

Inverso multiplicativo modular

De la identidad de Bézout al inverso

Daniel Felipe Triviño

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

1. ¿Qué es un inverso multiplicativo?

En los números reales

$$3 \cdot \frac{1}{3} = 1$$

1. ¿Qué es un inverso multiplicativo?

En los números reales

$$3 \cdot \frac{1}{3} = 1$$

En aritmética modular

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

a^{-1} : el entero que, multiplicado por a , deja residuo 1 al dividir entre m .

1. ¿Qué es un inverso multiplicativo?

En los números reales

$$3 \cdot \frac{1}{3} = 1$$

En aritmética modular

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

$$3 \cdot 7 = 21 \equiv 1 \pmod{10} \Rightarrow 3^{-1} \equiv 7 \pmod{10}$$

a^{-1} : el entero que, multiplicado por a , deja residuo 1 al dividir entre m .

2. Lo que no es

No es una fracción


$$3^{-1} = \frac{1}{3} = 0,333 \dots$$

Eso es aritmética de números reales.

El inverso modular no es una fracción ni un decimal.

2. Lo que no es

No es una fracción

~~$$3^{-1} = \frac{1}{3} = 0,333\dots$$~~

Eso es aritmética de números reales.

Es un entero, y depende del módulo

$$3^{-1} \equiv 7 \pmod{10} \checkmark$$

$$3 \cdot 7 = 21 = 2 \cdot 10 + 1$$

$$3^{-1} \equiv 5 \pmod{7} \checkmark$$

$$3 \cdot 5 = 15 = 2 \cdot 7 + 1$$

El inverso modular es un entero entre 0 y $m - 1$, y cambia con el módulo.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7

No todos los números tienen inverso.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7

No todos los números tienen inverso.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7
$4 \cdot k \bmod 10$	4	8	2	6	0	4	8	2	6

No todos los números tienen inverso.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7
$4 \cdot k \bmod 10$	4	8	2	6	0	4	8	2	6

Los múltiplos de 4 nunca dejan residuo 1 al dividir entre 10.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9	
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7	$\text{mcd}(3, 10) = 1$
$4 \cdot k \bmod 10$	4	8	2	6	0	4	8	2	6	$\text{mcd}(4, 10) = 2$

Los múltiplos de 4 nunca dejan residuo 1 al dividir entre 10.

3. ¿Cuándo existe el inverso?

k	1	2	3	4	5	6	7	8	9	
$3 \cdot k \bmod 10$	3	6	9	2	5	8	1	4	7	$\text{mcd}(3, 10) = 1$
$4 \cdot k \bmod 10$	4	8	2	6	0	4	8	2	6	$\text{mcd}(4, 10) = 2$

$$a^{-1} \bmod m \text{ existe} \iff \text{mcd}(a, m) = 1$$

Hay inverso solo si a y m son primos relativos.

4. De Bézout al inverso

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	−45
4	3	4	−1	46
5	2	1	5	−229
6	1	2	−6	275

La última fila de la tabla del video anterior.

4. De Bézout al inverso

$$779 \times (-6) + 17 \times 275 = 1$$

i	r_i	q_i	s_i	t_i
1	779	—	1	0
2	17	45	0	1
3	14	1	1	-45
4	3	4	-1	46
5	2	1	5	-229
6	1	2	-6	275

La última fila de la tabla del video anterior.

4. De Bézout al inverso

$$779 \times (-6) + 17 \times 275 = 1$$

$\text{mcd}(779, 17) = 1$: el inverso existe.

4. De Bézout al inverso

$$a \cdot s + b \cdot t = 1$$

$$779 \times (-6) + 17 \times 275 = 1$$

$\text{mcd}(779, 17) = 1$: el inverso existe.

4. De Bézout al inverso

$$a \cdot s + m \cdot t = 1$$

$$779 \times (-6) + 17 \times 275 = 1$$

b pasa a llamarse m : va a ser el módulo.

4. De Bézout al inverso

$$a \cdot s + m \cdot t \equiv 1 \pmod{m}$$

$$779 \times (-6) + 17 \times 275 \equiv 1 \pmod{17}$$

Una igualdad también es una congruencia, en cualquier módulo.

4. De Bézout al inverso

$$a \cdot s \equiv 1 \pmod{m}$$

$$779 \times (-6) \equiv 1 \pmod{17}$$

Módulo 17, todo múltiplo de 17 vale 0.

4. De Bézout al inverso

Definición: $a \cdot \boxed{a^{-1}} \equiv 1 \pmod{m}$

$$a \cdot \boxed{s} \equiv 1 \pmod{m}$$

$$779 \times \boxed{(-6)} \equiv 1 \pmod{17}$$

Lo que queda tiene la forma de la definición: s ocupa el lugar del inverso.

