

Lista 1

1.

Divisibilidad 2

- Sabemos que un número es divisible por 2 si la última cifra de un número N es número par, es decir, que sea $\{0, 2, 4, 6, 8\}$

Siendo N de la forma $N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0$,

por lo que si a_0 es par $\rightarrow N \equiv 0 \pmod{2}$

si a_0 no es par $\rightarrow N \equiv 1 \pmod{2}$

Divisibilidad 3

- Sabemos que un número es divisible por 3 si la suma de los dígitos de un número N es divisible por 3, ya que:

$$10 \equiv 1 \pmod{3} \Rightarrow 10^k \equiv 1 \pmod{3} \quad k \geq 1$$

Tomando N como un número $N = a_n \cdot 10^n + \dots + a_0$

$$\Rightarrow N \equiv a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \pmod{3}$$

$$\Rightarrow N \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + \dots + a_0 \pmod{3}$$

$$\Rightarrow N \equiv a_n + a_{n-1} + \dots + a_0 \pmod{3}$$

Divisibilidad 5

- Sabemos que un número es divisible por 5 si su último dígito es un 5 o un 0. Suponiendo un número $N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0$

Sabemos que $10 \equiv 0 \pmod{5} \Rightarrow 10^k \equiv 0 \pmod{5}$ para $k \geq 1$

$$\Rightarrow N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0$$

$$N \equiv a_n \cdot 0 + a_{n-1} \cdot 0 + \dots + a_0 \pmod{5}$$

$$N \equiv a_0 \pmod{5}$$

• Divisibilidad 11

Un número es divisible por 11 si $N \equiv 0 \pmod{11}$, si ponemos los términos utilizando base 10 $\Rightarrow 10 \equiv -1 \pmod{11}$, si escalamos para k positivos:

$$10^0 \equiv 1 \pmod{11}$$

$$10^1 \equiv -1 \pmod{11}$$

$$10^2 \equiv 1 \pmod{11}$$

$$10^3 \equiv -1 \pmod{11}$$

Por tanto, las potencias pares tendrán residuo 1, mientras que las impares tendrán -1.

$$N \equiv a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \pmod{11}$$

$$N \equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \dots + a_0 \pmod{11}$$

$$N \equiv (a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n \cdot a_n) \pmod{11}$$

Por tanto, un número es divisible por 11 si la suma alterna de sus dígitos es divisible por 11.

• Divisibilidad 13

Utilizando $40 \equiv 1 \pmod{13}$, tenemos que escribir un número N en términos de 40, ya que como sabemos que $40 \equiv 1 \pmod{13}$, por lo cual dividiremos N en bloques de dos dígitos comenzando por el final, si N tiene un número impar de dígitos, el primer bloque puede ser de un dígito.

Por lo que ahora en vez de trabajar con potencias de 10, vamos a agrupar los números de N en bloques de 2 en 2.

$$40 \equiv 1 \pmod{13}$$

$$40^k \equiv 1^k \pmod{13} \Rightarrow 40^k \equiv 1 \pmod{13}$$

$$\text{Ej: } 74289 \Rightarrow N = 74 \cdot 100 + 28 \cdot 1 + 9$$

$$\rightarrow \text{Como sabemos que } 100 = 40 \cdot 2 + 20 \text{ y } 40 \equiv 1 \pmod{13}$$

$$\Rightarrow 100 \equiv 1 \pmod{13}$$

$$\Rightarrow N \equiv 74 \cdot 1 + 28 \cdot 1 + 9 \pmod{13}$$

$$N \equiv 111 \pmod{13}$$

$$\rightarrow \text{Calculamos } 111 : 13 = 8 \text{ con } 7 \Rightarrow 111 \equiv 7 \pmod{13}$$

\therefore no es divisible por 13

2. Como x es un generador, podemos escribir todos los elementos de G
 x^k siendo $k \in \{0, 1, 2, \dots, n-1\}$

Con los elementos $y_1 = x^{n_1}$, $y_2 = x^{n_2}$ queremos encontrar un m
tal que $y_1^m = y_2$, por lo que despejando:

$$(x^{n_1})^m = x^{n_2}$$

$$x^{n_1 m} = x^{n_2}$$

Como sabemos que x es un generador, podemos cancelar dichas potencias
y ponerlas módulo n .

$$n_1 \cdot m \equiv n_2 \pmod{n} \Rightarrow m \equiv n_2 \cdot n_1^{-1} \pmod{n}$$

Para hallar solución sabemos que m existiría si n_1 tiene inverso,
para ello si n y n_1 son coprimos $\gcd(n, n_1) \mid n_2$, se podría
obtener solución utilizando el Algoritmo Extendido de Euclides.

