Aritmética Modular

Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 14) 23.septiembre.2021

Algoritmo de Euclides

Algoritmo: (de Euclides para calcular el MDC). *Inputs*: $a, b \in \mathbb{N}$ números naturales. *Outputs*: (a, b) el máximo divisor común de a y b.

```
int gcd(a, b):
    if (a == 0):
        return b
    else:
        return gcd(b% a, a).
```

Algoritmo de Euclides

Algoritmo: (Extendido de Euclides para calcular el $(a, b) = xa + yb$).
Inputs: $a, b \in \mathbb{N}$ números naturales.
Outputs: $d = (a, b)$ el máximo divisor común de a y b,
$x, y =$ enteros tales que $(a, b) = xa + yb$.

```
int gcdExtended(a, b):
    if (a == 0):
        x = 0
        y = 1
        return b, x, y
    else:
        d, x1, y1 = gcdExtended(b% a, a)
        x = y1 - (b/a)*x1
        y = x1
        return d, x, y
```

Inversos Módulo n

Recordemos que los elementos de $U(n)$ son los elementos invertibles módulo n, esto es, aquellos que satisfacen $(a, n) = 1$.

Ejemplo: ¿Cuál es el inverso de 2 módulo n? $(n, 2) = 1$.

Respuesta: $\frac{n+1}{2}$.
Basta ver que

$$2 \cdot \frac{n+1}{2} = \frac{2n+2}{2} = n + 1 \equiv 1 \pmod{n}.$$

Pregunta: ¿Cómo calcular inversos módulo n?
Usamos la propiedad de Bezout:

$$\begin{aligned} (a, n) = 1 \quad \Longrightarrow \quad & \text{existen } x, y \in \mathbb{Z} \text{ con } ax + ny = 1 \\ & ax \equiv 1 \pmod{n}. \end{aligned}$$

Así, x es el inverso de a módulo n.

Podemos entonces usar el algoritmo extendido de Euclides para calcular este inverso x

Inversos Módulo n

Algoritmo: (Inversos módulo n). *Inputs*: $a, n \in \mathbb{N}$ números naturales, con $n > 1$ y $(a, n) = 1$.
Outputs: a^{-1} el inverso de a módulo n.

```
int inverseMod(a, n):
    Compute d, x, y = gcdExtended(a, n),
    if (d == 1):
        return x % n
    else:
        return Error or display "not invertible".
```

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

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

Ejemplos:

$\varphi(1) = 1$	$\varphi(11) = 10$	$\varphi(21) = 12$	$\varphi(31) = 30$
$\varphi(2) = 1$	$\varphi(12) = 4$	$\varphi(22) = 10$	$\varphi(32) = 16$
$\varphi(3) = 2$	$\varphi(13) = 12$	$\varphi(23) = 22$	$\varphi(33) = 20$
$\varphi(4) = 2$	$\varphi(14) = 6$	$\varphi(24) = 8$	$\varphi(34) = 16$
$\varphi(5) = 4$	$\varphi(15) = 8$	$\varphi(25) = 20$	$\varphi(35) = 24$
$\varphi(6) = 2$	$\varphi(16) = 8$	$\varphi(26) = 12$	$\varphi(36) = 12$
$\varphi(7) = 6$	$\varphi(17) = 16$	$\varphi(27) = 18$	$\varphi(37) = 36$
$\varphi(8) = 4$	$\varphi(18) = 6$	$\varphi(28) = 12$	$\varphi(38) = 18$
$\varphi(9) = 6$	$\varphi(19) = 18$	$\varphi(29) = 28$	$\varphi(39) = 24$
$\varphi(10) = 4$	$\varphi(20) = 8$	$\varphi(30) = 8$	$\varphi(40) = 16$

La Función de Euler

Algunas propiedades de la función φ:

1. $\varphi(1) = \varphi(2) = 1$.
2. Para $n > 2$, se tiene que $1 < \varphi(n) < n$ (1 y $n-1$ son primos relativos con n).
3. Si p es primo, entonces $\varphi(p) = p - 1$.
4. Si p es primo, entonces $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.
5. Si $m, n \in \mathbb{Z}^+$ tales que $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

A partir de las propiedades 3, 4, y 5, 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

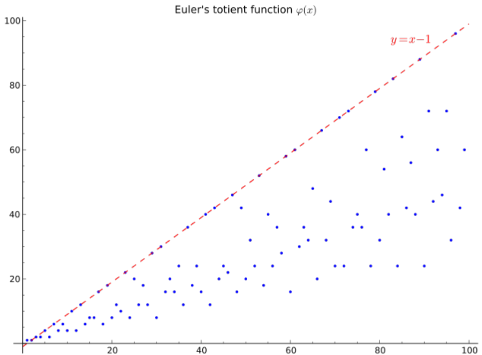
$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1) = \prod_{i=1}^{r} p^{k_i}\Big(\frac{p_i - 1}{p_i}\Big) = n \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

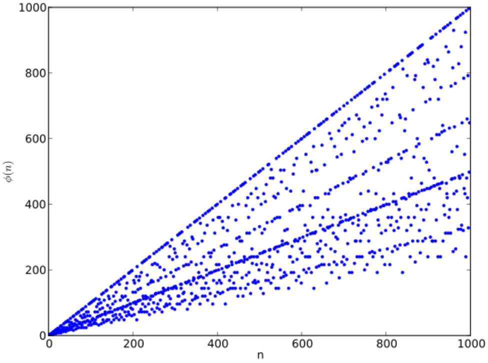
UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

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

Ejemplos:

- $n = 5, a = 3$. Tenemos $\varphi(n) = \varphi(5) = 5 - 1 = 4$. Luego
$$3^{\varphi(5)} = 3^4 = 81 \equiv 1 \pmod{5}.$$
- $n = 12, a = 7$. Tenemos $\varphi(n) = \varphi(12) = \varphi(3)\varphi(4) = 4$. Luego
$$7^{\varphi(12)} = 7^4 = 2401 \equiv 1 \pmod{12}.$$

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.

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: 0 si n es compuesto, en caso contrario responde, primo con alta probabilidad.

```
For i = 1, 2, ..., k:
    Pick a randomly in the range [2, n − 2].
    If a^(n−1) ≢ 1 (mod n): then return 0.
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.