

La función φ de Euler

Cómo reducir el exponente de una potencia modular

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

El problema

$$92^{727} \bmod 45 = ?$$

$$92^{727} = 47179189981253657324821082681127 \dots$$

un número de 1428 cifras

El problema

$$92^{727} \bmod 45 = ?$$

$$92^{727} = 47179189981253657324821082681127 \dots$$

un número de 1428 cifras

Atajo: reducir el exponente antes de calcular.

El problema

$$92^{727} \bmod 45 = ?$$

$$92^{727} = 47179189981253657324821082681127 \dots$$

un número de 1428 cifras

$$92^{727} \equiv 2^7 \pmod{45}$$

Atajo: reducir el exponente antes de calcular.

1. ¿Qué cuenta $\varphi(n)$?

$\varphi(n)$ = cantidad de enteros k entre 1 y n con $\text{mcd}(k, n) = 1$

$\varphi(n)$: cuántos enteros de 1 a n son primos relativos con n .

1. ¿Qué cuenta $\varphi(n)$?

$\varphi(n)$ = cantidad de enteros k entre 1 y n con $\text{mcd}(k, n) = 1$

Primos relativos: sin factores en común, $\text{mcd}(k, n) = 1$.

1. ¿Qué cuenta $\varphi(n)$?

$\varphi(n)$ = cantidad de enteros k entre 1 y n con $\text{mcd}(k, n) = 1$

1 2 3 4 5 6 7 8 9 10

$$10 = 2 \times 5$$

Comparten un factor con 10 los múltiplos de 2 y los de 5.

1. ¿Qué cuenta $\varphi(n)$?

$\varphi(n)$ = cantidad de enteros k entre 1 y n con $\text{mcd}(k, n) = 1$

1 ~~2~~ 3 ~~4~~ ~~5~~ ~~6~~ 7 ~~8~~ 9 ~~10~~

$$10 = 2 \times 5$$

Comparten un factor con 10 los múltiplos de 2 y los de 5.

1. ¿Qué cuenta $\varphi(n)$?

$\varphi(n)$ = cantidad de enteros k entre 1 y n con $\text{mcd}(k, n) = 1$



$$10 = 2 \times 5$$

$$\varphi(10) = 4$$

$\varphi(10) = 4$: entre 1 y 10 hay 4 primos relativos con 10.

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

Regla 2: potencia de un primo

Regla 3: m y n primos relativos

Contar uno por uno no sirve con números grandes.

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

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

1 2 3 4 5 6 ~~7~~

$$\varphi(7) = 7 - 1 = 6$$

Regla 2: potencia de un primo

Regla 3: m y n primos relativos

Con un primo solo se descarta el propio p .

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

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

1 2 3 4 5 6 ~~7~~

$$\varphi(7) = 7 - 1 = 6$$

Regla 2: potencia de un primo

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

Regla 3: m y n primos relativos

A p^k se le resta la potencia anterior, p^{k-1} .

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

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

1 2 3 4 5 6 ~~7~~

$$\varphi(7) = 7 - 1 = 6$$

Regla 2: potencia de un primo

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

1 2 ~~3~~ 4 5 ~~6~~ 7 8 ~~9~~

$$\varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

Regla 3: m y n primos relativos

A p^k se le resta la potencia anterior, p^{k-1} .

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

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

1 2 3 4 5 6 ~~7~~

$$\varphi(7) = 7 - 1 = 6$$

Regla 2: potencia de un primo

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

1 2 ~~3~~ 4 5 ~~6~~ 7 8 ~~9~~

$$\varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

Regla 3: m y n primos relativos

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

$$\varphi(10) = \varphi(2) \times \varphi(5) = 1 \times 4 = 4$$

La regla 3 solo vale si m y n no comparten factores.

2. Calcular $\varphi(n)$ sin contar

Regla 1: p primo

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

1 2 3 4 5 6 ~~7~~

$$\varphi(7) = 7 - 1 = 6$$

Regla 2: potencia de un primo

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

1 2 ~~3~~ 4 5 ~~6~~ 7 8 ~~9~~

$$\varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

Regla 3: m y n primos relativos

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

$$\varphi(10) = \varphi(2) \times \varphi(5) = 1 \times 4 = 4$$

Receta: factorizar, aplicar la regla 2 a cada potencia de primo y multiplicar.

3. El pequeño teorema de Fermat

k	1	2	3	4	5	6
$2^k \bmod 7$						
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$						
$5^k \bmod 7$						
$6^k \bmod 7$						

Cada casilla: la anterior por 3, módulo 7.

3. El pequeño teorema de Fermat

k	1	2	3	4	5	6
$2^k \bmod 7$						
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$						
$5^k \bmod 7$						
$6^k \bmod 7$						

Después del 1, las potencias se repiten.

