<u>Ejercicio</u>: He comprado entre 50 y 100 artículos a 17€. He vendido unos cuantos por 49 euros y he ganado 245€. ¿Cuántos me quedan por vender?

$x \equiv$ vendidos
$y \equiv$ comprados

El enunciado nos plantea la ecuación:

$$49x - 17y = 245$$

Por el lema de Bezout sabemos que existen x_0 e y_0 tales que

$$49x_0 - 17y_0 = mcd(49,17) = 1$$

Vamos a calcular $mcd(49,17)$ utilizando el algoritmo de Euclides:

$$49 = 17\cdot 2 + 15 \rightarrow 15 = 49 - 17\cdot 2$$
$$17 = 15\cdot 1 + 2 \rightarrow 2 = 17 - 15$$
$$15 = 2\cdot 7 + \boxed{1} \rightarrow 1 = 15 - 2\cdot 7$$
$$2 = 1\cdot 2 + 0$$

$$1 = 15 - 2\cdot 7 = 15 - (17-15)\cdot 7 = 15\cdot 8 - 17\cdot 7 =$$
$$= (49 - 17\cdot 2)\cdot 8 - 17\cdot 7 = 49\cdot 8 - 17\cdot 23$$

$x_0 = 8$, $y_0 = 23$ verifican

$$49\cdot \underset{x_0}{8} - 17\cdot \underset{y_0}{23} = 1$$

Entonces una solución a la ecuación

$$49x - 17y = 245$$

será

$$245(49x_0 - 17y_0) = (1)\cdot 245$$

$$49(245x_0) - 17(245y_0) = 245$$

Es decir

$$x = 245\cdot 8 = 1960 \quad , \quad y = 245\cdot 23 = 5635$$

No es solución del problema. Deberemos calcular la solución general:

$$\begin{aligned} & 49x - 17y = 245 \\ \overset{\pm \frac{49\cdot 17}{1}K}{\Longleftrightarrow} \quad & 49x - 17y + 49\cdot 17K - 49\cdot 17K = 245 \\ \Longleftrightarrow \quad & 49(x - 17K) - 17(y - 49K) = 245 \end{aligned}$$

Es decir, la solución general es:

$$x_K = 1960 - 17K \quad , \quad y_K = 5635 - 49K$$

$$\begin{array}{r|l} 5635 & 49 \\ \hline 0 & 115 \end{array}$$

Entonces: $K = 115: \; x_{115} = 5 \; , \; y_{115} = 0$

$K = 114: \; x_{114} = 22 \; , \; y_{114} = 49$

$K = 113: \; x_{113} = 39 \; , \; y_{113} = 98$ ✓ Hemos comprado entre 50 y 100.

Si hemos comprado 98 y hemos vendido 39, faltan por vender $98 - 39 = 59$.

Ejercicio: Un billete de avión vale 700, 550 ó 390 euros según se viaje en primera, negocio ó turista. Si un vuelo de 69 pasajeros ha recaudado 32.740€. ¿Cuántos billetes de cada clase volaron?

$$\begin{cases} x \equiv \text{primera} \\ y \equiv \text{negocio} \\ z \equiv \text{turista} \end{cases} \longrightarrow \begin{cases} x+y+z = 69 \\ 700x+550y+390z = 32740 \end{cases}$$

Vamos a reducir el sistema a una ecuación diofántica. Vamos a eliminar la variable z: Restando a la segunda fila la primera multiplicada por 390:

$$\begin{array}{rl} & 700x + 550y + 390z = 32740 \\ - & 390x - 390y - 390z = -69\cdot 390 = -26910 \\ \hline & 310x + 160y = 5830 \end{array}$$

Ahora podemos trabajar con la ecuación diofántica

$$310x+160y=5830 \iff 31x+16y=583$$

Vamos a resolver la ecuación mediante Euclides:

$$31 = 16\cdot 1 + 15 \rightarrow 15 = 31-16$$
$$16 = 15\cdot 1 + \boxed{1} \longrightarrow 1 = 16-15$$
$$15 = 1\cdot 15 + 0$$

$$1 = 16-15 = 16-(31-16) = 16\cdot 2 - 31.$$

Entonces $\quad 31\cdot(-1) + 16\cdot(2) = 1$

y por tanto, multiplicando por 583:

$$31(-583) + 16(583\cdot 2) = 583$$

Es decir, $31x + 16y = 583$ tiene como solución

$$x = -583 \quad , \quad y = 583\cdot 2 = 1166$$

Es solución de la ecuación pero no del problema.

