RelacionEjerciciosTema1.pdf

CV_03

Matemática Discreta

1º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

Números Enteros

$\mathbb{Z} = \{-2,-1,0,1,2\}$

$\mathbb{N} = \{0,1,2\}$

$\mathbb{N}^* = \{1,2,3\}$ ó $\mathbb{N} - \{0\}$

División Euclídea en $\mathbb{Z}$

$n \,\underline{|\, m}$, resto R, cociente q $\longrightarrow n = mq + R$

$0 \leq R < |m|$

Sistemas de Numeración

$(341)_{10}$ a base 2

341 | 2 → 170 resto 1; 170 | 2 → 85 resto 0; 85 | 2 → 42 resto 1; 42 | 2 → 21 resto 0; 21 | 2 → 10 resto 1; 10 | 2 → 5 resto 0; 5 | 2 → 2 resto 1; 2 | 2 → 1 resto 0

$(341)_{10} = (101010101)_2 = 1\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4 + 0\cdot 2^5$
$+ 1\cdot 2^6 + 0\cdot 2^7 + 1\cdot 2^8 = 256 + 64 + 16 + 4 + 1 = (341)_{10}$

Relación de ejercicios 1

① Determina los enteros q, R, tales que $0 \leq R < |b|$ y $a = b\cdot q + R$, sabiendo que:

a) $a = 23, b = -7$

$23 \,\underline{|\, -7}$, resto 2, cociente -3 $\longrightarrow 23 = -7\cdot(-3) + 2$

b) $a=-335, b=24$

$$\begin{array}{r|l} +335 & 24 \\ \hline 95 & +13 \\ +23 & \end{array} \longrightarrow -335=-24\cdot 13-23$$

$$\longrightarrow -335=+24(-13)-23$$
$$=24(-13)-23+24-24$$
$$=24(-13)+1-24$$
$$=24(-13-1)+1$$
$$-335=24(-14)+1$$

c) $a=-107, b=-23$

$$\begin{array}{r|l} -107 & -23 \\ \hline 15 & 4 \end{array} \longrightarrow -107=-23\cdot 4+15$$

② Exprese en base decimal los siguientes números:

a) $10011101_2 = 1\cdot 2^0 + 1\cdot 2^2 + 1\cdot 2^3 + 1\cdot 2^4 + 1\cdot 2^7 = 157_{10}$

b) $1231_7 = 1\cdot 7^0 + 3\cdot 7^1 + 2\cdot 7^2 + 1\cdot 7^3 = 463_{10}$

③ Exprese en base 2, 8, 11 los siguientes números en base decimal:

a) $237_{10} \longrightarrow$

$$\begin{array}{r|l} 237 & 2 \\ \hline 1 & 118 \end{array}\quad \begin{array}{r|l} 118 & 2 \\ \hline 0 & 59 \end{array}\quad \begin{array}{r|l} 59 & 2 \\ \hline 1 & 29 \end{array}\quad \begin{array}{r|l} 29 & 2 \\ \hline 1 & 14 \end{array}\quad \begin{array}{r|l} 14 & 2 \\ \hline 0 & 7 \end{array}\quad \begin{array}{r|l} 7 & 2 \\ \hline 1 & 3 \end{array}\quad \begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array}$$

$237_{10} = 11101101_2$

$$237_{10} \longrightarrow \begin{array}{r|l} 237 & 8 \\ \hline 5 & 29 \end{array}\quad \begin{array}{r|l} 29 & 8 \\ \hline 5 & 3 \end{array} = 355_8$$

$$237_{10} \longrightarrow \begin{array}{r|l} 237 & 11 \\ \hline 6 & 21 \end{array}\quad \begin{array}{r|l} 21 & 11 \\ \hline 10 & 1 \end{array} = 1A6_{11}$$

