-La función de Euler-

Anteriormente calculamos el resto de dividir 2^{7541} por 7. Vimos que la idea era encontrar un exponente k tal que $2^k \equiv 1 \pmod 7$. En este caso, se puede tomar $k = 3$. Luego, como $7541 = 3 \cdot 2513 + 2$, tenemos

$$2^3 \equiv 1 \pmod 7 \Rightarrow (2^3)^{2513} \equiv 1 \pmod 7$$
$$\Rightarrow 2^{3 \cdot 2513} \equiv 1 \pmod 7$$
$$\Rightarrow 2^2 \cdot 2^{3 \cdot 2513} \equiv 2^2 \pmod 7$$
$$\Rightarrow 2^{3 \cdot 2513 + 2} \equiv 4 \pmod 7$$
$$\Rightarrow 2^{7541} \equiv 4 \pmod 7.$$

El problema general consiste en calcular restos de números de la forma a^n al ser divididos por m. Bajo ciertas condiciones, es posible hallar $k < n$ tal que $a^k \equiv 1 \pmod m$. A saber, $mcd(a, m) = 1$ es una condición suficiente. Bajo esta suposición, podemos hallar al menos un valor de k tal que $a^k \equiv 1 \pmod m$. Veremos que

$$k = \#\text{ de números entre } 0 \text{ y } m \text{ coprimos con } m.$$

La cantidad anterior se conoce como función de Euler evaluada en m.

Definición: Sea $m \in \mathbb{Z}^+$ y considere el conjunto

$$A_m = \{ k \in \mathbb{Z}^+ / \; k \leq m \text{ y } mcd(k, m) = 1 \}.$$

Se define $\varphi(m)$ como el número

$$\varphi(m) := Card(A_m).$$

Es decir, $\varphi(m)$ es la cantidad de números naturales menores que m y copnimos con m.

Lo anterior define una función

$$\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$
$$m \longmapsto \varphi(m)$$

conocida como la **función φ de Euler**.

Antes de probar que $a^{\varphi(m)} \equiv 1 \pmod{m}$ si $mcd(a, m) = 1$, estudiaremos varias propiedades de φ, orientadas a cómo calcular $\varphi(m)$ de manera óptima. Comencemos viendo algunos ejemplos.

Ejemplo:
$\varphi(2) = 1$
$\varphi(3) = 2$
$\varphi(4) = 2$
$\varphi(5) = 4$
$\varphi(6) = 2$
$\varphi(7) = 6$
$\varphi(8) = 4$

Podemos observar que si p es primo, entonces

$$\varphi(p) = p - 1.$$

Sabemos de manera precisa cuánto vale φ en los números que son los bloques de construcción de cualquier número m. Por otro lado, recuerde que

$$m = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$$

donde $p_1 < p_2 < \cdots < p_n$ son primos y $d_1, d_2, \ldots, d_n \in \mathbb{Z}^+$. Entonces, si hallamos una fórmula para calcular cada $\varphi(p_i^{d_i})$, y si además sabemos cómo se comporta φ respecto a la multiplicación, sabremos cómo calcular $\varphi(m)$ para cualquier m.

Proposición: Si p es primo y $d \in \mathbb{Z}^+$, entonces

$$\varphi(p^d) = p^{d-1}(p-1).$$

· Demostración: Sea $n \in \mathbb{Z}^+$ con $n \leq p^d$. Como p es primo, se tiene que

$$\text{mcd}(n, p^d) = 1 \iff p \nmid n.$$

Entonces, $\varphi(p^d) = \text{Card}(\{n \in \mathbb{Z}^+ / n \leq p^d \text{ y } p \nmid n\})$

$$= p^d - \text{Card}(\{n \in \mathbb{Z}^+ / n \leq p^d \text{ y } n \text{ múltiplo de } p\})$$

Entre 1 y p^d, hay exactamente p^{d-1} números divisibles por p, los cuales son

$$p, 2p, \ldots, (p-1)p, p^2, 2p^2, \ldots, p^{d-1}p.$$

Por lo tanto,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1). \blacksquare$$

