d. Probar que 3 es raíz primitiva módulo 43, y hallar $\log_3 38 \in \mathbb{Z}_{42}$.

Ejercicio 7. Para cada una de las siguientes congruencias: determinar si existe solución, y en caso afirmativo hallar una solución.

a. $x^{11} \equiv 38 \pmod{43}$.

b. $x^{27} \equiv 38 \pmod{43}$.

c. $x^{20} \equiv 38 \pmod{43}$.

d. $28^z \equiv 38 \pmod{43}$

$\varphi(43) = 42 = 2 \cdot 21 = 2 \cdot 3 \cdot 7$

$3^{42/2} = 3^{21} \not\equiv 1 \ (43)$

$3^{42/3} = 3^{14} \not\equiv 1 \ (43)$

$3^{42/7} = 3^{6} \not\equiv 1 \ (43)$

n	$3^n \bmod 43$
0	3
1	9
2	$81 \equiv -5$
3	25
4	$625 \equiv 23$

$3^{21} = 3^{16+4+1} = 3^4 \cdot 3^2 \cdot 3^0 \equiv 23 \cdot (-5) \cdot 3$

$625 \ \boxed{43}$
$195 \ \ 14$
23

$= 69 \cdot (-5) \equiv 26 \cdot (-5) = -130 \equiv 42 \not\equiv 1 \ (43)$

$3^{14} = 3^{8+4+2} = 3^3 \cdot 3^2 \cdot 3^1 \equiv 25 \cdot (-5) \cdot 9 = 25 \cdot (-45) \equiv 25 \ (-2)$

$= -50 \equiv -7 \equiv 36 \not\equiv 1 \ (43)$

$3^6 = 3^{4+2} = 3^2 \cdot 3^1 \equiv (-5) \cdot 9 = -45 \equiv -2 \equiv 41 \not\equiv 1 \ (43)$

n	1	2	3	4
$3^n \bmod 43$	3	9	27	$81 \equiv 38$

$\Rightarrow 3^4 \equiv 38 \ (43)$

$\Rightarrow \log_3(38) \equiv 4 \ (42)$

a. $x^{11} \equiv 38 \pmod{43}$

$x \equiv 0 \Rightarrow x^{11} \equiv 0^{11} = 0 \not\equiv 38 \ (43)$

$\Rightarrow x \in U(43) = \langle 3 \rangle \Rightarrow \exists k \in \mathbb{Z}_{42}, \ x = 3^k$

$(3^k)^{11} = 3^{11k} \equiv 3^4 \ (43) \iff 11k \equiv 4 \ (42) \Rightarrow$

$11k = 4 + 42q \iff 11k - 42q = 4$

$$\begin{pmatrix} 42 \\ 11 \end{pmatrix}$$

$$42 \cdot 5 + 11(-19) = 1$$

$$\begin{pmatrix} 11 \\ 9 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$$

$$\Rightarrow 11(-19) - 42(-5) = 1$$

$$\Rightarrow 11(-76) - 42(-20) = 4$$

$$\begin{pmatrix} 9 \\ 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$$

$$\Rightarrow K \equiv -76 \ (42)$$

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} -1 & 4 \\ 5 & -19 \end{pmatrix}$$

$$\Rightarrow K \equiv 8 \ (42)$$

$$\Rightarrow X \equiv 3^8 \ (43)$$

$$\Rightarrow X \equiv 25 \ (43)$$

Ex Julio 2020

Ejercicio 2. Hallar todas las soluciones del sistema de congruencias:

$$\begin{cases} x \equiv 82 \pmod{24} = 2^3 \cdot 3 \\ x \equiv 64 \pmod{90} = 2 \cdot 3^2 \cdot 5 \\ x \equiv 34 \pmod{100}\ 2^2 \cdot 5^2 \end{cases}$$

$$\Longleftrightarrow \begin{cases} X \equiv 82 \ (2^3) \\ X \equiv 82 \ (3) \\ X \equiv 64 \ (2) \\ X \equiv 64 \ (3^2) \\ X \equiv 64 \ (5) \\ X \equiv 34 \ (2^2) \\ X \equiv 34 \ (5^2) \end{cases} \Longleftrightarrow \begin{cases} X \equiv 2 \ (2^3) \\ X \equiv 1 \ (3) \\ X \equiv 0 \ (2) \\ X \equiv 1 \ (3^2) \\ X \equiv 4 \ (5) \\ X \equiv 2 \ (2^2) \\ X \equiv 9 \ (5^2) \end{cases}$$

$$\begin{cases} X \equiv 2 \ (2^3) \\ X \equiv 2 \ (2^2) \\ X \equiv 0 \ (2) \\ X \equiv 1 \ (3^2) \\ X \equiv 1 \ (3) \\ X \equiv 9 \ (5^2) \\ X \equiv 4 \ (5) \end{cases}$$

$$X = 2 + 2^3 \cdot q$$
$$= 2 + 2(2^2 q)$$
$$\Rightarrow X \equiv 2 \ (2)$$

$$\Longleftrightarrow \begin{cases} X \equiv 2 \ (2^3) \\ X \equiv 1 \ (3^2) \\ X \equiv 4 \ (5) \end{cases} \Longleftrightarrow \begin{cases} X \equiv 10 \ (8) \\ X \equiv 10 \ (9) \\ X \equiv 4 \ (5) \end{cases}$$