Por lo que si $\gcd(n, n_1) = 1 \Rightarrow$ siempre existiría un inverso multiplicativo
 n_1^{-1} que resuelva la ecuación $m \equiv n_2 \cdot n_1^{-1} \pmod{n}$

3. Para determinar los enteros de x , descompondremos el módulo en
sus factores primos y utilizaremos el T. Chino del Resto

i) $4x \equiv 3 \pmod{385}$ $385 = 5 \cdot 7 \cdot 11$

$$\hookrightarrow \begin{cases} 4x \equiv 3 \pmod{5} \\ 4x \equiv 3 \pmod{7} \\ 4x \equiv 3 \pmod{11} \end{cases}$$

• $4x \equiv 3 \pmod{5} \Rightarrow x \equiv 3 \cdot 4^{-1} \pmod{5}$
 $\Rightarrow x \equiv 3 \cdot 4 \pmod{5} \Rightarrow x \equiv 2 \pmod{5}$

Como $4 \cdot 4 \equiv 1 \pmod{5}$
 \Rightarrow el inv. de 4 en mod 5
es 4

• $4x \equiv 3 \pmod{7} \Rightarrow x \equiv 3 \cdot 4^{-1} \pmod{7}$
 $x \equiv 3 \cdot 2 \pmod{7} \Rightarrow x \equiv 6 \pmod{7}$

Como $4 \cdot 2 \equiv 1 \pmod{7}$
 \Rightarrow el inv. de 4 en mod 7
es 2

• $4x \equiv 3 \pmod{11} \Rightarrow x \equiv 3 \cdot 4^{-1} \pmod{11}$
 $x \equiv 3 \cdot 3 \pmod{11} \Rightarrow x \equiv 9 \pmod{11}$

Como $4 \cdot 3 \equiv 1 \pmod{11}$
 $4^{-1} = 3$

Aplicando el Teorema chino de los restos:

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 6 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases}$$

Tomamos 2 ecuaciones como $x \equiv 2 \pmod{5}$ y $x \equiv 6 \pmod{7}$ y las expresamos como

$$x \equiv 2 \pmod{5} = X = 5 \cdot K + 2 \rightarrow \text{Sustituimos } X \text{ en el } 2^\circ \text{ Ec.}$$

$$5K + 2 \equiv 6 \pmod{7}$$

$$5K \equiv 4 \pmod{7}$$

$$\text{Como } 5 \cdot 3 \equiv 1 \pmod{7}$$

$$K \equiv 4 \cdot 5^{-1} \pmod{7}$$

$$5^{-1} = 3$$

$$K \equiv 4 \cdot 3 \pmod{7}$$

$$K \equiv 5 \pmod{7}$$

Por lo tanto $K = 7 \cdot m + 5$; sustituimos en $X = 5K + 2$ y obtenemos

$$X = 5(7m + 5) + 2 \Rightarrow X = 35m + 25 + 2 \Rightarrow X = 35m + 27$$

Expresándolo de forma modular: $X \equiv 27 \pmod{35}$

Por último, utilizamos esta ecuación y la última para obtener la sig. relación

$$X \equiv 27 \pmod{35} \rightarrow X = 35K + 27$$

$$X \equiv 9 \pmod{11} \rightarrow X = 11m + 9$$

\therefore Sustituimos: $35K + 27 \equiv 9 \pmod{11}$

$$K \equiv -18 \cdot 35^{-1} \pmod{11}$$

$$\text{Como } 35 \equiv 2 \pmod{11}$$

$$K \equiv 4 \cdot 35^{-1} \pmod{11}$$

$$K \equiv 4 \cdot 2^{-1} \pmod{11}$$

$$\text{Como } 2 \cdot 6 \equiv 1 \pmod{11}$$

$$K \equiv 4 \cdot 6 \pmod{11}$$

$$K \equiv 2 \pmod{11} \rightarrow K = 11m + 2$$

\therefore Sustituimos nuevamente.