Vamos a calcular la solución general:

$$x_k = -583 + 16k \quad , \quad y_k = 1166 - 31k$$

$583 \; \underline{|16}$
$\quad\quad 36'\ldots$

Entonces: $k = 37 : \; x_{37} = 9 \; , \; y_{37} = 19$

$k = 36 : \; x_{36} < 0$

$k = 38 : \quad\quad y_{38} < 0$

} no son válidas para nuestro problema

Y además, de $x + y + z = 69$, obtenemos que

$$z = 69 - 9 - 19 = 41$$

Por tanto se vendieron 9 billetes de primera, 19 de negocio y 41 de turista.

<u>Ejercicio</u>

¿Cuándo podemos afirmar que $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$

tiene solución? (Pensar que $\mathrm{mcd}(m_1, m_2) \neq 1$)

$$X \equiv b_1 \pmod{m_1} \iff X = b_1 + m_1 \cdot \alpha$$

Sustituyendo:

$$b_1 + m_1\alpha \equiv b_2 \pmod{m_2} \iff b_1 - b_2 \equiv m_1\alpha \pmod{m_2}$$

$$\iff b_1 - b_2 = m_1\alpha + m_2\beta \underset{\downarrow}{=} \mathrm{mcd}(m_1, m_2)\cdot(t\cdot\alpha + s\cdot\beta)$$

$$(m_1 = \mathrm{mcd}(m_1,m_2)\cdot t,\ m_2 = \mathrm{mcd}(m_1,m_2)\cdot s)$$

Es decir: $b_1 - b_2 = \mathrm{mcd}(m_1, m_2)\cdot(t\alpha + s\cdot\beta)$

Por tanto mcd (m_1, m_2) debe dividir a $b_1 - b_2$

<u>Ejercicio</u>: Calcular el primer nº de 5 cifras múltiplo de 13 y cuyas dos últimas cifras es 21.

Nos plantea el sistema de congruencias:

$$\begin{cases} X \equiv 0 \pmod{13} \\ X \equiv 21 \pmod{100} \end{cases}$$

Resolvemos:

$$X \equiv 21 \pmod{100} \iff \boxed{X = 21 + 100\alpha}$$

Sustituyendo en la primera:

$$\begin{array}{r|l} 100 & 13 \\ \hline 9 & 7 \end{array}$$

$$21 + 100\alpha \equiv 0 \pmod{13} \iff 8 + 9\alpha \equiv 0 \pmod{13}$$

$$\iff 9\alpha \equiv -8 \pmod{13}$$

$$\left(\begin{array}{l} \iff -4\alpha \equiv -8 \pmod{13} \\ \implies \boxed{\alpha = 2 + 13\beta} \end{array}\right)$$

$$\iff 9\alpha \equiv 5 \pmod{13}$$

Vamos a resolver $9\alpha \equiv 5 \pmod{13}$. Debemos calcular mcd $(9,13) \underset{\downarrow}{=} 1$ y comprobar que divide a 5.

(tiene una única solución)

Debemos aplicar Euclides:

$9\alpha \equiv 5 \pmod{13}$

Ec diofántica.

$9\alpha = 5 + 13K \iff 9\alpha - 13K = 5$

$$13 = 9\cdot 1 + 4 \rightarrow 4 = 13 - 9$$
$$9 = 4\cdot 2 + \boxed{1} \longrightarrow 1 = 9 - 4\cdot 2$$
$$4 = 1\cdot 4 + 0$$

$$1 = 9 - 4\cdot 2 = 9 - (13-9)\cdot 2 = 9\cdot 3 - 13\cdot 2$$

Entonces $9\cdot 3 - 13\cdot 2 = 1$ y multiplicando por 5

$$9\cdot(3\cdot 5) - 13(2\cdot 5) = 5$$
$$9\cdot \underbrace{15}_{\alpha} - 13\cdot \underbrace{10}_{K} = 5$$

Por tanto $\alpha = 15$ verifica: $9\cdot 15 \equiv 5 \pmod{13}$

Luego la solución es $[\alpha]_{13} = [15]_{13} = [2]_{13}$

$[\alpha]_{13} = [2]_{13} \iff \alpha = 2 + 13\cdot\beta$

Sustituyendo en $x = 21 + 100\alpha$:

$$x = 21 + 100(2 + 13\beta) = 21 + 200 + 1300\beta$$
$$= 221 + 1300\beta$$

La solución es: $[x]_{1300} = [221]_{1300}$

$= [10621]_{1300}$

$10.000 \,\lfloor 1300$
$7, \ldots$

El primer número de cinco cifras múltiplo de 13 cuyas dos últimas cifras es 21 es 10621.

Ejercicio. Hallar, sin usar la calculadora, el resto de dividir 27! entre 29.