$10 = A$

) Halla el valor de $x \in \mathbb{N}, y \in \mathbb{N}$ para que se verifiquen estas igualdades:

a) $331_x = 106_{11} = 127_{10}$

$106_{11} = 6 \cdot 11^0 + 0 \cdot 11^1 + 1 \cdot 11^2 = 127_{10}$

$1 \cdot x^0 + 3 \cdot x^1 + 3x^2 = 127$

$3x^2 + 3x - 126 = 0$

$x = \dfrac{-3 \pm \sqrt{9 - 4(3)(-126)}}{6} \rightarrow x = 6$, $\rightarrow \cancel{x = -7}$

b) $274_8 = y_2$

$274_8 = 4 \cdot 8^0 + 7 \cdot 8^1 + 2 \cdot 8^2 = 188_{10}$

188 | 2
0 94 | 2
0 47 | 2
1 23 | 2
1 11 | 2
1 5 | 2
1 2 | 2
0 1

$188_{10} = 10111100_2 \longrightarrow y = 10111100_2$

Divisibilidad

Si quiero decir que 3 es divisor de 8, lo expresamos como $3|8$, pero $3 \nmid 8$

Se dice que $a|b$ si $b = aq$, en el que q es un entero que es el cociente de la división

El 1 y el -1 son números enteros divisores de cualquier número entero $\longrightarrow 1|n, -1|n$

Lo mismo ocurre con el mismo número y el opuesto de él $\rightarrow n|n, -n|n$

⑤ Da un ejemplo para cada una de las propiedades alg. de la divisibilidad. Demuéstralas:

① Propiedad Reflexiva $\longrightarrow n|n \ \forall n \in \mathbb{Z}$

$3|3 \longrightarrow 3:3=1$

$n|n$ si $n = nq \longrightarrow q=1$

② Propiedad transitiva $\longrightarrow$ si $n|m$, y $m|k$, entonces $n|k$ $\forall n,m,k \in \mathbb{Z}$

$2|12$, $12|24$, entonces $2|24$

$n=2, m=12, k=24$

$\underbrace{n|m, m|k}_{\text{hipótesis}}$

Como $n|m$, $\exists q \in \mathbb{Z}$ tq $m=nq$

Como $m|k$, $\exists q' \in \mathbb{Z}$ tq $k=mq'$

$k=nqq'$

¿$\underbrace{n|k?}_{\text{tesis}}$ ¿Existe un $q'' \in \mathbb{Z}$ tal que $k=nq''$?

$\cancel{n}q'' = \cancel{n}qq' \longrightarrow q''=q'q$

$q, q' \in \mathbb{Z}$, tq $q \cdot q' \in \mathbb{Z}$, tq $q'' \in \mathbb{Z}$

③ Propiedad antisimétrica $\longrightarrow$ si $n \geq 0$, $m \geq 0$, $n|m$, $m|n$, entonces $m=n$

Hipótesis $\longrightarrow n|m, m|n$

Como $n|m$, $\exists q \in \mathbb{N}$ tq $m=nq$

Como $m|n$, $\exists q' \in \mathbb{N}$ tq $n=mq'$

$\cancel{n} = \cancel{n}qq' \longrightarrow qq'=1$, como $q, q' \in \mathbb{N}$, $qq'=1$ si $q=q'$, por lo que

$n=m$

④ $1|n$ y $(-1)|n \ \forall n \in \mathbb{Z}$

$n=1q \longrightarrow n=q$

$n=-1q \longrightarrow n=-q$

Ejemplo: $1|8, -1|8$

$n | -n, -n | n \ \forall n \in \mathbb{Z}$

$n = nq, q = -1$

$n = -nq, q = -1$

⑥ Si $\underbrace{k|n \text{ y } k|m}_{\text{hipótesis}}$, entonces $\underbrace{k|(n+m) \text{ y } k(n-m)}_{\text{tesis}}$

Como $k|n$, $\exists q \in \mathbb{Z}$ tq $n = kq$

Como $k|m$, $\exists q' \in \mathbb{Z}$ tq $m = kq'$

$n-m = kq - kq'$ o $n+m = kq + kq'$

¿$k|(n+m)$? ¿$\exists q_3 \in \mathbb{Z}$ tq $n+m = kq_3$?

$n+m = kq+kq'$

$n+m = k(q+q')$

$q+q' = q_3$, $q, q' \in \mathbb{Z}$, por lo que $q+q' \in \mathbb{Z}$

¿$k|(n-m)$? ¿$\exists q_4 \in \mathbb{Z}$ tq $n-m = kq_4$?

