UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

La Función de Euler y el Teorema de Fermat

Alan Reyes-Figueroa

Teoría de Números (Aula 10) 12.agosto.2021

La Función de Euler

Definición

Diremos que los números enteros $b_1, b_2, \ldots, b_k$ forman un ***sistema completo de invertibles*** *módulo n si*

$$\{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k\} = (\mathbb{Z}/n\mathbb{Z})^* = U(n).$$

En otras palabras, $b_1, b_2, \ldots, b_k$ forman un sistema completo de invertibles, si todas las clases de congruencia invertibles, módulo n, están representadas en los b_i. Equivalente, eso ocurre si y sólo si los b_i satisfacen $(b_i, n) = 1$, $\forall i$, y $b_i \equiv b_j \pmod{n} \Rightarrow i = j$.

El conjunto $\{k \in \mathbb{Z} : \ 1 \leq k \leq n, \ (k, n) = 1\}$ se llama el sistema de invertibles **canónico** módulo n.

Estamos interesados en saber la cardinalidad de $U(n)$.

Definición

La función $\varphi : \mathbb{Z}^+ \to \mathbb{Z}$, dada por $\varphi(n) = |U(n)|$, se llama ***función φ de Euler****.*

La Función de Euler

Alternativamente, podemos definir a la función de Euler como

$$\varphi(n) = \#\{k : 1 \leq k \leq n : (k, n) = 1\}.$$

Algunas observaciones:

- $\varphi(1) = \varphi(2) = 1$.
- Para $n > 2$, se tiene que $1 < \varphi(n) < n$ (1 y $n - 1$ son primos relativos con n).
- Si p es primo, entonces $\varphi(p) = p - 1$.
- Si p es primo, entonces $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

  Prueba: Para mostrar esta afirmación, basta ver que si $1 \leq a \leq p^k$, $(a, p^k) = 1$ si y sólo si, a no es múltiplo de p; y hay precisamente p^{k-1} múltiplos de p en el intervalo $1 \leq a \leq p^k$.
- Para calcular la función φ en el caso general, vamos a mostrar antes una propiedad útil de esta función.

Proposición

Sean $m, n \in \mathbb{Z}^+$ tales que $(m, n) = 1$. Entonces $\varphi(mn) = \varphi(m)\varphi(n)$.
Esto es, φ es una función multiplicativa.

Prueba: Consideramos los números $1, 2, \ldots, mn$, con $(m, n) = 1$ y los colocamos en forma matricial como sigue:

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \ldots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \ldots & mn \end{array}$$

Como $(m + j, n) = (j, n)$, si un número en esta table es primo relativo con n, entonces todos los números en esa columna son primos relativos con n. De ahí, existen $\varphi(n)$ columnas con elementos primos relativos con n.

La Función de Euler

Por otro lado, toda columna posee un sistema completo de residuos módulo m: si dos entradas i_1, i_2 son tales que $ni_1 + j \equiv ni_2 + j \pmod{m}$, entonces $i_1 \equiv i_2 \pmod{m}$. (Aquí se usa el hecho que n es invertible módulo m)

Así, en cada columna existen $\varphi(m)$ números que son primos relativos con m, y portanto la cantidad de números que son simultáneamente primos relativos con n y con m es $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Obs! La propiedad anterior se generaliza: $\varphi(n_1 n_2 \cdots n_r) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_r)$, si los n_i son coprimos a pares. Basta aplicar inducción.

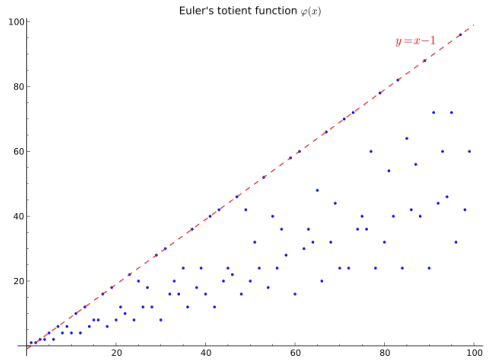
La conclusión de la proposición anterior es que tenemos un método sistemático para hallar $\varphi(n)$ para cualquier $n \in \mathbb{N}$. Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factoración en primos de n. Como $(p_i^{k_i}, p_j^{k_j}) = 1$ para $i \neq j$, entonces