Por el th de Wilson: $(p-1)!+1 \equiv 0 \pmod{p}$

Entonces si $p=29$:

$$28!+1 \equiv 0 \pmod{29}$$

$$\iff 28! \equiv -1 \pmod{29}$$

$$\iff 28! \equiv 28 \pmod{29}$$

$$\iff 28 \cdot 27! \equiv 28 \pmod{29}$$

Como $\mathbb{Z}_{29}$ es cuerpo 28 es inversible $\iff 28^{-1} \cdot 28 \cdot 27! \equiv 28^{-1} \cdot 28 \pmod{29}$

(como mcd$(28,29)=1$ $\Rightarrow$ 28 es inversible) $\iff 27! \equiv 1 \pmod{29}$

El resto de dividir $27!$ entre 29 da de resto 1.

<u>Ejercicio</u>

Resolver
$$\begin{cases} x \equiv 2 \pmod{6} \\ 7x \equiv 2 \pmod{8} \\ 3x \equiv 0 \pmod{10} \end{cases}$$

Primero vamos a despejar las x's:

- $7x \equiv 2 \pmod{8} \iff -x \equiv 2 \pmod{8} \iff x \equiv -2 \pmod{8}$
  $x \equiv 6 \pmod{8}$

(El inverso de 7 en $\mathbb{Z}_8$)

Debemos calcular "a" tal que $7 \cdot a \equiv 1 \pmod{8} \rightsquigarrow [a]_8 = [-1]_8 = [7]_8$

Para después multiplicar "a" en $7x \equiv 2 \pmod{8} \rightsquigarrow -7x \equiv -2 \pmod{8}$
$\iff x \equiv 6 \pmod{8}$

- $3x \equiv 0 \pmod{10}$ no nos preocupa quién es el inverso. Sólo que tenga inverso. En este caso 3 es inversible módulo 10 ya que mcd$(3,10)=1$. Luego existe 3^{-1}.

Multiplicando por 3^{-1}:

$$3^{-1}\cdot 3x \equiv 3^{-1}\cdot 0 \pmod{10} \iff x \equiv 0 \pmod{10}$$

$$\begin{cases} x \equiv 2 & (\text{mód } 6) \\ 7x \equiv 2 & (\text{mód } 8) \\ 3x \equiv 0 & (\text{mód } 10) \end{cases} \iff \begin{cases} x \equiv 2 & (\text{mód } 6) \\ x \equiv 6 & (\text{mód } 8) \\ x \equiv 0 & (\text{mód } 10) \end{cases}$$

Tiene solución (aplicando el criterio mencionado en un ejercicio anterior)

- $x \equiv 2 \ (\text{mód } 6) \iff \boxed{x = 2 + 6\alpha}$

Sustituyendo en la segunda:

$$2 + 6\alpha \equiv 6 \ (\text{mód } 8) \iff 6\alpha \equiv 4 \ (\text{mód } 8)$$

Como mcd $(6,8) = 2$, consideramos la congruencia auxiliar:

$$\begin{aligned} 3\alpha \equiv 2 \ (\text{mód } 4) &\iff -\alpha \equiv 2 \ (\text{mód } 4) \\ &\iff \alpha \equiv -2 \ (\text{mód } 4) \\ &\Rightarrow \alpha \equiv 2 \ (\text{mód } 4) \\ &\Rightarrow \alpha = 2 + 4\cdot\beta \end{aligned}$$

Entonces $x = 2 + 6\alpha = 2 + 6(2 + 4\beta) = 2 + 12 + 24\beta = 14 + 24\beta$

$$[x]_{24} = [14]_{24} \iff x \equiv 14 \ (\text{mód } 24)$$

Teniendo ahora que:

$$\begin{cases} x \equiv 2 & (\text{mód } 6) \\ x \equiv 6 & (\text{mód } 8) \\ x \equiv 0 & (\text{mód } 10) \end{cases} \iff \begin{cases} x \equiv 14 & (\text{mód } 24) \\ x \equiv 0 & (\text{mód } 10) \end{cases}$$

De nuevo: $x \equiv 14 \pmod{24} \iff \boxed{x = 14 + 24\alpha}$

Sustituyendo:

$$14 + 24\alpha \equiv 0 \pmod{10} \iff 4 + 4\alpha \equiv 0 \pmod{10}$$
$$\iff 4\alpha \equiv -4 \pmod{10}$$

Entonces como $\text{mcd}(4,10) = 2$, debemos considerar la congruencia auxiliar:

$$2\alpha \equiv -2 \pmod 5$$
$$\iff \alpha \equiv -1 \pmod 5$$
$$\Rightarrow \alpha = -1 + 5\beta$$

Entonces: $x = 14 + 24\alpha = 14 + 24(-1 + 5\beta) = 14 - 24 + 120\beta$
$= -10 + 120\beta$

Luego $[x]_{120} = [-10]_{120} = [110]_{120}$.

es la solución al sistema es $x \equiv 110 \pmod{120}$