

Matemáticas Discretas

Oscar Bedoya

`oscar.bedoya@correounivalle.edu.co`

`http://eisc.univalle.edu.co/~oscarbed/MD/`

- * Algoritmo de Euclides
- * Combinación lineal
- * Inverso de a mod m

Teoría de números

Algoritmo de Euclides

```
public int mcd(int a, int b){  
    x=a;  
    y=b;  
    int x, r;  
    while (y != 0){  
        r = x mod y;  
        x = y;  
        y = r;  
    }  
    return x;  
}
```

Teoría de números

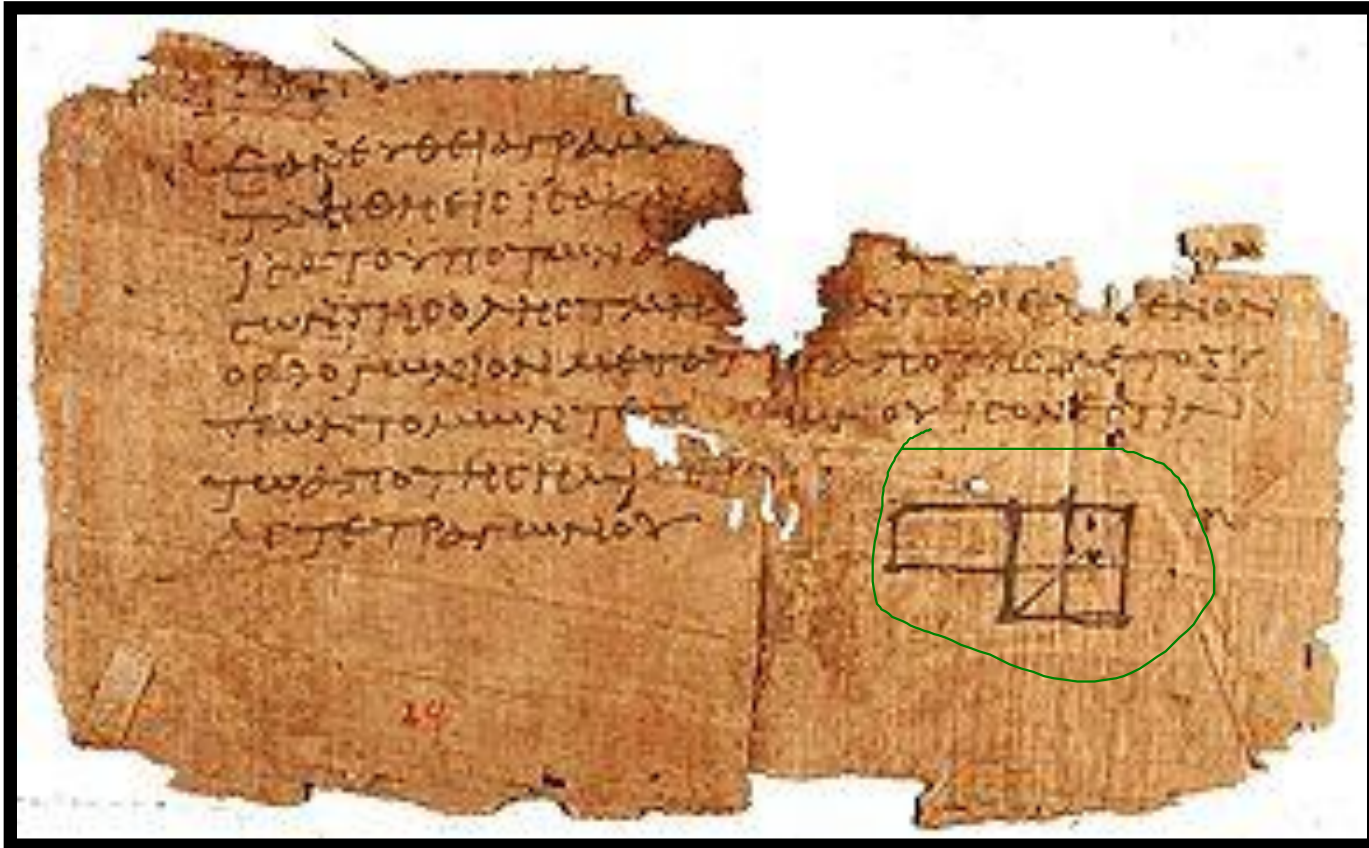
Euclides

- Matemático y geómetra griego
- Se le conoce como el padre de la geometría



(300a.c - ?)

Teoría de números



Fragmento de **Los elementos**
de Euclides escrito en papiro

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

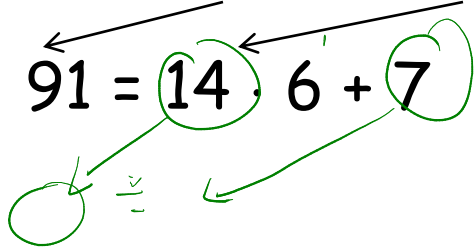
- $287 = 91 \cdot 3 + 14$

$$\begin{array}{c} \swarrow \quad \nwarrow \\ 91 = 14 \cdot ? + ? \end{array}$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

$$91 = 14 \cdot 6 + 7$$


Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot ? + ?$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287, 91)$

- $287 = 91 \cdot 3 + 14$

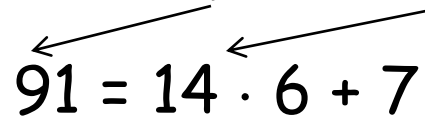
$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot 2 + 0$$

Teoría de números

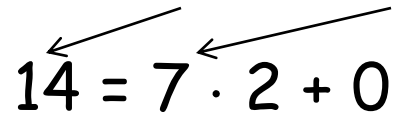
Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(287,91)$

- $287 = 91 \cdot 3 + 14$



$91 = 14 \cdot 6 + 7$

The diagram shows two arrows pointing from the right-hand side of the first equation to the left-hand side of the second equation. One arrow points from the '14' to the '14' in the second equation, and the other points from the '91' to the '14' in the second equation.



