolo es multiplicativo: para cualesquiera a, b y todo primo p se cumple
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

2) **La ley de reciprocidad cuadrática**: si p y q son diferentes primos impares, entonces
$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}$$

3) **La primera ley suplementaria**: si p es un primo impar, entonces
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

4) **La segunda ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Estas propiedades nos siguieren que para calcular el símbolo de Legendre $\left(\frac{a}{p}\right)$, se puede factorizar a en números primos:

$$a = \pm 2^k q_1^{k_1} \cdots q_s^{k_s},$$

y luego por la multiplicatividad

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^k \left(\frac{q_1}{p}\right)^{k_1} \cdots \left(\frac{q_s}{p}\right)^{k_s},$$

donde $\left(\frac{\pm 1}{p}\right)$ se calcula mediante la primera ley suplementaria, $\left(\frac{2}{p}\right)$ se calcula mediante la segunda ley suplementaria, y el resto de los símbolos $\left(\frac{q_i}{p}\right)$ pueden ser calculados aplicando la ley de reciprocidad y repitiendo el mismo proceso. Sin embargo, este método no es muy eficaz porque requiere factorización en primos. En la siguiente sección veremos que hay mejor algoritmo.

Veamos algún ejemplo de cálculos del símbolo de Legendre a partir de las propiedades de arriba.

11.1. Ejemplo. El número 2017 es primo. Usando las congruencias

$$2017 \equiv 1 \pmod 4, \quad 2017 \equiv 1 \pmod 3, \quad 2017 \equiv 2 \pmod 5,$$

calculamos a partir de la ley de reciprocidad que

$$\left(\frac{15}{2017}\right) = \left(\frac{3}{2017}\right) \left(\frac{5}{2017}\right) = \left(\frac{1}{3}\right) \left(\frac{2}{5}\right) = (+1)(-1) = -1.$$

Luego 15 no es un cuadrado módulo 2017. De la misma manera podemos calcular

$$\left(\frac{21}{2017}\right) = \left(\frac{3}{2017}\right) \left(\frac{7}{2017}\right) = \left(\frac{1}{3}\right) \left(\frac{1}{7}\right) = +1,$$

y por lo tanto 21 es un cuadrado módulo 2017. Podemos ver con ayuda de una computadora que

$$174^2 \equiv 21 \pmod{2017}.$$

▲

Ejercicio 14. *Demuestre que* $2, 3, 4, 5$ *y* 64 *son todos cuadrados módulo* 241.
Nota: 241 *es primo.*

11.2. Ejemplo. Tenemos

$$\left(\frac{14}{57}\right) = \left(\frac{2}{57}\right) \left(\frac{7}{57}\right).$$

Luego, $57 \equiv 1 \pmod 8$, así que $\left(\frac{2}{57}\right) = +1$. Dado que $57 \equiv 1 \pmod 4$, la reciprocidad cuadrática nos da $\left(\frac{7}{57}\right) = \left(\frac{57}{7}\right) = \left(\frac{1}{7}\right) = +1$. Entonces, $\left(\frac{14}{57}\right) = +1$...

Hay solo un pequeño problema: $57 = 3 \cdot 19$ es un número compuesto, así que el símbolo de Legendre $\left(\frac{14}{57}\right)$ no está definido. En realidad, si 14 fuera un cuadrado módulo 57, este también sería un cuadrado módulo 3, pero $14 \equiv 2 \pmod 3$ no lo es. ▲

12 El símbolo de Jacobi

lección 6
30.11.18

El símbolo de Legendre $\left(\frac{a}{p}\right)$ está definido solamente para p primo. Si en lugar de p tenemos un número compuesto, podemos tratar de aplicar las mismas reglas, pero como vimos en 11.2, esto nos puede llevar a conclusiones equivocadas. Para entender qué está pasando, se introduce la siguiente generalización.

12.1. Definición. Sea $n \geq 3$ un entero impar y a cualquier entero. Sea $n = p_1 p_2 \cdots p_s$ la factorización de n en números primos. Entonces, el **símbolo de Jacobi** $\left(\frac{a}{n}\right)$ está definido como el siguiente producto de símbolos de Legendre:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right).$$

12.2. Observación. *Se tiene* $\left(\frac{a}{n}\right) = \pm 1$ *si y solamente si* $\operatorname{mcd}(a,n) = 1$. *En caso contrario,* $\left(\frac{a}{n}\right) = 0$.

Demostración. Tenemos $\left(\frac{a}{n}\right) = \pm 1$ si y solo si $\left(\frac{a}{p_i}\right) = \pm 1$ para todo i, si y solo si $p_i \nmid a$ para todo i. ■

Entonces, $\left(\frac{a}{n}\right) = 0$ significa nada más que $\operatorname{mcd}(a,n) \neq 1$. En este caso a puede o no puede ser un cuadrado módulo n. Por ejemplo, los cuadrados módulo 9 son $0, 1, 4, 7$. Los números 3 y 6 no son cuadrados módulo 9, aun cuando $\left(\frac{3}{9}\right) = \left(\frac{6}{9}\right) = 0$.