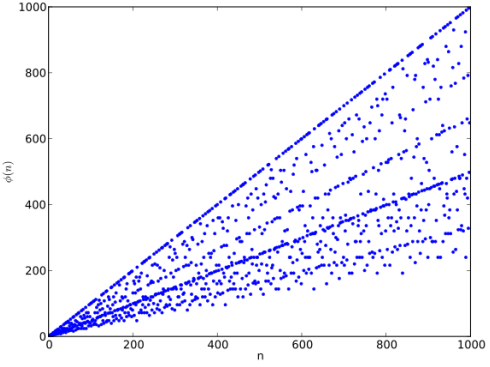
$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

La Función de Euler

Ejemplo: Hallar $\varphi(372)$. Como $372 = 2^2 \cdot 3 \cdot 31$, entonces

$$\varphi(372) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(31) = 2(1) \cdot 2 \cdot 30 = 120.$$





Valores para la función φ de Euler.

Teorema (Teorema de Euler-Fermat)

Sean $a, n \in \mathbb{Z}$, $n > 1$ dos enteros tales que $(a, n) = 1$. Entonces

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

Prueba: Observe que si $r_1, r_2, \ldots, r_{\varphi(n)}$ es un sistema completo de invertibles módulo n, y si $(a, n) = 1$, entonces también $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ es un sistema completo de invertibles módulo n. De hecho, tenemos que $(ar_i, n) = 1$, y si $ar_i \equiv ar_j \pmod{n}$, entonces podemos cancelar a para obtener $r_i \equiv r_j \pmod{n}$. Luego $r_i = r_j$, y portanto $i = j$.

En consecuencia, cada ar_i debe ser congruente con algún r_j, y

$$\prod_{i=1}^{\varphi(n)} ar_i \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n} \quad \Longrightarrow \quad a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}.$$

Como los r_i son invertibles módulo n, también el producto $\prod_i r_i$ es invertible. Simplificanto este factor, resulta $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Teorema (Pequeño Teorema de Fermat)

Sean $a \in \mathbb{Z}$, y p un número primo. Entonces

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

Prueba: Si $p \mid a$, el resultado es inmediato, pues $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$.
En el caso $p \nmid a$, entonces $(a, p) = 1$. Como $\varphi(p) = p - 1$, del Teorema de Euler-Fermat, tenemos que $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$. $\square$

Obs! El Teorema de Euler-Fermat también puede probarse utilizando el Teorema de Lagrange para grupos: si G es un grupo finito, y $g \in G$, entonces $g^{|G|} = 1$.
Aplicando esto en el caso $G = U(n)$, con $|G| = \varphi(n)$, se tiene que para $a \in U(n)$

$$a^{\varphi(n)} \equiv a^{|U(n)|} \equiv 1 \pmod{n}.$$

Dado un entero n, con factoración en primos de la forma $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, consideramos el número

$$M = [\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})] = mmc[\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})].$$

La Función de Euler

El Teorema de Euler puede ser optimizado de la siguiente forma

Proposición

Sean $a, n \in \mathbb{Z}$, $n > 1$ dos enteros tales que $(a, n) = 1$, y n se factora de la forma $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Entonces

$$a^M \equiv 1 \pmod{n}. \qquad \textit{donde} \quad M = [\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})].$$

Prueba: Por el Teorema de Euler-Fermat, sabemos que $a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$, para todo $i = 1, 2, \ldots, r$. Elevando la congruencia anterior al exponente $M/\varphi(p_i^{k_i})$, obtenemos

$$a^M \equiv 1 \pmod{p_i^{k_i}}, \qquad \text{para } i = 1, 2, \ldots, r.$$

Así, $a^M - 1$ es múltiplo de $p_i^{k_i}$, para todo $i = 1, 2, \ldots, r$, y como estos números son coprimos dos a dos, se tiene que $n \mid a^M - 1 \Rightarrow a^M \equiv 1 \pmod{n}$. □

Aplicaciones

El teorema de Euler-Fermat tiene muchas aplicaciones y es fundamental para gran parte de lo que se hace en teoría de números.