$14 = 7 \cdot 2 + 0$

The diagram shows two arrows pointing from the right-hand side of the second equation to the left-hand side of the third equation. One arrow points from the '14' to the '14' in the third equation, and the other points from the '7' in the second equation to the '7' in the third equation.

Se toma el último residuo diferente de 0, en este caso,
 $\text{mcd}(287,91)=7$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(91, 287)$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar $\text{mcd}(91, 287)$

$$\text{mcd}(91, 287) = 7$$

- Para aplicar el algoritmo de Euclides se inicia **siempre** dividiendo el mayor (287) entre el menor (91)

$$287 = 91 \cdot 3 + 14$$

$$91 = 14 \cdot 6 + 7$$

$$14 = 7 \cdot 2 + 0$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

- $\text{mcd}(342, 76)$

Teoría de números

- $\text{mcd}(342, 76)$

$$342 = 76 \cdot 4 + 38$$

$$76 = 38 \cdot 2 + 0$$

- $\text{mcd}(342, 76) = 38$

$$\begin{aligned} 38 &= 342 \bmod 76 \\ 0 &= 76 \bmod 38 \end{aligned}$$

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

• $\text{mcd}(48, 512) = 16$

1) $512 \bmod 48$

$$512 = 48 \times 10 + 32$$

$$48 = 32 \times 1 + 16$$

$$32 = 16 \times 2 + 0$$

Teoría de números

- $\text{mcd}(48, 512)$

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

- **$\text{mcd}(48, 512) = 16$**

Teoría de números

Aplicar el algoritmo de Euclides para encontrar:

18

• $\text{mcd}(252, 198) = 18$

$$252 = 198 \times 1 + 54$$

$$198 = 54 \times 3 + 36$$

$$54 = 36 \times 1 + 18$$

$$36 = 18 \times 2 + 0$$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

Teorema: si a y b son enteros positivos, entonces existen enteros s y t tales que $\text{mcd}(a,b)=a \cdot (s) + b \cdot (t)$

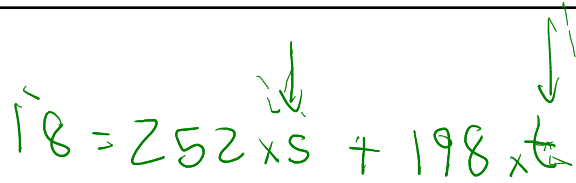
Teoría de números

Teorema: si a y b son enteros positivos, entonces existen enteros s y t tales que $\text{mcd}(a,b)=a \cdot (s) + b \cdot (t)$

El $\text{mcd}(a,b)$ se puede expresar como
una combinación lineal de a y b

Teoría de números

$$\text{mcd}(252, 198) = 18$$

$$18 = 252 \times s + 198 \times t$$


$$18 = 252 \times s + 198 \times t$$

Teoría de números

$$\text{mcd}(252,198) = 18 = 252 \cdot x + 198 \cdot y$$

Teoría de números

$$\text{mcd}(252,198) = 18 = 252 \cdot (4) + 198 \cdot (-5)$$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54 \quad - \quad 54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36 \quad \rightarrow \quad 36 = 198 - 54 \cdot 3$$

$$54 = 36 \cdot 1 + 18 \quad 18 = 54 - 36 \cdot 1$$

$$36 = 18 \cdot 2 \quad \times$$

- $\text{mcd}(252, 198) = 18$

Se despejan los residuos

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$\textcircled{36} = 198 - 54 \cdot 3$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - \textcircled{36} \cdot 1$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

Se reemplazan siempre en la ecuación que tiene al mcd

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - (198 - 54 \cdot 3) \cdot 1$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

$$54 = 252 - 198 \cdot 1$$
$$18 = 54 - 198 \cdot 1 + 54 \cdot 3$$

4×54

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 54 - 36 \cdot 1$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

Teoría de números

- $\text{mcd}(252, 198)$


$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

$$54 = 252 - 198 \cdot 1$$


$$18 = 54 \cdot 4 - 198 \cdot 1$$

- $\text{mcd}(252, 198) = 18$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = (252 - 198 \cdot 1) \cdot 4 - 198 \cdot 1$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

$$18 = 252 \cdot 4 - 198 \cdot 4 - 198 \cdot 1$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$18 = 252 \cdot 4 - 198 \cdot 5$$

$$36 = 18 \cdot 2$$

- **$\text{mcd}(252, 198) = 18$**

Teoría de números

- $\text{mcd}(252, 198)$

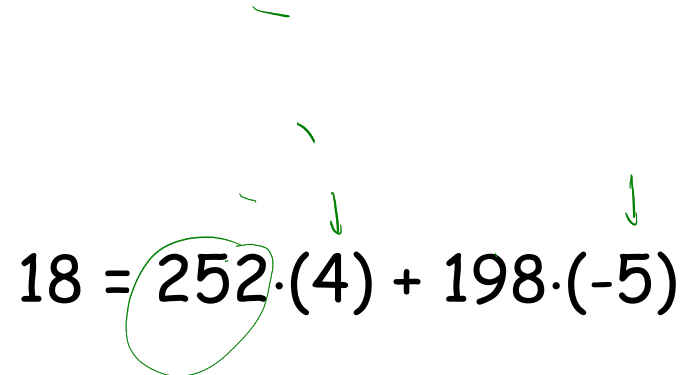
$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2$$