Propiedad multiplicativa: Si $\text{mcd}(m,n)=1$, entonces

$$\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n).$$

· Demostración: Recuerde que si A y B son conjuntos, entonces

$$\text{Card}(A\times B) = \text{Card}(A)\cdot\text{Card}(B).$$

Luego, bastaría construir una biyección entre A_{mn} y $A_m \times A_n$, ya que en tal caso se tendría

$$\varphi(mn) = \text{Card}(A_{mn}) = \text{Card}(A_m\times A_n) = \text{Card}(A_m)\cdot\text{Card}(A_n) = \varphi(m)\cdot\varphi(n).$$

Construyamos ahora una biyección

$$f: A_{mn} \longrightarrow A_m \times A_n.$$

Sea $k\in A_{mn}$. Luego, $k\in\mathbb{Z}^+$ es tal que $k\leq mn$ y $\text{mcd}(k,mn)=1$. Por el teorema de la división entera, existen $0\leq a<m$ y $0\leq b<n$ tales que

$$k\equiv a \pmod m \quad \text{y} \quad k\equiv b \pmod n.$$

Veamos que $\text{mcd}(a,m)=1$. Como $\text{mcd}(k,mn)=1$, tenemos por el teorema de Bézout que existen

$x_0, y_0 \in \mathbb{Z}$ tales que $kx_0 + mny_0 = 1$. Por otro lado, $k = a + qm$ para algún $q \in \mathbb{Z}$. Luego,

$$1 = kx_0 + mny_0 = (a + qm)x_0 + mny_0 = ax_0 + m(qx_0 + ny_0)$$
$$1 = ax_0 + m(qx_0 + ny_0).$$

De nuevo, por el teorema de Bézout, la igualdad anterior implica que $\text{mcd}(a, m) = 1$. De manera similar, se tiene que $\text{mcd}(b, n) = 1$. Por lo tanto, $a \in A_m$ y $b \in A_n$. Más aún, como tales a y b son únicos, se tiene una función $f: A_{mn} \to A_m \times A_n$ bien definida dada por

$$f(k) := (a, b).$$

El siguiente paso consiste en probar que φ es biyectiva.

Sea $(a,b) \in A_m \times A_n$.

$0 \leq a < m$ y $\text{mcd}(a,m) = 1$

$0 \leq b < n$ y $\text{mcd}(b,n) = 1$.

Como $\text{mcd}(m,n) = 1$, por el teorema chino del resto se tiene que el sistema $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ tiene solución única módulo mn.

Sea k la solución del sistema anterior, es decir

$$k \equiv a \pmod{m} \quad \text{y} \quad k \equiv b \pmod{n}.$$

La prueba concluirá cuando demostremos que

$$\text{mcd}(k, mn) = 1.$$

Por un lado, $\text{mcd}(a,m) = 1 \Rightarrow \exists\, x_0, y_0 \in \mathbb{Z} \,/\, ax_0 + my_0 = 1$

$\text{mcd}(b,n) = 1 \Rightarrow \exists\, x_1, y_1 \in \mathbb{Z} \,/\, bx_1 + ny_1 = 1$

Por otro lado, $k \equiv a \pmod{m} \Rightarrow \exists\, q_0 \in \mathbb{Z} \,/\, a = k + q_0 m$

$k \equiv b \pmod{n} \Rightarrow \exists\, q_1 \in \mathbb{Z} \,/\, b = k + q_1 n$

Luego, $(k + q_0 m) \cdot x_0 + my_0 = 1$

$kx_0 + (q_0 x_0 + y_0) m = 1$

$kx_0 + my_0' = 1$

donde $y_0' = q_0 x_0 + y_0$.

y $(k + q_1 n) x_1 + n y_1 = 1$

$kx_1 + (q_1 n + y_1) n = 1$

$kx_1 + ny_1' = 1$

donde $y_1' = q_1 n + y_1$.