3. El pequeño teorema de Fermat

k	1	2	3	4	5	6
$2^k \bmod 7$	2	4	1	2	4	1
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1	4	2	1
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1	6	1	6	1

Con cualquier base, la potencia 6 da 1 módulo 7.

3. El pequeño teorema de Fermat

k	1	2	3	4	5	6
$2^k \bmod 7$	2	4	1	2	4	1
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1	4	2	1
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1	6	1	6	1

$$p \text{ primo, } p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$$

Con módulo primo p , el exponente $p - 1$ siempre da 1.

3. El pequeño teorema de Fermat

$$p \text{ primo, } p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$$

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

El exponente de Fermat es $\varphi(p)$.

3. El pequeño teorema de Fermat

$$p \text{ primo, } p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$$

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

$$\text{Si } p \mid a : \quad a^k \equiv 0 \pmod{p}$$

Si a es múltiplo de p , el teorema no aplica.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

5^{123} tiene 86 cifras. Hay que reducir el exponente.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

Fermat con $p = 13$: el exponente que da 1 es $p - 1 = 12$.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

Cada grupo de 12 en el exponente vale 1.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

Cada grupo de 12 en el exponente vale 1.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$5^{123} = 5^{12 \times 10 + 3}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

Cada grupo de 12 en el exponente vale 1.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

$$5^{123} = 5^{12 \times 10 + 3}$$

$$= (5^{12})^{10} \times 5^3$$

Leyes de los exponentes: $a^{x \cdot y + z} = (a^x)^y \times a^z$.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

$$5^{123} = 5^{12 \times 10 + 3}$$

$$= (5^{12})^{10} \times 5^3$$

$$\equiv 1^{10} \times 5^3$$

Todos los grupos completos desaparecen.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

$$5^{123} = 5^{12 \times 10 + 3}$$

$$= (5^{12})^{10} \times 5^3$$

$$\equiv 1^{10} \times 5^3$$

$$= 125 \equiv 8 \pmod{13}$$

División: $125 = 13 \times 9 + 8$.

4. Primer ejemplo: 5^{123} módulo 13

$$5^{123} \bmod 13$$

13 es primo y $13 \nmid 5$

$$5^{12} \equiv 1 \pmod{13}$$

$$123 = 12 \times 10 + 3$$

el exponente, dividido entre 12

$$5^{123} = 5^{12 \times 10 + 3}$$

$$= (5^{12})^{10} \times 5^3$$

$$\equiv 1^{10} \times 5^3$$

$$= 125 \equiv 8 \pmod{13}$$

$$5^{123} \equiv 8 \pmod{13}$$

El exponente se reduce módulo $p - 1 = 12$: de 123 a 3.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

Teorema de Euler. Fermat es el caso en que n es primo.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

k	1	2	3	4	$\varphi(10) = 4$
$3^k \bmod 10$					
$7^k \bmod 10$					
$9^k \bmod 10$					

Teorema de Euler. Fermat es el caso en que n es primo.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

k	1	2	3	4
$3^k \bmod 10$	3	9	7	1
$7^k \bmod 10$	7	9	3	1
$9^k \bmod 10$	9	1	9	1

$$\varphi(10) = 4$$

Teorema de Euler. Fermat es el caso en que n es primo.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

k	1	2	3	4	$\varphi(10) = 4$
$3^k \bmod 10$	3	9	7	1	$\text{mcd}(3, 10) = 1$
$7^k \bmod 10$	7	9	3	1	$\text{mcd}(7, 10) = 1$
$9^k \bmod 10$	9	1	9	1	$\text{mcd}(9, 10) = 1$

3, 7 y 9 son primos relativos con 10: su potencia 4 es 1.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

k	1	2	3	4	$\varphi(10) = 4$
$3^k \bmod 10$	3	9	7	1	$\text{mcd}(3, 10) = 1$
$7^k \bmod 10$	7	9	3	1	$\text{mcd}(7, 10) = 1$
$9^k \bmod 10$	9	1	9	1	$\text{mcd}(9, 10) = 1$
$2^k \bmod 10$	2	4	8	6	$\text{mcd}(2, 10) = 2$

3, 7 y 9 son primos relativos con 10: su potencia 4 es 1.

5. Si el módulo no es primo: el teorema de Euler

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

Fermat: p primo, $p \nmid a$



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

Euler: $\text{mcd}(a, n) = 1$

k	1	2	3	4	$\varphi(10) = 4$
$3^k \bmod 10$	3	9	7	1	$\text{mcd}(3, 10) = 1$
$7^k \bmod 10$	7	9	3	1	$\text{mcd}(7, 10) = 1$
$9^k \bmod 10$	9	1	9	1	$\text{mcd}(9, 10) = 1$
$2^k \bmod 10$	2	4	8	6	$\text{mcd}(2, 10) = 2$

Antes de usar el teorema: revisar que $\text{mcd}(a, n) = 1$.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

45 no es primo: se usa el teorema de Euler.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

1. La base $92 = 45 \times 2 + 2 \implies 92 \equiv 2 \pmod{45}$

Paso 1: la base se reduce módulo n .