- $\text{mcd}(252, 198) = 18$


$$18 = 252 \cdot (4) + 198 \cdot (-5)$$

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

$$32 = 512 - 48 \times 10$$

$$16 = 48 - 32 \times 1$$

$$16 = 48 - (512 - 48 \times 10)$$

$$16 = (11)48 + (-1)512$$

$$s = -1 \quad t = 11$$

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32 \qquad 32 = 512 - 48 \cdot 10$$

$$48 = 32 \cdot 1 + 16 \qquad 16 = 48 - 32 \cdot 1$$

$$32 = 16 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(512, 48) = 16$ como una combinación lineal

$$512 = 48 \cdot 10 + 32$$

$$48 = 32 \cdot 1 + 16$$

$$32 = 16 \cdot 2 + 0$$

$$16 = 48 - (512 - 48 \cdot 10) \cdot 1$$

$$16 = \underline{48} - 512 \cdot 1 + \underline{48 \cdot 10}$$

$$16 = 48 \cdot 11 - 512 \cdot 1$$

$$16 = 48 \cdot (11) + 512 \cdot (-1)$$

Teoría de números

- Expresar el $\text{mcd}(322, 51) = 1$ como una combinación lineal

$$322 = 51 \cdot 6 + 16$$

$$51 = 16 \cdot 3 + 3$$

$$16 = 3 \cdot 5 + 1$$

$$3 = 1 \cdot 3 + 0$$

$$16 = 322 - 51 \cdot 6$$

$$3 = 51 - 16 \cdot 3$$

$$1 = 16 - 3 \cdot 5$$

$$1 = 16 - (51 - 16 \cdot 3) \cdot 5$$

$$1 = 16 + (5) 51 + (15) 16$$

$$1 = (16) 16 + (5) 51$$

$$1 = 16(322 - 51(6)) + (5) 51$$

$$1 = (16) 322 - (96) 51 + (5) 51$$

$$1 = (16) 322 + (-101) 51$$

$$1 = \underline{(16)} 322 + \underline{(-101)} 51$$

Teoría de números

- Exprese el $\text{mcd}(322, 51) = 1$ como una combinación lineal

$$322 = 51 \cdot 6 + 16 \qquad 16 = 322 - 51 \cdot 6$$

$$51 = 16 \cdot 3 + 3 \qquad 3 = 51 - 16 \cdot 3$$

$$16 = 3 \cdot 5 + 1 \qquad 1 = 16 - 3 \cdot 5$$

$$3 = 1 \cdot 3 + 0$$

Teoría de números

- Exprese el $\text{mcd}(322, 51) = 1$ como una combinación lineal

$$322 = 51 \cdot 6 + 16$$

$$16 = 322 - 51 \cdot 6$$

$$51 = 16 \cdot 3 + 3$$

$$3 = 51 - 16 \cdot 3$$

$$16 = 3 \cdot 5 + 1$$

$$1 = 16 - 3 \cdot 5$$

$$3 = 1 \cdot 3 + 0$$

$$1 = 322 \cdot (16) + 51 \cdot (-101)$$

Teoría de números

- Expresar el $\text{mcd}(235, 37) = 1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$13 = 235 - 37 \times 6$$

$$11 = 37 - 13 \times 2$$

$$2 = 13 - 11 \times 1$$

$$1 = 11 - 2 \times 5$$

$$1 = 11 - 5(13 - 11 \times 1)$$

$$1 = 11 - 5 \times 13 + 5 \times 11$$

$$1 = 6(11) - 5 \times 13$$

$$1 = 6(37 - 13 \times 2) - 5 \times 13$$

$$1 = (6)37 - (17)13$$

$$1 = (6)37 - 17 \times 13$$

$$1 = (6)37 - \underline{17}(235 - 37 \times 6)$$

$$1 = (108)37 - (17)235$$

$$1 = (-17)235 + (108)37$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11 \qquad 11 = 37 - 13 \cdot 2$$

$$13 = 11 \cdot 1 + 2 \qquad 2 = 13 - 11 \cdot 1$$

$$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 2 \cdot 5$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11 \qquad 11 = 37 - 13 \cdot 2$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 13 \cdot 5 + 11 \cdot 5 = 11 \cdot 6 - 13 \cdot 5$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13 \qquad 13 = 235 - 37 \cdot 6$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$1 = 37 \cdot 6 - 13 \cdot 12 - 13 \cdot 5 = 37 \cdot 6 - 13 \cdot 17$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Exprese el $\text{mcd}(235, 37) = 1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot 6 - (235 - 37 \cdot 6) \cdot 17$$