Entonces, $1 = (kx_0 + my_0')(kx_1 + ny_1')$

$1 = k^2 x_0 x_1 + kn x_0 y_1' + km x_1 y_0' + mn y_0' y_1'$

$1 = k(kx_0 x_1 + n x_0 y_1' + m x_1 y_0') + mn(y_0' y_1')$,

lo cual implica que $\text{mcd}(k, mn) = 1$.

Por lo tanto, $k \in A_{mn}$ y $(a,b) = f(k)$. ■

(único)

Volvamos a condidenan para $m \in \mathbb{Z}^+$ con $m \geq 2$ su descomposición como producto de potencias de primos:

$$m = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}.$$

Para $i, j \in \{1, \ldots, n\}$ con $i \neq j$, se tiene que

$$\text{mcd}(p_i^{d_i}, p_j^{d_j}) = 1,$$

ya que p_i y p_j son primos. Aplicando la propiedad multiplicativa, tenemos que

$$\varphi(m) = \varphi(p_1^{d_1}) \varphi(p_2^{d_2}) \cdots \varphi(p_n^{d_n}).$$

Además, pon sen cada p_i primo, también sabemos que

$$\begin{aligned} \varphi(p_i^{d_i}) &= p_i^{d_i - 1}(p_i - 1) \\ &= p_i^{d_i}\left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Pon lo tanto,

$$\begin{aligned} \varphi(m) &= p_1^{d_1 - 1}(p_1 - 1) p_2^{d_2 - 1}(p_2 - 1) \cdots p_n^{d_n - 1}(p_n - 1) \\ &= p_1^{d_1}\left(1 - \frac{1}{p_1}\right) p_2^{d_2}\left(1 - \frac{1}{p_2}\right) \cdots p_n^{d_n}\left(1 - \frac{1}{p_n}\right) \end{aligned}$$

Es decin,

$$\boxed{\varphi(m) = \prod_{i=1}^{n} p_i^{d_i - 1}(p_i - 1) = m \prod_{i=1}^{n}\left(1 - \frac{1}{p_i}\right).}$$

Ejemplo: Calcule $\varphi(5040)$.

En primer lugar, $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$

Luego,

$$\varphi(5040) = 5040\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$$

$$= 5040 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7}$$

$$= \frac{5040}{5 \cdot 7} \cdot 8 = \frac{1008}{7} \cdot 8$$

$$= 144 \cdot 8$$

$$= 1152.$$

Existen 1152 enteros positivos coprimos con el número 5040. //

Ahora estamos listos para probar el teorema de Euler.

Teorema de Euler: Sean $a, m \in \mathbb{Z}^+$ con $m \geq 2$.
Si $mcd(a, m) = 1$, entonces

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

· **Demostración**: Consideremos el conjunto

$$A_m = \{r_1, r_2, \ldots, r_{\varphi(m)}\}.$$

La demostración se dividirá en dos partes:

1) Para cada $i \in \{1, 2, \ldots, \varphi(m)\}$, existe $j \in \{1, 2, \ldots, \varphi(m)\}$ tal que

$$a r_j \equiv r_i \pmod{m}.$$

2) $a r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$.

- Parte 1: Fijamos $i \in \{1, 2, \ldots, \varphi(m)\}$, y consideramos la ecuación de congruencia

$$ax \equiv r_i \pmod{m}.$$

Como $\text{mcd}(a, m) = 1$, la ecuación anterior tiene solución única módulo m. Entonces, existe $r \in \mathbb{Z}$ único módulo m tal que

$$ar \equiv r_i \pmod{m}.$$

Podemos tomar $0 \leq r < m$. Veamos que $\text{mcd}(r, m) = 1$.

$ar \equiv r_i \pmod{m} \Rightarrow r_i = ar + qm$ para algún $q \in \mathbb{Z}$.