12.3. Observación. *Si* $\left(\frac{a}{n}\right) = -1$, *entonces* a *no es un cuadrado módulo* n.

Demostración. Si $\left(\frac{a}{n}\right) = -1$, entonces entre los símbolos de Legendre correspondientes $\left(\frac{a}{p_i}\right)$ hay por lo menos uno que es igual a -1, así que a no es un cuadrado módulo p_i y en particular a no puede ser un cuadrado módulo n. ■

Por otro lado, si $\left(\frac{a}{n}\right) = +1$, la definición implica que $\left(\frac{a}{p_i}\right) = -1$ para un número par de índices i (posiblemente distinto de cero). Se sigue que $\left(\frac{a}{n}\right) = +1$ *no implica* que a sea un cuadrado módulo n.

12.4. Ejemplo. Volvamos a 11.2 y calculemos correctamente el símbolo de Jacobi $\left(\frac{14}{57}\right)$. Por la definición,

$$\left(\frac{14}{57}\right) := \left(\frac{14}{3}\right)\left(\frac{14}{19}\right).$$

Luego

$$\left(\frac{14}{3}\right) = \left(\frac{2}{3}\right) = -1, \quad \left(\frac{14}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{7}{19}\right).$$

Aquí $\left(\frac{2}{19}\right) = -1$, dado que $19 \equiv 3 \pmod 8$, y por la reciprocidad cuadrática

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = +1.$$

En consecuencia

$$\left(\frac{14}{57}\right) := \left(\frac{14}{3}\right)\left(\frac{14}{19}\right) = (-1)\cdot(-1) = +1.$$

Aunque este símbolo es igual a $+1$, esto no significa que 14 sea un cuadrado módulo 57: de hecho no es cuadrado ni módulo 3, ni módulo 19. ▲

12.5. Ejemplo. He aquí algunos símbolos de Jacobi $\left(\frac{a}{n}\right)$ para $n = 9, 15, 21$. Los valores subrayados corresponden a los casos cuando $\left(\frac{a}{n}\right) = +1$, pero a no es un cuadrado módulo n.

n \ a	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
9	+	0	+	+	0	+	+												
15	+	0	+	0	0	−	+	0	0	−	0	−	−						
21	−	0	+	+	0	0	−	0	−	−	0	−	0	0	+	+	0	−	+

Los cuadrados módulo $9, 15, 21$ son los siguientes:

$$\begin{aligned} n = 9&: \overline{0}, \overline{1}, \overline{4}, \overline{7}, \\ n = 15&: \overline{0}, \overline{1}, \overline{4}, \overline{6}, \overline{9}, \overline{10}, \\ n = 21&: \overline{0}, \overline{1}, \overline{4}, \overline{7}, \overline{9}, \overline{15}, \overline{16}, \overline{18}. \end{aligned}$$

Por ejemplo,

$$\left(\frac{8}{15}\right) := \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)(-1) = +1,$$

aun cuando 8 no es un cuadrado módulo 15. ▲

El símbolo de Jacobi tiene las siguientes propiedades.

12.6. Proposición. *Sean $m, n \geq 3$ enteros impares.*

0) Si $a' \equiv a \pmod{n}$, entonces $\left(\frac{a'}{n}\right) = \left(\frac{a}{n}\right)$.

1) El símbolo es multiplicativo en a y n: para cualesquiera a, b, m, n se cumple

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

2) Si $m \neq n$, entonces

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right) = \begin{cases} +\left(\frac{n}{m}\right), & \text{si } n \equiv 1 \text{ o } m \equiv 1 \pmod 4, \\ -\left(\frac{n}{m}\right), & \text{si } n \equiv 3 \text{ y } m \equiv 3 \pmod 4. \end{cases}.$$

3)

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} +1, & \text{si } n \equiv 1 \pmod 4, \\ -1, & \text{si } n \equiv 3 \pmod 4. \end{cases}.$$

4)

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} +1, & \text{si } n \equiv \pm 1 \pmod 8, \\ -1, & \text{si } n \equiv \pm 3 \pmod 8. \end{cases}.$$

Demostración. Todo esto se sigue de la definición del símbolo de Jacobi y las propiedades correspondientes del símbolo de Legendre. Sea $n = p_1 \cdots p_s$ la factorización de n en primos. Si $a' \equiv a \pmod{n}$, entonces $a' \equiv a \pmod{p_i}$ para todo i, y entonces

$$\left(\frac{a'}{n}\right) := \left(\frac{a'}{p_1}\right) \cdots \left(\frac{a'}{p_s}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_s}\right) =: \left(\frac{a}{n}\right).$$

Esto establece la parte 0). Para la parte 1), notamos que

$$\left(\frac{ab}{n}\right) := \left(\frac{ab}{p_1}\right)\cdots\left(\frac{ab}{p_s}\right) = \left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_s}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_s}\right) =: \left(\frac{a}{n}\right)\left(\frac{b}{n}\right),$$

y de la misma manera, si $m = q_1 \cdots q_t$, entonces $mn = q_1 \cdots q_t\, p_1 \cdots p_s$

$$\left(\frac{a}{mn}\right) := \left(\frac{a}{q_1}\right)\cdots\left(\frac{a}{q_t}\right)\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_s}\right) =: \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