$$X = 35(11m + 2) + 27$$

$$X = 385m + 70 + 27 \Rightarrow X = 385m + 97$$

$$\hookrightarrow X \equiv 97 \pmod{385}$$

Por tanto, concluimos que los enteros x que satisfacen la congruencia

$$4x \equiv 3 \pmod{385} \text{ son } x \equiv 97 \pmod{385}$$

$$\text{O } x = 97 + 385K; \text{ siendo } K \text{ un entero } //$$

$$ii) 128x \equiv 10 \pmod{17}$$

Para este caso, operamos de la misma forma que el anterior caso, pero antes simplificaremos 128 donde $128 \div 17 = 9 \Rightarrow$

$$128x \equiv 10 \pmod{17} \Leftrightarrow 9x \equiv 10 \pmod{17} \Rightarrow x \equiv 10 \cdot 9^{-1} \pmod{17}$$

para encontrar el 9^{-1} , $\gcd(9, 17) = 1$ es decir que son coprimos,

Como se satisface podemos usar el Algoritmo Extendido de Euclides

que tenemos programado en las prácticas y obtenemos que el

inverso modular de 9 módulo 17 es 2 ya que $9 \cdot 2 \equiv 1 \pmod{17}$

(esta filosofía es la necesaria a seguir, pero realmente podemos hacerla de cabeza como en el apartado i).)

$$x \equiv 10 \cdot 2 \pmod{17} \Rightarrow x \equiv 3 \pmod{17}$$

por tanto $128x \equiv 10 \pmod{17} = x \equiv 3 \pmod{17}$ donde los

enteros de x vienen definidos como $x = 3 + 17k$ siendo k entero,

$$iii) 2047 \equiv 3 \pmod{1024} \quad \text{Operamos de igual manera}$$

$$2047 \div 1024 = 1023 \Rightarrow 1023 \equiv 3 \pmod{1024}$$

$$x \equiv 3 - 1023 \pmod{1024}$$

$$x \equiv -1020 \pmod{1024} \rightarrow \text{lo expresamos en base a el módulo.}$$

$$x \equiv 4 \pmod{1024}$$

Por tanto, los números x enteros que se satisfacen son $x \equiv 4 \pmod{1024}$

$$o \quad x = 4 + 1024k \text{ siendo } k \text{ un entero.}$$

4.

$$\begin{cases} 3x \equiv 1 \pmod{4} \\ 2x \equiv 3 \pmod{25} \end{cases}$$

Para resolverlo, utilizaremos el Teorema Chino de los restos, pero antes, resolveremos la primera congruencia y simplificaremos la segunda.

• $3x \equiv 1 \pmod{4} \Rightarrow x \equiv 1 \cdot 3^{-1} \pmod{4}$ Como $3 \cdot 3 \equiv 1 \pmod{4}$
 $x \equiv 1 \cdot 3 \pmod{4}$ $3^{-1} = 3$
 $x \equiv 3 \pmod{4}$

• $2x \equiv 3 \pmod{25} \rightarrow$ Simplificamos 25 en factores primos $\Rightarrow 25 = 5 \cdot 5$
(Aunque en este caso como es sencillo, vamos a continuar como lo haríamos normalmente.)

$x \equiv 3 \cdot 2^{-1} \pmod{25}$ Como $2 \cdot 13 \equiv 1 \pmod{25}$
 $x \equiv 3 \cdot 13 \pmod{25}$ $2^{-1} = 13$
 $x \equiv 39 \pmod{25}$
 $x \equiv 14 \pmod{25}$

\rightarrow Recopilamos las congruencias resultantes en un sistema de Ecuaciones.

$$\begin{cases} x \equiv 3 \pmod{4} \rightarrow x = 4m + 1 \\ x \equiv 14 \pmod{25} \rightarrow x = 25k + 14 \rightarrow \text{Sustituimos en la 1ª congruencia} \end{cases}$$

$$25k + 14 \equiv 3 \pmod{4} \Rightarrow 25k \equiv -11 \pmod{4}$$

$$25k \equiv 1 \pmod{4} \quad \text{Como } 25 \cdot 1 \equiv 1 \pmod{4}$$

$$k \equiv 1 \cdot 25^{-1} \pmod{4} \quad 25^{-1} = 1$$

$$k \equiv 1 \cdot 1 \pmod{4}$$

$$k \equiv 1 \pmod{4}$$

Utilizamos $k = 4m + 1$ y sustituimos en la 2ª congruencia

$$x = 25 \cdot (4m + 1) + 14 \Rightarrow x = 100m + 25 + 14 \Rightarrow x = 100m + 39$$

$$\therefore x \equiv 39 \pmod{100}$$

Por consiguiente, podemos concluir que los dos últimos dígitos son 39. //

5.