$\text{mcd}(r_i, m) = 1 \Rightarrow \exists\, x_0, y_0 \in \mathbb{Z} \;/\; r_i x_0 + m y_0 = 1.$

Luego, $1 = r_i x_0 + m y_0 = (ar + qm) x_0 + m y_0$

$$1 = r(a x_0) + m(q x_0 + y_0).$$

Lo anterior implica que $\text{mcd}(r, m) = 1$.

Por lo tanto, $r \in A_m$, es decir, $r = r_j$ para algún $j \in \{1, 2, \ldots, \varphi(m)\}$.

- Parte 2: La aplicación $\Lambda_i \mapsto \Lambda_j$ descrita en la parte 1 es biyectiva, es decir,

$$a\Lambda_i \equiv a\Lambda_j \pmod{m} \Rightarrow \Lambda_i = \Lambda_j,$$

donde $\Lambda_i, \Lambda_j \in A_m$. Efectivamente, como $a\Lambda_i \equiv a\Lambda_j \pmod{m}$, se tiene que $m \mid a(\Lambda_i - \Lambda_j)$. Como $\text{mcd}(a, m) = 1$, el Lema de Euclides implica que

$$\Lambda_i \equiv \Lambda_j \pmod{m}.$$

Por otro lado, $\Lambda_i, \Lambda_j \in \{0, 1, \ldots, m-1\}$, lo anterior implica que $\Lambda_i = \Lambda_j$.

A partir de las observaciones anteriores, tenemos que

$$(a\Lambda_1)(a\Lambda_2)\cdots(a\Lambda_{\varphi(m)}) \equiv \Lambda_1\Lambda_2\cdots\Lambda_{\varphi(m)} \pmod{m}$$

$$a^{\varphi(m)}(\Lambda_1\Lambda_2\cdots\Lambda_{\varphi(m)}) \equiv \Lambda_1\Lambda_2\cdots\Lambda_{\varphi(m)} \pmod{m}.$$

Para finalizar, basta probar que

$$\text{mcd}(\Lambda_1\Lambda_2\cdots\Lambda_{\varphi(m)}, m) = 1,$$

para poder aplicar la propiedad cancelativa y concluir que

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

Sea $d = mcd(r_1 r_2 \cdots r_{q(m)}, m)$. Luego,

$$d \mid r_1 r_2 \cdots r_{q(m)} \quad y \quad d \mid m.$$

Consideremos $d_1 = mcd(d, r_1)$. Como $d_1 \mid d$ y $d \mid m$, tenemos que d_1 es un divisor común de r_1 y m, y como $mcd(r_1, m) = 1$, obtenemos $d_1 = 1$.

$mcd(d, r_1) = 1 \Longrightarrow d \mid r_2 \cdots r_{q(m)}$, por el lema de Euclides.

Procediendo de la manera anterior inductivamente, llegaremos a que $d \mid r_{q(m)}$, y como $mcd(r_{q(m)}, m) = 1$, obtenemos finalmente que $d = 1$. ■

Como $\varphi(p) = p - 1$ para p primo, se tiene el siguiente corolario del teorema de Euler:

<u>Teorema de Fermat</u>: Si p es primo y $a \in \mathbb{Z}$ es tal que $p \nmid a$, entonces

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

Recuerde que este teorema también es un corolario del pequeño teorema de Fermat.

Otra aplicación del teorema de Euler tiene que ver con determinar soluciones de ciertas ecuaciones de congruencia.

Corolario: Si $a, b \in \mathbb{Z}$ y $\text{mcd}(a, m) = 1$, entonces la ecuación

$$ax \equiv b \pmod{m}$$

tiene solución única módulo m, dada por

$$x \equiv a^{\varphi(m)-1} b \pmod{m}.$$

· **Demostración:** Sabemos que $\text{mcd}(a, m) = 1$ implica que la ecuación $ax \equiv b \pmod{m}$ tiene solución única módulo m. Por otro lado, por el teorema de Euler, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Es decir, $a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$.