Teoría de números

- Exprese el $\text{mcd}(235,37)=1$ como una combinación lineal

$$235 = 37 \cdot 6 + 13$$

$$37 = 13 \cdot 2 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 37 \cdot 6 - 235 \cdot 17 + 37 \cdot 102$$

$$1 = 37 \cdot 108 - 235 \cdot 17$$

$$1 = 37 \cdot (108) + 235 \cdot (-17)$$

Teoría de números

- Expresar el $\text{mcd}(426, 37)$ como una combinación lineal

$$\text{mcd}(426, 37) = \underline{1} = 426 \cdot (\underline{2}) + 37 \cdot (\underline{-23})$$

$$\begin{array}{l|l} 426 = 37 \times 11 + 19 & 19 = 426 - 37 \times 11 \\ 37 = 19 \times 1 + 18 & 18 = 37 - 19 \times 1 \\ 19 = 18 \times 1 + 1 & 1 = 19 - 18 \times 1 \end{array}$$

$$1 = 19 - (37 - 19 \times 1)$$

$$1 = 19(2) - 37$$

$$1 = (426 - 37 \times 11)(2) - 37$$

$$1 = (2)(426) - (22)(37) - 37$$

$$1 = 426(2) + 37(-23)$$

Teoría de números

El inverso de a mod m

- Dado a mod m , su inverso se denota como \overline{a}

Teoría de números

El inverso de $a \bmod m$

- Dado $a \bmod m$, su inverso se denota como \overline{a}
- Se cumple que $\overline{a} \cdot a \equiv 1 \pmod{m}$

$$\overline{a} \cdot a \bmod m = 1 \bmod m$$

Teoría de números

El inverso de $a \bmod m$

- Dado $a \bmod m$, su inverso se denota como \overline{a}
- Se cumple que $\overline{a} \cdot a \equiv 1 \pmod{m}$

Se tiene $3 \bmod 7$

$$\overline{a} = -2$$

Se puede verificar que:

$$(-2) \cdot 3 \equiv 1 \pmod{7}$$

$$-6 \bmod 7 \equiv 1 \bmod 7$$

$$1 = 1$$

Teoría de números

El inverso de a mod m

- Solo existe un inverso si $\text{mcd}(a,m)=1$

Teoría de números

El inverso de $a \bmod m$

- Para encontrar \overline{a} , calcule $\text{mcd}(a, m)$, debe ser 1
- Expresa $\text{mcd}(a, m) = 1$ como una combinación lineal

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

- El coeficiente que acompaña a a , es decir s , es el inverso \overline{a}

Teoría de números

- Encuentre el inverso de $235 \bmod 37$

$$\gcd(235, 37) = 1$$

$$235 = 37 \times 6 + 13$$

$$37 = 13 \times 2 + 11$$

$$13 = 11 \times 1 + 2$$

$$11 = 2 \times 5 + 1$$

$$13 = 235 - 37 \times 6$$

$$11 = 37 - 13 \times 2$$

$$2 = 13 - 11 \times 1$$

$$1 = 11 - 2 \times 5$$

$$1 = 11 - 5(13 - 11 \times 1)$$

$$1 = (6)11 - 5 \times 13$$

$$1 = (6)(37 - 13 \times 2) - 5 \times 13$$

$$1 = (6)37 - (17)13$$

$$1 = 6(37) - (17)(235 - 37 \times 6)$$

$$1 = 6(37) - (17)(235) + (102)37$$

$$1 = (-17)235 + (108)37$$

$$2^{-1} = -17$$

Teoría de números

- $\text{mcd}(235, 37) = 1$
- $1 = 235 \cdot (-17) + 37 \cdot (108)$

Teoría de números

- $\text{mcd}(235, 37) = 1$
- $1 = 235 \cdot (-17) + 37 \cdot (108)$
- **-17 es el inverso de 235 mod 37**