Para calcular las siguientes potencias, podemos utilizar el Teorema de Fermat (si p es primo y a no es divisible por p) o también podemos utilizar la exponenciación modular (binaria).

El Teorema de Fermat nos da una solución con relativa simplicidad pero no podemos calcular dicho resultado sin la presencia de un ordenador (que no sea o mano), es por ello que utilizaremos la exponenciación modular vista en clase.

i) $31^{96} \pmod{359}$

Primero tenemos que calcular 96 en base 2 $\Rightarrow 96 = 2^5 + 2^6$

$$31^{96} \pmod{359}$$

$$31^{(2^5+2^6)} \pmod{359}$$

$$31^{(2^5+2^6)} = 31^{(2^5)} \cdot 31^{(2^6)} = 31^{(2^5)} \cdot 31^{(2^4)} \cdot 31^{(2^3)} \cdot 31^{(2^2)} \cdot 31^{(2^1)} \cdot 31^{(2^0)}$$

importante
 \hookrightarrow

$$31^0 \equiv 1 \pmod{359}$$

$$31^1 \equiv 243 \pmod{359}$$

$$1 \cdot 243^0 \equiv 31 \pmod{359}$$

\rightarrow Es 1 por la iteración 0.

$$2 \quad 243^2 \equiv 173 \pmod{359}$$

$$1 \cdot 173^0 \equiv 31 \pmod{359}$$

$$3 \quad 173^2 \equiv 132 \pmod{359}$$

$$1 \cdot 132^0 \equiv 31 \pmod{359}$$

$$4 \quad 132^2 \equiv 192 \pmod{359}$$

$$1 \cdot 192^0 \equiv 31 \pmod{359}$$

$$5 \quad 192^2 \equiv 246 \pmod{359}$$

$$1 \cdot 246^1 \equiv 246 \pmod{359}$$

$$6 \quad 246^2 \equiv 204 \pmod{359}$$

$$246 \cdot 204^1 \equiv 283 \pmod{359}$$

//

(i) $27^{33} \bmod 157 \rightarrow$ Procedemos de igual forma

$$33 = 100001_2 \rightarrow 33 = 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$27^{(1+2^5)} = \underbrace{(27^1)^1}_1 + \underbrace{(27^2)^0}_2 + \underbrace{(27^3)^0}_3 + \underbrace{(27^4)^0}_4 + \underbrace{(27^5)^0}_5 + \underbrace{(27^6)^1}_6$$

1 $27^1 \equiv 27 \bmod 157$

2 $27^2 \equiv 401 \bmod 157$

$27 \cdot 401 \equiv 27 \bmod 157$

3 $401 \equiv 153 \bmod 157$

$27 \cdot 153 \equiv 27 \bmod 157$

4 $153^2 \equiv 16 \bmod 157$

$27 \cdot 16 \equiv 27 \bmod 157$

5 $16^2 \equiv 99 \bmod 157$

$27 \cdot 99 \equiv 27 \bmod 157$

6 $99^2 \equiv 67 \bmod 157$

$27 \cdot 67 \equiv 82 \bmod 157 //$

(ii) $40^{65} \bmod 199 \rightarrow$ Mismo procedimiento

$$65 = 1000001_2 \rightarrow 65 = 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$40^{(1+2^6)} = \underbrace{(40^1)^1}_1 + \underbrace{(40^2)^0}_2 + \underbrace{(40^3)^0}_3 + \underbrace{(40^4)^0}_4 + \underbrace{(40^5)^0}_5 + \underbrace{(40^6)^0}_6 + \underbrace{(40^7)^1}_7$$

1 $40 \equiv 40 \bmod 199$

2 $40^2 \equiv 8 \bmod 199$

$40 \cdot 8 \equiv 40 \bmod 199$

3 $8^2 \equiv 64 \bmod 199$

$40 \cdot 64 \equiv 40 \bmod 199$

4 $64^2 \equiv 116 \bmod 199$

$40 \cdot 116 \equiv 40 \bmod 199$

5 $116^2 \equiv 123 \bmod 199$

$40 \cdot 123 \equiv 40 \bmod 199$

6 $123^2 \equiv 5 \bmod 199$

$40 \cdot 5 \equiv 40 \bmod 199$

7 $5^2 \equiv 25 \bmod 199$

$40 \cdot 25 \equiv 5 \bmod 199 -8- //$

6 Antes de nada, para comprobar que los sistemas tienen solución, deberemos de comprobar que los módulos de las ecuaciones dadas sean coprimos es decir $\gcd(n_1, n_2, n_3) = 1$; ya que si no se satisface, no podemos garantizar que tenga solución.

