



Actividad 2.-Inverso multiplicativo

Con la función de Euler calcula

$$\phi(27) = 18$$

$$\phi(239) = 238$$

$$\phi(256) = 128$$

$$\phi(41895) = 18144$$

Por factorización en números primos encuentra:

$$\gcd(482, 1180) = 2$$

$$\gcd(12345, 11111) = 1$$

Con el algoritmo de Euclides (factorización del número mayor en términos del número menor) encuentra:

$$\gcd(17, 27) = 1$$

$$\gcd(239, 97) = 1$$

Con el algoritmo extendido de euclides encuentra

$$97^{-1} \bmod 239 = 69$$

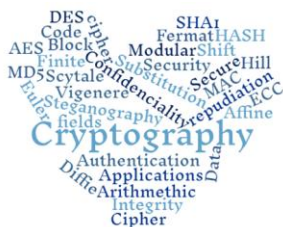
$$17^{-1} \bmod 27 = 8$$

Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.

M. en C. Nidia A. Cortez Duarte





Actividad 2.-Inverso multiplicativo

Actividad de Classroom

Obtener:

$$\phi(27) = 3^3 \left(1 - \frac{1}{3}\right) = 3^3 \left(\frac{2}{3}\right) = 3^2(2) = 9(2) = 18$$
$$27 = 3 \times 3 \times 3$$
$$\therefore \phi(27) = 18$$
$$\phi(239) = 239 - 1 = 238$$
$$239 \text{ es primo} \quad \phi(239) = 238$$
$$\phi(256) = 2^8 \left(1 - \frac{1}{2}\right) = 2^8 \left(\frac{1}{2}\right) = 2^7 = 128$$

256	2
128	2
64	2
32	2
16	2
8	2
4	2
2	2

$$\phi(256) = 128$$
$$\phi(41895) = 3^2 \cdot 5 \cdot 7^2 \cdot 19 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{19}\right)$$
$$= 3^2 \cdot 5 \cdot 7^2 \cdot 19 \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) \left(\frac{18}{19}\right)$$
$$= 3 \cdot 2 \cdot 4 \cdot 6 \cdot 7 \cdot 18 = 18144$$
$$\phi(41895) = 18144$$

41895	3
13965	3
4655	5
931	7
133	7
19	19
1	



Actividad 2.-Inverso multiplicativo

Por ATE

$$97^{-1} \bmod 239 = 69$$

$$\text{gcd}(97, 239) = 1$$

$$239 = 97(2) + 45 \quad ; \quad 45 = 239 - 97(2) \quad \dots d$$

$$97 = 45(2) + 7 \quad ; \quad 7 = 97 - 45(2) \quad \dots c$$

$$45 = 7(6) + 3 \quad ; \quad 3 = 45 - 7(6) \quad \dots b$$

$$7 = 3(2) + 1 \quad ; \quad 1 = 7 - 3(2) \quad \dots a$$

$$3 = 1(3) + 0$$

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

\swarrow
Sub b

$$1 = 7 - (45 - 7(6))2$$

$$1 = 7 - 45(2) + 7(12)$$

$$1 = 7(13) - 45(2)$$

\swarrow
Sub c

$$1 = (97 - 45(2))13 - 45(2)$$

$$1 = 97(13) - 45(26) - 45(2)$$

$$1 = 97(13) - 45(28)$$

\swarrow
Sub d

$$1 = 97(13) - 28(239 - 97(2))$$

$$1 = 97(13) - 239(28) + 97(56)$$

$$1 = 97(69) - 239(28)$$

$$1 = ax + by$$

$$1 = 97(69) + 239(28)$$

$$a^{-1} \bmod b = x$$

$$97^{-1} \bmod 239 = 69$$

Comprobación

$$97(69) \bmod 239 = 6693 \bmod 239$$

$$97(69) \bmod 239 = 1$$



Actividad 2.-Inverso multiplicativo

$$17^{-1} \bmod 27 = 8$$

~~$\gcd(17, 27)$~~

$$27 = 17(1) + 10 \quad ; \quad 10 = 27 - 17 \quad -d$$

$$17 = 10(1) + 7 \quad ; \quad 7 = 17 - 10 \quad -c$$

$$10 = 7(1) + 3 \quad ; \quad 3 = 10 - 7 \quad -b$$

$$7 = 3(2) + 1 \quad ; \quad 1 = 7 - 3(2) \quad -a$$

$$3 = 1(3) + 0$$

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

Sub. b

$$1 = 7 - 2(10 - 7)$$

$$1 = 7 - 2(10) + 7(2)$$

$$1 = 7(3) - 2(10)$$

Sub. c

$$1 = (17 - 10)3 - 2(10)$$

$$1 = 17(3) - 10(3) - 2(10)$$

$$1 = 17(3) - 10(5)$$

Sub. d

$$1 = 17(3) - (27 - 17)(5)$$

$$1 = 17(3) - 27(5) + 17(5)$$

$$1 = 17(8) - 27(5)$$

$$1 = ax + by$$

$$1 = 17(8) + 27(5)$$

$$a^{-1} \bmod b = x$$

$$17^{-1} \bmod 27 = 8$$

Comprobación

$$17(8) \bmod 27 = 136 \bmod 27 = 1$$

$$17(8) \bmod 27 = 1$$