Teoría de números

- Se puede verificar que

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

ya que

$$-17 \cdot 235 \equiv 1 \pmod{37}$$

$$-3995 \equiv 1 \pmod{37}$$

Teoría de números

- Encuentre el inverso de $3 \bmod 7$

$$\gcd(3, 7) = 1$$

$$7 = 3 \times 2 + 1$$

$$1 = 7 - 3 \times 2$$

$$1 = 3(-2) + 7$$

$$1 = 3 \times s + 7 \times t$$

$$a = 5, -2, -2$$

$$q = -z$$

$$-2 \times 3 \equiv 1 \pmod{7}$$

$$-6 \equiv 1 \pmod{7}$$

$$\begin{array}{cc} \gamma & \gamma \\ \downarrow & \downarrow \\ \mathbb{1} & \mathbb{1} \end{array}$$

Teoría de números

- Encuentre el inverso de 3 mod 7

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

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$. Ahora se expresa como combinación lineal

$$1 = 7 - 3 \cdot 2$$

$$1 = 3 \cdot (-2) + 7 \cdot (1)$$

- El inverso de 3 mod 7 es -2

Teoría de números

- Encuentre el inverso de $7 \bmod 3$

Teoría de números

- Encuentre el inverso de $7 \bmod 3$

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

$$3 = 1 \cdot 3 + 0$$

- Se verifica que $\text{mcd}(7,3)=1$. Ahora se expresa como combinación lineal

$$1 = 7 - 3 \cdot 2$$

$$1 = 3 \cdot (-2) + 7 \cdot (1)$$

- El inverso de $7 \bmod 3$ es 1

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$\bar{a} =$

$$\gcd(7, 26) = 1$$

3

$$1 = 5 - (2)(7 - 5 \times 1)$$

$$1 = (3)(5) - (2)(7)$$

$$26 = 7 \times 3 + 5$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

$$5 = 26 - 7 \times 3$$

$$2 = 7 - 5 \times 1$$

$$1 = 5 - 2 \times 2$$

$$1 = (3)(26 - 7 \times 3) - 2 \times 7$$

$$1 = (3)26 + (-11)7$$

$$a = -11$$

$$-11 \times 7 \equiv 1 \bmod 26$$

$$\bar{11} = 1$$

$$\begin{array}{r} -26 \\ -52 \\ -78 \end{array}$$

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5$$

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(26,7)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de **7 mod 26**

$$26 = 7 \cdot 3 + 5 \qquad 5 = 26 - 7 \cdot 3$$

$$7 = 5 \cdot 1 + 2 \qquad 2 = 7 - 5 \cdot 1$$

$$5 = 2 \cdot 2 + 1 \qquad 1 = 5 - 2 \cdot 2$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5 \qquad 5 = 26 - 7 \cdot 3$$

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

$$5 = 2 \cdot 2 + 1 \qquad 1 = 5 - (7 - 5 \cdot 1) \cdot 2 = 5 \cdot 3 - 7 \cdot 2$$

$$2 = 1 \cdot 2 + 0$$

Teoría de números

- Encuentre el inverso de 7 mod 26

$$26 = 7 \cdot 3 + 5$$

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = (26 - 7 \cdot 3) \cdot 3 - 7 \cdot 2$$