Al multiplicar por b, tenemos

$$a \cdot (a^{\varphi(m)-1} b) \equiv b \pmod{m}$$

Entonces, $a^{\varphi(m)-1} b$ es la única solución de la ecuación $ax \equiv b \pmod{m}$. ∎

Ejemplo:

① Volvamos a calcular el resto de dividir 37^{7541} entre 7, usando los resultados vistos recientemente.

$\varphi(7) = 6$, y por el teorema de Euler se tiene que $37^6 \equiv 1 \pmod{7}$, pues $\text{mcd}(37, 7) = 1$.

Por otro lado, $7541 = 6 \cdot 1256 + 5$.

Entonces,

$$37^6 \equiv 1 \pmod 7 \Rightarrow (37^6)^{1256} \equiv 1 \pmod 7$$
$$\Rightarrow 37^{6\cdot 1256} \equiv 1 \pmod 7$$
$$\Rightarrow 37^5 \cdot 37^{6\cdot 1256} \equiv 37^5 \pmod 7$$
$$\Rightarrow 37^{7541} \equiv 37^5 \pmod 7$$

El problema ahora se reduce a calcular $37^5 \pmod 7$.

$$37 \equiv 2 \pmod 7 \Rightarrow 37^5 \equiv 2^5 \pmod 7$$
$$\Rightarrow 37^5 \equiv 32 \pmod 7$$
$$\Rightarrow 37^5 \equiv 4 \pmod 7.$$

Por lo tanto, $37^{7541} \equiv 4 \pmod 7$.

② Hallar el valor de $x \in \mathbb{Z}$, con $0 \leq x < 17$, para el cual $1211^{339} x \equiv 22 \pmod{17}$

Primero, como $22 \equiv 5 \pmod{17}$ la ecuación se convierte en

$$1211^{339} x \equiv 5 \pmod{17}$$

Por otro lado, por el teorema de Euler (note que $\text{mcd}(1211, 17) = 1$) se tiene que

$$1211^{16} \equiv 1 \pmod{17}.$$

Ahora, $339 = 16 \cdot 21 + 3$, por lo cual:

$$1211^{16} \equiv 1 \pmod{17} \Rightarrow 1211^{16 \cdot 21} \equiv 1 \pmod{17}$$

$$\Rightarrow 1211^{339} \equiv 1211^{3} \pmod{17}$$

Como $1211 = 17 \cdot 71 + 4$, tenemos

$$1211^{3} \equiv 4^{3} \pmod{17}$$

$$1211^{3} \equiv 64 \pmod{17}$$

$$1211^{3} \equiv 13 \pmod{17}$$

Por lo tanto, $5 \equiv 1211^{339} x \pmod{17}$ y

$$1211^{339} x \equiv 13x \pmod{17},$$

implican que

$$13x \equiv 5 \pmod{17}.$$

Y por el corolario anterior,

$$x \equiv 13^{\varphi(17)-1} \cdot 5 \pmod{17}$$

$$x \equiv 13^{15} \cdot 5 \pmod{17}.$$

- $13 \cdot 13 = 169 = 9 \cdot 17 + 16$

  $13^{2} \equiv 16 \pmod{17}$

  $13^{14} \equiv 16^{7} \pmod{17}$ ⟶

- $16 \cdot 16 = 256 = 15 \cdot 17 + 1$

  $16^{2} \equiv 1 \pmod{17}$

  $16^{6} \equiv 1 \pmod{17}$

  $16^{7} \equiv 16 \pmod{17}$ ⟶

$13^{14} \equiv 16 \pmod{17}$

$13^{15} \equiv 16 \cdot 13 \pmod{17}$

$16 \cdot 13 = 208 = 12 \cdot 17 + 4$

$16 \cdot 13 \equiv 4 \pmod{17}$

Entonces, $13^{15} \equiv 4 \pmod{17}$

$13^{15} \cdot 5 \equiv 20 \pmod{17}$

$13^{15} \cdot 5 \equiv 3 \pmod{17}$.

Por lo tanto, $x \equiv 3 \pmod{17}$.

③ Hallan las últimas 4 cifras binarias de 1993^{1994}.

