Ejercicio 7. Resolver las siguientes congruencias:

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

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

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

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

p primo impar, r raíz primitiva módulo p

$r^a \equiv r^b \pmod p \iff a \equiv b \pmod{p-1}$

$r^a \equiv r^b \pmod p \iff r^{a-b} \equiv 1 \pmod p \iff \bar{r}^{a-b} = \bar{1} \iff p-1 \mid a-b$

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

sabemos que 3 es raíz primitiva módulo 43

* $x \equiv 3^k \pmod{43}$ para algún $k \in \{1, \dots, 42\}$
* $38 \equiv 3^4 \pmod{43}$

$3^2 \equiv 9 \pmod{43}$

$3^3 \equiv 27 \pmod{43}$

$3^4 \equiv 81 \equiv 38 \pmod{43} \rightsquigarrow \log_3 38 = 4$

$x^{20} \equiv 38 \pmod{43} \iff 3^{20k} \equiv 3^4 \pmod{43}$

$\iff 20k \equiv 4 \pmod{42}$

$42 = 2 \cdot 3 \cdot 7$

$$\iff \begin{cases} 20k \equiv 4 \pmod 7 \iff 6k \equiv 4 \pmod 7 \\ 20k \equiv 4 \pmod 3 \iff 2k \equiv 1 \pmod 3 \\ 20k \equiv 4 \pmod 2 \iff 0 \equiv 0 \pmod 2 \end{cases}$$

$6y \equiv 1 \pmod 7$

$$\iff \begin{cases} 6k \equiv 4 \pmod 7 \\ 2k \equiv 1 \pmod 3 \end{cases}$$

$$\iff \begin{cases} 6 \cdot 6k \equiv 6 \cdot 4 \pmod 7 \\ 2 \cdot 2k \equiv 2 \cdot 1 \pmod 3 \end{cases}$$

$$\iff \begin{cases} k \equiv 3 \pmod 7 \rightsquigarrow \overset{\times}{3}, \overset{\times}{10}, \overset{\checkmark}{17}, 24, 31, \dots \\ k \equiv 2 \pmod 3 \qquad\qquad 17 \equiv 2 \pmod 3 \end{cases}$$

$\iff k \equiv 17 \pmod{21}$

$x^{20} \equiv 38 \pmod{43} \iff k \equiv 17 \pmod{21}$

$x \equiv 3^k \pmod{43}$

$3^a \equiv 3^b \pmod{43} \iff a \equiv b \pmod{42}$

$k \equiv 17 \pmod{21} \rightsquigarrow$ 17, 38, 59, 80 (+21, +21, +21; +42)

$$k \equiv 17 \pmod{21} \iff \begin{cases} k \equiv 17 \pmod{42} \\ \text{o} \\ k \equiv 38 \pmod{42} \end{cases}$$

$$\iff \begin{cases} 3^k \equiv 3^{17} \pmod{43} \\ \text{o} \\ 3^k \equiv 3^{38} \pmod{43} \end{cases}$$

$$\iff \begin{cases} x \equiv 3^{17} \pmod{43} \\ \text{o} \\ x \equiv 3^{38} \pmod{43} \end{cases}$$

$x^{20} \equiv 38 \pmod{43}$ tiene dos soluciones $\begin{cases} x \equiv 3^{17} \pmod{43} \\ x \equiv 3^{38} \pmod{43} \end{cases}$

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

3 raiz primitiva modulo 43

* $38 \equiv 3^4 \pmod{43}$
* $28 \equiv 3^5 \pmod{43}$

$3^z \equiv 9 \pmod{43}$

$3^3 \equiv 27 \pmod{43}$

$3^4 \equiv 38 \pmod{43}$

$3^5 \equiv 38 \cdot 3 \equiv 114 \equiv 28 \pmod{43} \Rightarrow \log_3 28 = 5$

$28^z \equiv 38 \pmod{43} \iff 3^{5z} \equiv 3^4 \pmod{43}$

$\iff 5z \equiv 4 \pmod{42}$

$42 = 7 \cdot 3 \cdot 2$

$$\iff \begin{cases} 5z \equiv 4 \pmod 7 \\ 5z \equiv 4 \pmod 3 \iff 2z \equiv 1 \pmod 3 \\ 5z \equiv 4 \pmod 2 \iff z \equiv 0 \pmod 2 \end{cases}$$

$$\iff \begin{cases} 5z \equiv 4 \pmod 7 \\ 2z \equiv 1 \pmod 3 \\ z \equiv 0 \pmod 2 \end{cases}$$

$5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$

$5 \cdot 2 \equiv 10 \equiv 1 \pmod 3$

$$\iff \begin{cases} 3 \cdot 5z \equiv 3 \cdot 4 \pmod 7 \\ 5 \cdot 2z \equiv 5 \pmod 3 \\ z \equiv 0 \pmod 2 \end{cases}$$

$$\iff \begin{cases} z \equiv 5 \pmod 7 \Rightarrow 5, 12, 19, 26 \quad (\times, \times, \times, \checkmark) \\ z \equiv 2 \pmod 3 \quad 26 \equiv 2 \pmod 3 \\ z \equiv 0 \pmod 2 \quad 26 \equiv 0 \pmod 2 \end{cases}$$

$$\iff \boxed{z \equiv 26 \pmod{42}}$$

Método de cifrado de Vigenere

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

texto a cifrar: MANZANA

clave de cifrado: TRES

	M	A	N	Z	A	N	A	← texto a cifrar
	T	R	E	S	T	R	E	← clave de cifrado
número que le corresponde a cada letra →	12	0	13	26	0	13	0	
	20	18	4	19	20	18	4	
	32	18	17	45	20	31	4	← sumamos
	4	18	17	17	20	3	4	← reducimos modulo 28
	E	R	Q	Q	T	D	E	← texto cifrado

¿cómo hacer para intercambiar claves?