i)
$$\begin{cases} 1075x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$$

Vamos a operar de igual manera que en el ejercicio 3 i), no sin antes simplificar las congruencias anteriores ya que no están expresadas de manera correcta, no sin antes comprobar que $\gcd(8, 5, 3) = 1$. Para este problema, esto se satisface, (comprobado con código de prácticas) por lo que podemos continuar.

• $1075x \equiv 5312065 \pmod{8}$ expresamos en relación a mod 8

$$1x \equiv 1 \pmod{8}$$

• $36x \equiv 322 \pmod{5}$

$$1x \equiv 2 \pmod{5}$$

• $4x \equiv 7 \pmod{3}$

$$1x \equiv 1 \pmod{3}$$

→ Agrupando

$$\begin{cases} x \equiv 1 \pmod{8} \rightarrow x = 8k + 1 \\ x \equiv 2 \pmod{5} \quad x = 5m + 2 \\ x \equiv 1 \pmod{3} \end{cases}$$

Para resolverlo, agrupamos 2 ecuaciones (tomaré las 2 primeras)

$$\Rightarrow 8k + 1 \equiv 2 \pmod{5}$$

$$k \equiv 1 \cdot 8^{-1} \pmod{5}$$

$$\text{Como } 8 \cdot 2 \equiv 1 \pmod{5}; 8^{-1} = 2$$

$$k \equiv 1 \cdot 2 \pmod{5}$$

$$k \equiv 2 \pmod{5} \rightarrow k = 5m + 2; \text{ Sustituyendo en la 1}^\circ$$

$$x = 8 \cdot (5m + 2) + 1 \Rightarrow x = 40m + 16 + 1 \Rightarrow x = 40m + 17$$

$x \equiv 17 \pmod{40}$ → Ahora utilizamos esta congruencia con la 3ª Ec. por lo que tenemos

$$\begin{cases} x \equiv 17 \pmod{40} \rightarrow x = 40k + 17 \\ x \equiv 1 \pmod{3} \rightarrow x = 3m + 1 \end{cases}$$

$$40k + 17 \equiv 1 \pmod{3}$$

$$40k \equiv 1 - 17 \pmod{3}$$

$$40k \equiv -16 \pmod{3} \rightarrow \text{Expresamos en términos del módulo}$$

$$1k \equiv 2 \pmod{3}$$

$$k \equiv 2 \pmod{3} \rightarrow k = 3m + 2 \quad \text{Sustituimos en la 1ª Ec}$$

$$x = 40 \cdot (3m + 2) + 17 \Rightarrow x = 120m + 80 + 17 = 120m + 97$$

$$x \equiv 97 \pmod{120} //$$

$$(ii) \begin{cases} 2x \equiv 4 \pmod{6} \\ 8x \equiv 3 \pmod{13} \\ 12x \equiv 1 \pmod{18} \end{cases}$$

Podemos observar a simple vista que $18 = 6 \cdot 3$, por lo que van a compartir factores entre los módulos, resultando que ellos no sean coprimos. Comprobándolo obtenemos que $\gcd(8, 13)$

, $\gcd(6, 18) = 6$ y $\gcd(13, 18) = 1$. Por tanto no se cumple la condición necesaria para aplicar T.C.R., significando que aunque intentemos resolverlo, no encontraremos una solución.

$$(iii) \begin{cases} 2x \equiv 1 \pmod{3} \\ 8x \equiv 7 \pmod{11} \\ 5x \equiv 3 \pmod{13} \end{cases}$$