TCR

$$\Longleftrightarrow \begin{cases} X \equiv 10 \ (72) \\ X \equiv 4 \ (5) \end{cases} \Longleftrightarrow \begin{cases} X \equiv 154 \ (72) \\ X \equiv 154 \ (5) \end{cases} \Longleftrightarrow X \equiv 154 \ (360)$$

Ejercicio 4.

a. Considere el criptosistema RSA con módulo $n = pq$ y funciones de cifrado $E(x) = x^e \bmod n$ y descifrado $D(x) = x^d \bmod n$. Indique qué hipótesis deben satisfacer d y e y demuestre que

$$D(E(x)) \equiv x \pmod{n}$$

para todo $x \in \mathbb{Z}_n$.

b. Dados primos $p = 19$, $q = 29$ y $e = 5$, calcular explícitamente la función de descifrado D.

c. Descifrar el mensaje cifrado $x = 2$.

$D(x) = x^d \ (n)$ / $de \equiv 1 \ (\varphi(n))$

$\varphi(n) = \varphi(19 \cdot 29) = 18 \cdot 28 = 20 \cdot 28 - 2 \cdot 28 = 560 - 56 = 504$

$5d \equiv 1 \ (504) \Longrightarrow d \equiv 101 \ (504)$

$\Rightarrow D(x) = x^{101} \ (19 \cdot 29)$

$D(2) = 2^{101} \ (19 \cdot 29) \equiv y \iff \begin{cases} y \equiv 2^{101} \ (19) \\ y \equiv 2^{101} \ (29) \end{cases}$

$101 = 18 \cdot 5 + 11$

$101 = 28 \cdot 3 + 17$

$p \in \mathbb{P}, a \neq 0 \Rightarrow a^{p-1} \equiv 1 \ (p)$

$\Rightarrow 2^{101} = (2^{18})^5 \cdot 2^{11} \equiv 2^{11} \ (19)$

$2^{101} = (2^{28})^3 \cdot 2^{17} \equiv 2^{17} \ (29)$

$\Rightarrow \begin{cases} y \equiv 2^{11} \ (19) \\ y \equiv 2^{17} \ (29) \end{cases}$

n	$2^{2^n} \bmod 29$
0	2
1	4
2	16
3	$256 \equiv 24 \equiv -5$
4	$25 \equiv -4$

n	$2^{2^n} \bmod 19$
0	2
1	4
2	$16 \equiv -3$
3	9

$2^{11} = 2^{2^3} \cdot 2^{2^1} \cdot 2^{2^0} \equiv 9 \cdot 4 \cdot 2$

$= 18 \cdot 4 \equiv -4 \equiv 15$

$2^{17} = 2^{2^4} \cdot 2^{2^1} \equiv -4 \cdot 4 = -16$

$\equiv 13$

$\Rightarrow \begin{cases} y \equiv 15 \ (19) \\ y \equiv 13 \ (29) \end{cases}$

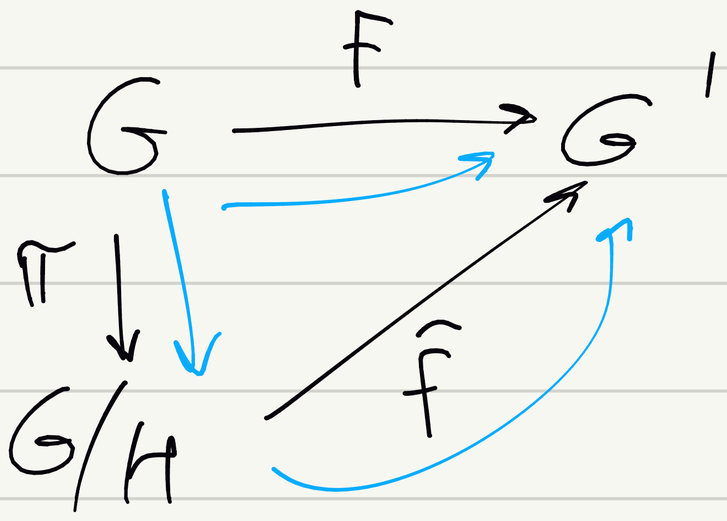
$290 - 58 = 232$

$$3^{39} \equiv 1 \ (7)$$

$3^6 \equiv 1 \ (7)$

$3^{39} = (3^6)^2 \cdot 3^3 \equiv 3^3 \equiv 6 \ (7)$

a) Sea G un grupo, H un subgrupo normal de G y la aplicación al cociente $\pi : G \to G/H$. Entonces demostrar que para todo morfismo de grupos $f : G \to G'$ tal que $H \subseteq Ker(f)$, existe un único morfismo de grupos $\hat{f} : G/H \to G'$ tal que $\hat{f} \circ \pi = f$.



$g' \in gH \iff$
$\exists h \in H,\ g' = gh$

$f(g') = f(gh) = f(g)\,F(h) = f(g)$