→ método de Diffie - Hellman

① Ana y Bernardo se ponen de acuerdo en un número primo p y una raiz primitiva g módulo p

② Ana elige un número n al azar (n es secreto)
→ calcula $g^n \pmod p$ y le envía el resultado a Bernardo

③ Bernardo elige un número m al azar (m es secreto)
→ calcula $g^m \pmod p$ y le envía el resultado a Ana

(4) la clave común es $c \equiv g^{nm} \pmod p$

$\rightarrow c \equiv (g^m)^n \pmod p$

$\rightarrow c \equiv (g^n)^m \pmod p$

Ejercicio 1.

a. Deseamos acordar una clave común con Romina usando el protocolo **Diffie-Hellman**. Elegimos el primo $p = 991$, y $g = 7$ como raíz primitiva módulo p; ambas de forma pública. Romina elige al azar, y en secreto, un número $n < p$, y nos envía públicamente $g^n \equiv 989 \pmod p$. Nosotros elegimos al azar $m = 11$ (secretamente).

i) ¿Cuál es la clave k común que acordamos con Romina?

ii) ¿Qué número tenemos que mandarle públicamente a Romina para que solamente ella pueda calcular la clave fácilmente?

b. Supongamos que deseamos comunicarnos con Romina a través de un **sistema Vigenere**, utilizando una palabra clave de 3 letras. Para esto tomamos la clave k común acordada con Romina en la parte anterior, y la escribimos en base 28:

$$k = L_2 28^2 + L_1 28 + L_0, \quad 0 \leq L_i < 28.$$

A partir de esto definimos la clave común como: $L_2 L_1 L_0$. Por ejemplo, si fuese $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$, la clave común sería `YAC`.

i) Cifrar los siguientes mensajes: `SIMULADOR`, `Y_WALTER`.

ii) Descifrar los siguientes mensajes enviados por Romina: `GZFAKPVP`, `NJÑJXDPX`.

a) $p = 991$ primo

7 raíz primitiva módulo 991

de Romina recibimos $7^n \equiv 989 \pmod{991}$

nosotros elegimos $m = 11$

i) cuál es la clave común k que acordamos?

$$k \equiv 7^{nm} \equiv (7^n)^m \equiv (989)^m \equiv 989^{11} \pmod{991}$$

$$\boxed{k \equiv 989^{11} \pmod{991}}$$

$989 \equiv -2 \pmod{991}$

$989^2 \equiv (-2)^2 \equiv 4 \pmod{991}$

$989^4 \equiv 4^2 \equiv 16 \pmod{991}$

$989^8 \equiv 16^2 \equiv 256 \pmod{991}$

$989^{11} \equiv 989^8 \cdot 989^2 \cdot 989 \pmod{991}$

$\equiv 256 \cdot 4 \cdot (-2) \pmod{991}$

$$\equiv 1024 \cdot (-2) \pmod{991}$$
$$\equiv -66 \pmod{991}$$
$$\equiv 925 \pmod{991}$$

$\Rightarrow$ la clave común es 925.

b) $p = 991$

$g = 7$ raíz primitiva módulo 991

nosotros elegimos $m = 11$

$\Rightarrow$ le tenemos que mandar a Romina:

$$7^{11} \pmod{991}$$

$$7^2 \equiv 49 \pmod{991}$$
$$7^4 \equiv 49 \cdot 49 \equiv 2401 \equiv 419 \pmod{991}$$
$$7^8 \equiv 419 \cdot 419 \equiv 154 \pmod{991}$$
$$7^{11} \equiv 7^8 \cdot 7^2 \cdot 7 \equiv 154 \cdot 49 \cdot 7 \equiv 299 \pmod{991}$$

tenemos que mandarle a Romina $7^m \equiv 299 \pmod{991}$

b. Supongamos que deseamos comunicarnos con Romina a través de un **sistema Vigenere**, utilizando una palabra clave de 3 letras. Para esto tomamos la clave k común acordada con Romina en la parte anterior, y la escribimos en base 28:

$$k = L_2 28^2 + L_1 28 + L_0, \quad 0 \leq L_i < 28.$$

A partir de esto definimos la clave común como: $L_2 L_1 L_0$. Por ejemplo, si fuese $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$, la clave común sería YAC.

i) Cifrar los siguientes mensajes: SIMULADOR, Y_WALTER.

ii) Descifrar los siguientes mensajes enviados por Romina: GZFAKPVP, NJÑJXDPX.

clave común 925.

* vamos 925 en base 28:

$$\begin{aligned} 925 &= 33 \cdot 28 + 1 \\ &= (28+5) \cdot 28 + 1 \\ &= 28^2 + 5 \cdot 28 + 1 \\ &= 1 \cdot 28^2 + 5 \cdot 28^1 + 1 \cdot 28^0 \end{aligned}$$

* la palabra clave para el cifrado de Vigenere es BFB

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

*

S I M U L A D O R

B F B B F B B F B

19 8 12 21 11 0 3 15 18

1 5 1 1 5 1 1 5 1

20 13 13 22 16 1 4 20 19 ← sumamos y reducimos módulo 28

T N N V P B E T S

mensaje cifrado