Cálculo de potencias: Como mínimo, puede ser un dispositivo que ahorra trabajo en ciertos cálculos.

Ejemplo: Se pide hallar $5^{38} \pmod{11}$.

Como $\varphi(11) = 10$, y $(5, 11) = 1$ entonces del Teorema de Euler-Fermat, sabemos que $5^{10} \equiv 1 \pmod{11}$. Así

$$5^{38} \equiv 5^{3(10)+8} \equiv (5^{10})^3 \cdot 5^8 \equiv (1)^3 \cdot 5^8 \equiv 5^8 \equiv (5^2)^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Ejemplo: Calcular $7^{91} \pmod{100}$.

Sabemos que $100 = 2^2 \cdot 5^2$. Entonces $\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 2(1) \cdot 5(4) = 2 \cdot 20 = 40$.

Como $(7, 100) = 1$, por el Teorema de Euler-Fermat tenemos que $7^{40} \equiv 1 \pmod{100}$. Entonces

$$7^{91} \equiv 7^{2(40)+11} \equiv (7^{40})^2 \cdot 7^{11} \equiv 7^{11} \pmod{100}.$$

Aplicaciones

Ahora calculamos $7^{11} \pmod{100}$ usando el algoritmo de exponenciación binaria: Observe que $11 = 2^3 + 2^1 + 2^0 = (1011)_2$. Entonces

$$\begin{aligned} 7^1 &\equiv 7 \pmod{100}, \\ 7^2 &\equiv 49 \pmod{100}, \\ 7^4 &\equiv 49^2 \equiv 2401 \equiv 1 \pmod{100}, \\ 7^8 &\equiv 1^2 \equiv 1 \pmod{100}. \end{aligned}$$

De ahí que

$$7^{91} \equiv 7^{11} \equiv 7^8 \cdot 7^2 \cdot 7^1 \equiv 1 \cdot 49 \cdot 7 \equiv 343 \equiv 43 \pmod{100}.$$

Aplicaciones

Ejemplo: Existen infinitos números enteros de la forma $2000\ldots0009$, que son múltiplos de 2009.

Observe primero que el problema es equivalente a encontrar infinitos valores de $k \in \mathbb{N}$ tales que $2 \cdot 10^k + 9 \equiv 0 \pmod{2009}$.
Pero

$$\begin{aligned} 2 \cdot 10^k + 9 \equiv 0 \pmod{2009} &\iff 2 \cdot 10^k + 9 \equiv 2009 \pmod{2009} \\ &\iff 2 \cdot 10^k \equiv 2000 \pmod{2009} \\ &\iff 10^k \equiv 1000 \equiv 10^3 \pmod{2009} \\ &\iff 10^{k-3} \equiv 1 \pmod{2009}, \end{aligned}$$

ya que $(2, 2009) = 1$ y $(1000, 2009) = 1$.

Como $(10, 2009) = 1$, por el Teorema de Euler-Fermat, tenemos que $10^{\varphi(2009)} \equiv 1 \pmod{2009}$, esto implica que $10^{t\varphi(2009)} \equiv 1^t \equiv 1 \pmod{2009}$, para todo $t \in \mathbb{N}$.
Basta entonces hacer $k - 3 = t(2009)$, de modo que cualquier número de la forma $n = 2 \cdot 10^{3+t\varphi(2009)} + 9$, $t \in \mathbb{N}$, satisface la condición requerida.

Aplicaciones

Ejemplo: No existen soluciones enteras para la ecuación $x^3 \equiv 2 \pmod{103}$.

Observe que 103 es primo. Entonces $\varphi(103) = 102$.

Supongamos que existe una solución $x \in \mathbb{Z}$ de $x^3 \equiv 2 \pmod{103}$. En particular, $103 \nmid x$.

Elevando ambos lados de la congruencia anterior a $\varphi(103)/3 = \frac{102}{3} = 34$, obtenemos

$$(x^3)^{34} \equiv x^{102} \equiv x^{\varphi(103)} \equiv 1 \pmod{103},$$

debido al Teorema de Euler-Fermat.