4. De Bézout al inverso

Definición: $a \cdot \boxed{a^{-1}} \equiv 1 \pmod{m}$

$$a \cdot \boxed{s} \equiv 1 \pmod{m}$$

$$779 \times \boxed{(-6)} \equiv 1 \pmod{17}$$

$$a^{-1} \equiv s \pmod{m}$$

$$779^{-1} \equiv -6 \pmod{17}$$

Lo que queda tiene la forma de la definición: s ocupa el lugar del inverso.

5. Si el inverso sale negativo

$$779^{-1} \equiv -6 \pmod{17}$$



resultados entre 0 y 16

El inverso se suele dar entre 0 y $m - 1 = 16$.

5. Si el inverso sale negativo

$$779^{-1} \equiv -6 \pmod{17}$$



$$-6 + 17 = 11$$

El inverso se suele dar entre 0 y $m - 1 = 16$.

5. Si el inverso sale negativo

$$779^{-1} \equiv -6 \pmod{17}$$



$$-6 + 17 = 11$$

$$-6 \equiv 11 \pmod{17}$$

Sumar o restar 17 no cambia la clase módulo 17.

5. Si el inverso sale negativo

$$779^{-1} \equiv -6 \pmod{17}$$

$$-6 \equiv 11 \pmod{17}$$

$$779 \times 11 = 8569 = 17 \times 504 + 1 \quad \checkmark$$

¿ $779 \cdot 11$ también deja residuo 1 al dividir entre 17?

5. Si el inverso sale negativo

$$779^{-1} \equiv -6 \pmod{17}$$

$$-6 \equiv 11 \pmod{17}$$

$$779 \times 11 = 8569 = 17 \times 504 + 1 \quad \checkmark$$

$$779^{-1} \pmod{17} = -6 \pmod{17} = 11$$

¿ $779 \cdot 11$ también deja residuo 1 al dividir entre 17?

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 = 19 \times 36 + 13$$

Primero Euclides: ¿el máximo común divisor es 1?

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 = 19 \times 36 + 13$$

$$19 = 13 \times 1 + 6$$

$$13 = 6 \times 2 + \boxed{1}$$

$$6 = 1 \times 6 + 0$$

$$\text{mcd}(697, 19) = 1 \checkmark$$

$\text{mcd}(697, 19) = 1$: el inverso existe.

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 = 19 \times 36 + 13$$

$$19 = 13 \times 1 + 6$$

$$13 = 6 \times 2 + \boxed{1}$$

$$6 = 1 \times 6 + 0$$

$$\text{mcd}(697, 19) = 1 \checkmark$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$, y lo mismo para t_i .

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 = 19 \times 36 + 13$$

$$19 = 13 \times 1 + 6$$

$$13 = 6 \times 2 + \boxed{1}$$

$$6 = 1 \times 6 + 0$$

$$\text{mcd}(697, 19) = 1 \checkmark$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$, y lo mismo para t_i .

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 \times 3 + 19 \times (-110) = 1$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$, y lo mismo para t_i .

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = ?$$

$$697 \times 3 + 19 \times (-110) = 1$$

$$697 \times 3 \equiv 1 \pmod{19}$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

Módulo 19, todo múltiplo de 19 vale 0.

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = 3$$

$$697 \times 3 + 19 \times (-110) = 1$$

$$697 \times 3 \equiv 1 \pmod{19}$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

3 ya está entre 0 y 18.

6. Otro ejemplo: 697^{-1} módulo 19

$$697^{-1} \bmod 19 = 3$$

$$697 \times 3 + 19 \times (-110) = 1$$

$$697 \times 3 \equiv 1 \pmod{19}$$

$$697 \times 3 = 2091 = 19 \times 110 + 1 \quad \checkmark$$

i	r_i	q_i	s_i	t_i
1	697	—	1	0
2	19	36	0	1
3	13	1	1	-36
4	6	2	-1	37
5	1	6	3	-110

Comprobación: el producto deja residuo 1.

Para hallar a^{-1} módulo m

Para hallar a^{-1} módulo m

1. Algoritmo extendido de Euclides con a y m .

Para hallar a^{-1} módulo m

1. Algoritmo extendido de Euclides con a y m .
2. Si $\text{mcd}(a, m) \neq 1$, el inverso no existe.

Para hallar a^{-1} módulo m

1. Algoritmo extendido de Euclides con a y m .
2. Si $\text{mcd}(a, m) \neq 1$, el inverso no existe.
3. La última fila da $a \cdot s + m \cdot t = 1$: el inverso es s .

Para hallar a^{-1} módulo m

1. Algoritmo extendido de Euclides con a y m .
2. Si $\text{mcd}(a, m) \neq 1$, el inverso no existe.
3. La última fila da $a \cdot s + m \cdot t = 1$: el inverso es s .
4. Si hace falta, reducir s para dejarlo entre 0 y $m - 1$.