Sabemos que existe $n \in \mathbb{Z}^+$ tal que

$$1993^{1994} = a_n 2^n + \cdots + a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 2 + a_0.$$

(con $a_0, a_1, \ldots, a_n \in \{0,1\}$)

a_0 es el resto de dividir 1993^{1994} por 2.

$$1993 \equiv 1 \pmod 2 \Rightarrow 1993^{1994} \equiv 1 \pmod 2$$

Así, $a_0 = 1$. Luego,

$$1993^{1994} - 1 = (a_n \cdot 2^{n-2} + \cdots + a_3 \cdot 2 + a_2) \cdot 4 + a_1 2,$$

por lo cual

$$1993^{1994} \equiv 2a_1 + 1 \pmod 4.$$

Como $\text{mcd}(1993, 4) = 1$, por el teorema de Euler se tiene que

$$1993^{\varphi(4)} \equiv 1 \pmod 4$$

$$1993^2 \equiv 1 \pmod 4$$

$$(1993^2)^{997} \equiv 1 \pmod 4$$

$$1993^{1994} \equiv 1 \pmod 4$$

Se sigue que $2a_1 + 1 \equiv 1 \pmod 4$, de donde

$$2a_1 \equiv 0 \pmod 4$$

Como $a_1 \in \{0,1\}$, nos queda $a_1 = 0$.

$$1993^{1994} = a_m 2^m + \cdots + a_3 2^3 + a_2 \cdot 2^2 + 1$$
$$= (a_m 2^{m-3} + \cdots + a_3)\, 8 + (4a_2 + 1)$$

$$1993^{1994} \equiv 4a_2 + 1 \pmod 8$$

Como $\text{mcd}(1993, 8) = 1$, se tiene nuevamente por el teorema de Euler que

$$1993^{\varphi(8)} \equiv 1 \pmod 8$$
$$1993^4 \equiv 1 \pmod 8.$$

Por otro lado, $1994 = 4 \cdot 498 + 2$. Así,

$$1993^{4 \cdot 498} \equiv 1 \pmod 8$$
$$1993^{1994} \equiv 1993^2 \pmod 8$$

Como $1993 = 8 \cdot 249 + 1$, $1993 \equiv 1 \pmod 8$
$1993^2 \equiv 1 \pmod 8$

Por lo cual, $1993^{1994} \equiv 1 \pmod 8$ y así

$$4a_2 + 1 \equiv 1 \pmod 8$$
$$4a_2 \equiv 0 \pmod 8.$$

De donde, $a_2 = 0$ ya que $a_2 \in \{0, 1\}$.

$$1993^{1994} = a_m 2^m + \cdots + a_3 \cdot 2^3 + 1$$
$$1993^{1994} \equiv 8a_3 + 1 \pmod{16}$$

$\text{mcd}(1993, 16) = 1 \Rightarrow 1993^{\varphi(16)} \equiv 1 \pmod{16}$

$16 = 2^4 \Rightarrow \varphi(16) = 2^4 - 2^3 = 16 - 8 = 8$

$$1993^8 \equiv 1 \pmod{16}.$$

Como $1994 = 8 \cdot 249 + 2$, tenemos

$$1993^{8 \cdot 249} \equiv 1 \pmod{16}$$
$$1993^{1994} \equiv 1993^2 \pmod{16}.$$

Por otro lado, $1993 = 16 \cdot 124 + 9$

$$1993 \equiv 9 \pmod{16}$$
$$1993^2 \equiv 81 \pmod{16}, \quad 81 = 16 \cdot 5 + 1$$
$$1993^2 \equiv 1 \pmod{16}.$$
$$1993^{1994} \equiv 1 \pmod{16}$$

Entonces, $8a_3 + 1 \equiv 1 \pmod{16}$

$$8a_3 \equiv 0 \pmod{16}.$$
$$a_3 = 0.$$

Por lo tanto,

$$1993^{1994} = (\cdots 0001)_2.$$