Como el gcd entre ellos es 1, esto significa que son coprimos entre ellos por tanto, existe solución. Seguimos el mismo método que en i)

$$\bullet 2x \equiv 1 \pmod{3}$$

$$x \equiv 1 \cdot 2^{-1} \pmod{3}$$

$$x \equiv 1 \cdot 2 \pmod{3}$$

$$\text{Como } 2 \cdot 2 \equiv 1 \pmod{3}; 2^{-1} = 2$$

$$\bullet 8x \equiv 7 \pmod{11}$$

$$x \equiv 7 \cdot 8^{-1} \pmod{11}$$

$$x \equiv 7 \cdot 7 \pmod{11}$$

$$x \equiv 5 \pmod{11}$$

$$\text{Como } 8 \cdot 7 \equiv 1 \pmod{11}; 8^{-1} = 7$$

$$\bullet 5x \equiv 3 \pmod{13}$$

$$x \equiv 3 \cdot 5^{-1} \pmod{13}$$

$$x \equiv 3 \cdot 8 \pmod{13}$$

$$x \equiv 11 \pmod{13}$$

$$\text{Como } 5 \cdot 8 \equiv 1 \pmod{13}; 5^{-1} = 8$$

Agrupando las congruencias obtenemos:

$$\begin{cases} x \equiv 2 \pmod{3} & \rightarrow x = 3k + 2 \\ x \equiv 5 \pmod{11} & \rightarrow x = 11m + 5 \\ x \equiv 11 \pmod{13} & \rightarrow x = 13n + 11 \end{cases}$$

Sustituyendo la 1ª con la 2ª

$$3k + 2 \equiv 5 \pmod{11}$$

$$3k \equiv 3 \pmod{11}$$

$$k \equiv 3 \cdot 3^{-1} \pmod{11}$$

$$\text{Como } 3 \cdot 4 \equiv 1 \pmod{11}, 3^{-1} = 4$$

$$k \equiv 3 \cdot 4 \pmod{11}$$

$$k \equiv 1 \pmod{11} \rightarrow k = 11m + 1; \text{ Sustituyendo en la 1ª}$$

$$x = 3 \cdot (11m + 1) + 2 \Rightarrow x = 33m + 3 + 2 \Rightarrow x = 33m + 5 \rightarrow x \equiv 5 \pmod{33}$$

→ Sustituimos dicho resultado en la tercera ecuación.

$$33m + 5 \equiv 11 \pmod{13}$$

$$7m \equiv 11 - 5 \pmod{13}$$

$$\text{Como } 7 \cdot 2 \equiv 1 \pmod{13}; 7^{-1} = 2$$

$$m \equiv 6 \cdot 7^{-1} \pmod{13}$$

$$m \equiv 6 \cdot 2 \pmod{13}$$

$$m \equiv 12 \pmod{13} \rightarrow m = 13z + 12 \rightarrow \text{Sustituimos}$$

$$x \equiv 33 \cdot (13z + 12) + 5 \Rightarrow x = 429z + 396 + 5 \Rightarrow x = 429z + 401 //$$

$$x \equiv 401 \pmod{429}$$

iv)
$$\begin{cases} 4x + 2 \equiv 3x - 1 \pmod{5} \\ 6x - 3 \equiv 2(x - 1) \pmod{7} \\ 2x \equiv 1 \pmod{3} \end{cases}$$

Procederemos de igual forma que las anteriores pero antes tenemos que simplificar y comprobar la coprimidad.

En este caso, $\gcd(5, 7, 3) = 1$ esto quiere decir que los módulos son coprimos por lo tanto podemos obtener solución. Vamos a simplificar

$$\bullet 4x + 2 \equiv 3x - 1 \pmod{5} \Rightarrow x \equiv -3 \pmod{5} \Rightarrow x \equiv 2 \pmod{5}$$

$$\bullet 6x - 3 \equiv 2(x - 1) \pmod{7} \Rightarrow 6x \equiv 3 + 2x - 2 \pmod{7} \Rightarrow 4x \equiv 1 \pmod{7}$$

$$x \equiv 1 \cdot 4^{-1} \pmod{7}$$

$$\text{Como } 4 \cdot 2 \equiv 1 \pmod{7}$$

$$x \equiv 2 \pmod{7}$$

$$4^{-1} = 2$$

$$\bullet 2x \equiv 1 \pmod{3} \Rightarrow x \equiv 1 \cdot 2^{-1} \pmod{3} \Rightarrow x \equiv 1 \cdot 2 \pmod{3} \Rightarrow x \equiv 2 \pmod{3}$$

Agrupando las congruencias obtenemos:

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 2 \pmod{3} \end{cases}$$

* Como las congruencias tienen la misma solución $x \equiv 2$, simplemente multiplicando los módulos, obtendremos la solución.

$$5 \cdot 7 \cdot 3 = 105 \Rightarrow x \equiv 2 \pmod{105} \Leftrightarrow x = 105k + 2 //$$