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

1. La base $92 = 45 \times 2 + 2 \implies 92 \equiv 2 \pmod{45}$

2. $\varphi(45)$ $45 = 3^2 \times 5$ $\varphi(45) = (3^2 - 3^1)(5 - 1) = 6 \times 4 = 24$

Paso 2: $\varphi(n)$, a partir de la factorización.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

1. La base $92 = 45 \times 2 + 2 \implies 92 \equiv 2 \pmod{45}$

2. $\varphi(45)$ $45 = 3^2 \times 5$ $\varphi(45) = (3^2 - 3^1)(5 - 1) = 6 \times 4 = 24$

3. La condición $\text{mcd}(2, 45) = 1 \implies 2^{24} \equiv 1 \pmod{45}$

Paso 3: la base y el módulo deben ser primos relativos.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

1. La base $92 = 45 \times 2 + 2 \implies 92 \equiv 2 \pmod{45}$

2. $\varphi(45)$ $45 = 3^2 \times 5$ $\varphi(45) = (3^2 - 3^1)(5 - 1) = 6 \times 4 = 24$

3. La condición $\text{mcd}(2, 45) = 1 \implies 2^{24} \equiv 1 \pmod{45}$

4. El exponente $727 = 24 \times 30 + 7$

Paso 4: el exponente, dividido entre $\varphi(n)$.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

$$92 \equiv 2 \pmod{45}$$

$$2^{24} \equiv 1 \pmod{45}$$

$$727 = 24 \times 30 + 7$$

$$92^{727} \equiv 2^{727}$$

$$= (2^{24})^{30} \times 2^7$$

Paso 5: reemplazar y simplificar.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

$$92 \equiv 2 \pmod{45}$$

$$2^{24} \equiv 1 \pmod{45}$$

$$727 = 24 \times 30 + 7$$

$$92^{727} \equiv 2^{727}$$

$$= (2^{24})^{30} \times 2^7$$

$$\equiv 1^{30} \times 2^7$$

$$= 128 \equiv 38 \pmod{45}$$

División: $128 = 45 \times 2 + 38$.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

$$92 \equiv 2 \pmod{45}$$

$$2^{24} \equiv 1 \pmod{45}$$

$$727 = 24 \times 30 + 7$$

$$92^{727} \equiv 2^{727}$$

$$= (2^{24})^{30} \times 2^7$$

$$\equiv 1^{30} \times 2^7$$

$$= 128 \equiv 38 \pmod{45}$$

$$92^{727} \equiv 38 \pmod{45}$$

El exponente bajó de 727 a 7.

6. Segundo ejemplo: 92^{727} módulo 45

$$92^{727} \bmod 45$$

$$92 \equiv 2 \pmod{45}$$

$$2^{24} \equiv 1 \pmod{45}$$

$$727 = 24 \times 30 + 7$$

$$92^{727} \equiv 2^{727}$$

$$= (2^{24})^{30} \times 2^7$$

$$\equiv 1^{30} \times 2^7$$

$$= 128 \equiv 38 \pmod{45}$$

$$92^{727} \equiv 38 \pmod{45}$$

Si el exponente reducido sigue siendo grande: square and multiply.

Para reducir a^e módulo n

Para reducir a^e módulo n

1. Reducir la base a módulo n .

Para reducir a^e módulo n

1. Reducir la base a módulo n .
2. Calcular $\varphi(n)$. Si n es primo, $\varphi(n) = n - 1$ (Fermat).

Para reducir a^e módulo n

1. Reducir la base a módulo n .
2. Calcular $\varphi(n)$. Si n es primo, $\varphi(n) = n - 1$ (Fermat).
3. Verificar que $\text{mcd}(a, n) = 1$: entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Para reducir a^e módulo n

1. Reducir la base a módulo n .
2. Calcular $\varphi(n)$. Si n es primo, $\varphi(n) = n - 1$ (Fermat).
3. Verificar que $\text{mcd}(a, n) = 1$: entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.
4. Dividir el exponente: $e = \varphi(n) \times q + r$.

Para reducir a^e módulo n

1. Reducir la base a módulo n .
2. Calcular $\varphi(n)$. Si n es primo, $\varphi(n) = n - 1$ (Fermat).
3. Verificar que $\text{mcd}(a, n) = 1$: entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.
4. Dividir el exponente: $e = \varphi(n) \times q + r$.
5. Reemplazar: $a^e \equiv a^r \pmod{n}$.