Por otro lado,

$$(x^3)^{34} \equiv 2^{34} \equiv (2^{14})^2 \cdot 2^6 \equiv (7)^2 \cdot 64 \equiv 49 \cdot 64 \equiv 3136 \equiv 46 \pmod{103},$$

lo que es una contradicción, pues $1 \not\equiv 46 \pmod{103}$.
Portanto, no existe tal solución.

Test de Primalidad de Fermat

Tests de primalidad: Otro uso del teorema de Euler-Fermat es como herramienta para probar la primalidad de un determinado entero n.
En este caso aplicamos el Pequeño Teorema de Fermat. Si pudiera demostrarse que la congruencia $a^n \equiv a \pmod{n}$ no se cumple para alguna elección de a, entonces n debe ser necesariamente compuesto.

Como ejemplo, veamos $n = 117$. El cálculo se mantiene bajo control si seleccionando un entero pequeño para a, digamos, $a = 2$.

Como $2^7 \equiv 128 \equiv 11 \pmod{117}$, resulta

$$2^{117} \equiv 2^{7(16)+5} \equiv (2^7)^{16} \cdot 2^5 \equiv 11^{16} \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

Pero $2^{21} \equiv (2^7)^3 \equiv 11^3 \pmod{117}$, lo que conduce a

$$2^{117} \equiv 2^{21} \equiv 11^3 \equiv (11)^2 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \not\equiv 1 \pmod{117}.$$

Esto muestra que 117 no es primo. De hecho, $117 = 3^2 \cdot 13$.

Test de Primalidad de Fermat

El Recíproco de Teorema de Fermat, no vale, esto es, si $a^{n-1} \equiv 1 \pmod{n}$, para algún entero a, no necesariamente n es primo.
Para ver esto, precisamos del siguiente lema:

Lema

Si p y q son primos distintos, y $a^p \equiv a \pmod{q}$, $a^q \equiv a \pmod{p}$, entonces $a^{pq} \equiv a \pmod{pq}$.

Prueba: Del Pequeño Teorema de Fermat, tenemos que $(a^q)^p \equiv a^q \pmod{p}$. Además, por hipótesis $a^q \equiv a \pmod{p}$. Combinando estas congruencias, se tiene $a^{pq} \equiv a \pmod{p}$. Análogamente, se muestra que $a^{pq} \equiv a \pmod{q}$.

Esto muestra que $p \mid a^{pq} - a$ y $q \mid a^{pq} - a$. Como p y q son primos distintos, entonces $pq \mid a^{pq} - a$, de modo que $a^{pq} \equiv a \pmod{pq}$. $\square$

Test de Primalidad de Fermat

Ejemplo: Vamos a mostrar que $2^{340} \equiv \pmod{341}$.

Observe que $2^{10} \equiv 1024 \equiv 31 \cdot 33 + 1$. Por lo tanto,

$$2^{11} \equiv 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31},$$

y

$$2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot (1)^3 \equiv 2 \pmod{11}.$$

Explotando el lema, $2^{341} \equiv 2^{11 \cdot 31} \equiv 2 \pmod{341}$, de modo que al cancelar un factor 2, obtenemos $2^{340} \equiv 1 \pmod{341}$, y el recíproco del Teorema de Fermat es falso.

Los matemáticos chinos hace 25 siglos afirmaban que n es primo si y sólo si $n \mid 2^n - 2$ (de hecho, este criterio evale para $n \leq 340$). Nuestro ejemplo de $n = 341$ es el contraejemplo (descubierto en 1819).
La situación en la que $n \mid 2^n - 2$, sin n ser primo, ocurre con suficiente frecuencia. Un entero compuesto n se llama **pseudoprimo** siempre que $n \mid 2^n - 2$. Hay infinitos pseudoprimos, por ejemplo: 341, 561, 645 y 1105.