Teoría de números

- Encuentre el inverso de $7 \bmod 26$

$$26 = 7 \cdot 3 + 5$$

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 26 \cdot 3 - 7 \cdot 9 - 7 \cdot 2 = 26 \cdot 3 - 7 \cdot 11$$

$$1 = 26 \cdot (3) + 7 \cdot (-11)$$

Teoría de números

- Encuentre el inverso de **7 mod 26**

$$26 = 7 \cdot 3 + 5$$

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

$$5 = 2 \cdot 2 + 1$$

$$1 = 26 \cdot 3 - 7 \cdot 9 - 7 \cdot 2 = 26 \cdot 3 - 7 \cdot 11$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 26 \cdot (3) + 7 \cdot (-11)$$

- Como $1 = 26 \cdot (3) + 7 \cdot (-11)$, el inverso de **7 mod 26** es -11

Teoría de números

Encuentre el inverso de:

$$\bar{a} =$$

$$5 \bmod 7$$

$$a\bar{a} \equiv 1 \bmod m$$

$$\gcd(5, 7) = 1$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 7 - 5 \times 1$$

$$1 = 5 - 2 \times 2$$

$$1 = 5 - 2(7 - 5 \times 1)$$

$$1 = (-2)5 + (4)7$$

$$\boxed{\bar{a} = 3}$$

$$3 \times 5 \equiv 1 \bmod 7$$

$$\underbrace{15}_{1} \equiv \underbrace{1}_{1} \bmod 7$$

Teoría de números

- Encuentre el inverso de **5 mod 7**

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de **5 mod 7**

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

$$1 = 5 \cdot (3) + 7 \cdot (-2)$$

Teoría de números

- Encuentre el inverso de **5 mod 7**

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

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(5,7)=1$. Ahora se expresa como combinación lineal

$$1 = 5 \cdot (3) + 7 \cdot (-2)$$

- El inverso de **5 mod 7** es 3

Teoría de números

Encuentre el inverso de:

- $3 \bmod 17$

Teoría de números

- Encuentre el inverso de 3 mod 17

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de 3 mod 17

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

$$1 = 3 \cdot (6) + 17 \cdot (-1)$$

Teoría de números

- Encuentre el inverso de **3 mod 17**

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- Se verifica que $\text{mcd}(3,17)=1$. Ahora se expresa como combinación lineal

$$1 = 3 \cdot (6) + 17 \cdot (-1)$$

- El inverso de **3 mod 17** es 6

Teoría de números

Encuentre el inverso de:

• 9 mod 32

$$\boxed{\bar{9} = -7}$$

$$32 = 9 \times 3 + 5$$

$$9 = 5 \times 1 + 4$$

$$5 = 4 \times 1 + 1$$

$$5 = 32 - 9 \times 3$$

$$4 = 9 - 5 \times 1$$

$$1 = 5 - 4 \times 1$$

$$1 = 5 - 9 + 5 \times 1$$

$$1 = (2)5 - 9$$

$$1 = (2)(32 - 9 \times 3) - 9$$

$$1 = (2)32 + (-7)9$$

Teoría de números

- Encuentre el inverso de 9 mod 32

$$32 = 9 \cdot 3 + 5$$

$$9 = 5 \cdot 1 + 4$$

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

- Se verifica que $\text{mcd}(9,32)=1$. Ahora se expresa como combinación lineal

Teoría de números

- Encuentre el inverso de 9 mod 32

$$32 = 9 \cdot 3 + 5$$

$$9 = 5 \cdot 1 + 4$$

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

- Se verifica que $\text{mcd}(9,32)=1$. Ahora se expresa como combinación lineal

$$1 = 9 \cdot (-7) + 32 \cdot (2)$$

Teoría de números

- Encuentre el inverso de **9 mod 32**

$$32 = 9 \cdot 3 + 5$$

$$9 = 5 \cdot 1 + 4$$

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

- Se verifica que $\text{mcd}(9,32)=1$. Ahora se expresa como combinación lineal

$$1 = 9 \cdot (-7) + 32 \cdot (2)$$

- El inverso de **9 mod 32** es **-7**