Las partes 2), 3), 4) se demuestran por inducción sobre el número de los primos en las factorizaciones

$$m = q_1 \cdots q_t \quad \text{y} \quad n = p_1 \cdots p_s.$$

Podemos asumir que $\operatorname{mcd}(m, n) \neq 1$ porque en caso contrario

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

La base de inducción es el caso cuando $s = t = 1$. Esto corresponde a la ley de reciprocidad cuadrática

$$\left(\frac{q_1}{p_1}\right) = (-1)^{\frac{q_1-1}{2}\,\frac{p_1-1}{2}}\left(\frac{p_1}{q_1}\right).$$

Para el paso inductivo, si $t > 1$, escribamos

$$m' = q_1 \cdots q_{t-1}, \quad m = m' q_t.$$

Luego, por la multiplicatividad y la hipótesis de inducción

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

Tenemos que probar que

$$(-1)^{\frac{m'-1}{2}\,\frac{n-1}{2}}\,(-1)^{\frac{q_t-1}{2}\,\frac{n-1}{2}} \stackrel{?}{=} (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}.$$

Por ejemplo, se pueden considerar todos los casos posibles $m', n, q_t \equiv \pm 1 \pmod 4$; dejo los detalles al lector. De la misma manera, si $s > 1$, podemos escribir

$$n' = p_1 \cdots p_{s-1}, \quad n = n' p_s$$

y luego

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

y se comprueba que este número es igual a $(-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}$.

La parte 3) se demuestra de la misma manera. Escribamos $n = p_1 \cdots p_s$. Si $s = 1$, ya sabemos que $\left(\frac{-1}{p_1}\right) = (-1)^{\frac{p_1-1}{2}}$. Esto sería la base de inducción. Si $s > 1$, pongamos $n' := p_1 \cdots p_{s-1}$. Luego, por la hipótesis de inducción

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{n'}\right)\left(\frac{-1}{p_s}\right) = (-1)^{\frac{n'-1}{2}}\,(-1)^{\frac{p_s-1}{2}},$$

y se ve que

$$(-1)^{\frac{n'-1}{2}}\,(-1)^{\frac{p_s-1}{2}} = (-1)^{\frac{n-1}{2}}$$

—dado que $n = n'\, p_s$, en particular $n \bmod 4 = (n' \bmod 4) \cdot (p_s \bmod 4)$.

La parte 4) es similar y la dejo como un ejercicio para el lector. ■

Ejercicio 15. *Complete los detalles de la demostración anterior.*

12.7. Ejemplo. Ya que $21 \equiv 1 \pmod 4$, tenemos $\left(\frac{21}{2017}\right) = \left(\frac{2017}{21}\right)$. Luego, $2017 \equiv 1 \pmod{21}$, y por lo tanto $\left(\frac{2017}{21}\right) = \left(\frac{1}{21}\right) = +1$. Aunque hemos usado las propiedades del símbolo de Jacobi, $\left(\frac{21}{2017}\right)$ es un símbolo de Legendre legítimo, y el resultado de este calculo nos permite concluir que 21 es un cuadrado módulo 2017. ▲

12.8. Ejemplo. Calculemos $(\frac{30}{127})$. No podemos relacionar este símbolo con $\left(\frac{127}{30}\right)$ porque 30 es par. Sin embargo, podemos escribir

$$\left(\frac{30}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{15}{127}\right).$$

Luego, $127 \equiv 7 \pmod 8$, así que $(\frac{2}{127}) = +1$. También $127 \equiv 3 \pmod 4$ y $15 \equiv 3 \pmod 4$, y la ley de reciprocidad para el símbolo de Jacobi nos dice que

$$\left(\frac{15}{127}\right) = -\left(\frac{127}{15}\right) = -\left(\frac{7}{15}\right) = +\left(\frac{15}{7}\right) = \left(\frac{1}{7}\right) = +1.$$

Entonces, $(\frac{30}{127}) = +1$. ▲

El último ejemplo explica la utilidad del símbolo de Jacobi: para calcular el símbolo de Legendre $\left(\frac{a}{p}\right)$ no hace falta factorizar a en números primos; se puede aplicar la reciprocidad para los símbolos de Jacobi. La única parte problemática es que tenemos que sacar un posible factor 2^k cuando a es par. *Se supone* que no existe ningún algoritmo eficaz de factorización de un número en primos (en esta conjetura se basa una gran parte de la criptografía aplicada en la vida cotidiana), pero el factor 2^k se encuentra fácilmente. Módulo este pequeño detalle, el cálculo del símbolo de Jacobi consiste en reducciones consecutivas de un número módulo otro. Esto es algo similar al algoritmo de Euclides.

Ejercicio 16. *Calcule el símbolo de Legendre* $(\frac{598}{977})$ *usando las propiedades del símbolo de Jacobi (sin factorizar* 598*). Puede usar el hecho de que el número* 977 *es primo y* $977 \equiv 1 \pmod 8$.