Test de Primalidad de Fermat

Definición

De manera más general, un entero compuesto n para el cual $a^n \equiv a \pmod{n}$ *se llama un* ***pseudoprimo*** *en la base a. (Cuando* $a = 2$*, simplemente se dice que n es un pseudoprimo).*

Ejemplo: 91 es el menor pseudoprimo para la base 3, mientras que 217 es el menor pseudoprimo en la base 5.

Observaciones:

- Se ha demostrado (1903) que hay infinitos pseudoprimos para cualquier base dada.
- Estos “primos impostores” son mucho más raros que los verdaderos primos. De hecho, hay sólo 247 pseudoprimos menores de un millón, en comparación con 78,498 primos.
- El primer ejemplo de un pseudoprimo par, a saber, el número 161,038 = $2 \cdot 73 \cdot 1103$ fue encontrado en 1950.

Test de Primalidad de Fermat

El **test de primalidad de Fermat** es un algoritmo probabilístico que hace uso del Pequeño Teorema de Fermat.

Resulta que el recíproco de este teorema suele (con alta probabilidad) ser verdad: si p es compuesto, entonces a^{p-1} es poco probable que sea congruente con $1 \pmod{p}$ para un valor arbitrario de a. Sin embargo, los pseudoprimos fallan este test.

Idea: Tome $a \in \mathbb{Z}$, $(a, n) = 1$ al azar. Si $a^{n-1} \equiv 1 \pmod{n}$, entonces n tiene alta probabilidad de ser primo.

Observe que si $a = 1$, la congruencia $a^{n-1} \equiv a \pmod{n}$ es trivial. También la congruencia $a^{n-1} \equiv a \pmod{n}$ se satisface de forma trivial si $a = n - 1$, y n es impar.
Por esta razón, usualmente se elige un candidato $1 < a < n - 1$.

Cualquier a que satisface $a^{n-1} \equiv a \pmod{n}$ cuando n es compuesto se llama un **mentiroso de Fermat** (*Fermat liar*). En este caso n es un pseudoprimo para la base a.
Si elegimos a tal que $a^{n-1} \not\equiv a \pmod{n}$, a se llama un **testigo de Fermat** (*Fermat witness*) para la no primalidad de n.

Test de Primalidad de Fermat

Algoritmo: (Test de Primalidad de Fermat)
Inputs: $n \in \mathbb{Z}^+$, $n > 3$, un entero a testar su primalidad, k número de réplicas del test.
Output: o si n es compuesto, en caso contrario responde, primo con alta probabilidad.
`For` $i = 1, 2, \ldots, k$:
    `Pick` a `randomly in the range` $[2, n-2]$.
    `If` $a^{n-1} \not\equiv 1 \pmod{n}$: `then return` o.
`return probably prime`.

El Test de Fermat es muy simple, sin embargo tiene fallas.

Existen números compuestos n que son pseudoprimos para cada base a; es decir, $a^{n-1} \equiv 1 \pmod{n}$, para todos los enteros a con $(a, n) = 1$.
Estos números se conocen como **números de** CARMICHAEL (descubiertos en 1910).

El menor de estos números excepcionales es $561 = 3 \cdot 11 \cdot 17$. Carmichael indicó otros tres: $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$ y $15841 = 7 \cdot 31 \cdot 73$. Dos años más tarde presentó 11 adicionales.

Test de Primalidad de Fermat

Para ver que $561 = 3 \cdot 11 \cdot 17$ es un número de Carmichael, un pseudoprimo absoluto, observe que $(a, 561) = 1$ prodcuce

$$(a, 3) = 1, \quad (a, 11) = 1, \quad (a, 17) = 1.$$

Aplicando el Teorema de Euler-Fermat, obtenemos las congruencias

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17},$$

que a su vez producen

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv (1)^{280} \equiv 1 \pmod{3}, \\ a^{560} &\equiv (a^{10})^{56} \equiv (1)^{56} \equiv 1 \pmod{11}, \\ a^{560} &\equiv (a^{16})^{35} \equiv (1)^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Siendo 3, 11 y 17 primos, esto da lugar a la congruencia $a^{560} \equiv 1 \pmod{561}$, siempre que $(a, 561) = 1$. Así, 561 es un número de Carmichael.