$n-m = kq - kq'$

$n-m = k(q-q')$

$q-q' = q_4 \in \mathbb{Z}$

⑦ Si $\underbrace{n|m}_{\text{hipótesis}}$, entonces $\underbrace{n|(km)}_{\text{tesis}}$ $\forall k \in \mathbb{Z}$

Como $n|m$, $\exists q \in \mathbb{Z}$ tq $m = nq$

¿$n|(km)$? ¿$\exists q' \in \mathbb{Z}$ tq $km = nq'$?

$k\cancel{n}q = \cancel{n}q'$

$kq = q'$, $k, q \in \mathbb{Z}$, por lo que $k \cdot q \in \mathbb{Z}$ y $q' \in \mathbb{Z}$

⑧ Si $\underbrace{k|n \text{ y } k|m}_{\text{hipótesis}}$, entonces $\underbrace{k|(sn+tm)}_{\text{tesis}}$ $\forall s,t \in \mathbb{Z}$

Como $k|n$, $\exists q \in \mathbb{Z}$ tq $n = kq \longrightarrow sn = kqs$

Como $k|m$, $\exists q' \in \mathbb{Z}$ tq $m = kq' \longrightarrow tm = kq't$

$sn + tm = k(qs + q't)$

¿$k|(sn+tm)$? ¿$\exists q_3 \in \mathbb{Z}$ tq $sn+tm = kq_3$

$sn+tm = k(qs+q't)$

$q_3 = qs + q't$, $q, s, q', t \in \mathbb{Z}$, por lo que $q_3 \in \mathbb{Z}$

(7) Da ejemplos de enteros a, b tales que:

a) a es divisor de bc, pero a no es divisor de b ni de c

Si $\underbrace{a|b, a|c}_{\text{hipótesis}}$, ¿existe un $q_3 \in \mathbb{Z}$ tq $\underbrace{bc = aq_3}_{\text{tesis}}$ ya que $\underbrace{a|bc}_{\text{tesis}}$?

Como $a|b, \exists q \in \mathbb{Z}$ tq $b = aq \longrightarrow bc = caq$

Como $a|c, \exists q' \in \mathbb{Z}$ tq $c = aq' \longrightarrow bc = baq'$

$\cancel{a}q_3 = c\cancel{a}q \longrightarrow q_3 = cq$

$\cancel{a}q_3 = b\cancel{a}q' \longrightarrow q_3 = bq'$

(6) Usa las propiedades algebraicas para demostrar que n y n+1, son coprimos entre sí $\forall n \in \mathbb{N}$:

$mcd(n, n+1) = 1$

$an + b(n+1) = 1$

$a = -1, b = 1 \longrightarrow -n + n + 1 = 1 \longrightarrow 1 = 1$

Como $d = 1$ (el único divisor común), los números son coprimos entre sí $\forall n \in \mathbb{N}$

(7) Da ejemplos de enteros a, b, c tales que:

a) a es divisor de bc, pero a no es divisor de b ni de c:

$\underline{a|bc}$, $\underline{a\nmid b}$, $\underline{a\nmid c}$

$a = 27$
$b = 9$
$c = 18$

$\left\{ 27|9\cdot 18, \ 27\nmid 9, \ 27\nmid 18 \right.$

) a y b son divisores de c, pero ab no es divisor de c

$a|c$, $b|c$, $ab\nmid c$

$$\left.\begin{array}{l} c=14 \\ a=7 \\ b=3 \end{array}\right\} 7|14,\ 3|14,\ 21\nmid 14$$

(8) Sean a, b, c, d enteros cualquiera. Demuestra o refuta el siguiente enunciado → Si a, b y c dividen a d, entonces a+c divide a b+d:

hipótesis — tesis — hipótesis

$a|d$
$b|d$
$c|d$
¿$a+c|b+d$?

Para refutar la afirmación uso el siguiente contraejemplo:

$a=2$	$2\|28$
$b=4$	$4\|28$
$c=7$	$7\|28$
$d=28$	$2+7\nmid 28+4$

(9) Demuestra que $2020^4+2020^3-2020-1$ no es un número primo:

$x=2020$

$x^4+x^3-x-1=(x-1)(x^3+2x^2+2x+1)$

$=(2020-1)\cdot(2020^3+2\cdot 2020^2+2\cdot 2020+1)$

Como el número original ahora, está expresado como el producto de 2 números, por definición, no puede ser primo

Congruencias lineales

$12x \equiv 14 \bmod 34$

$mcd(12,34)=2$, tiene 2 soluciones en $\mathbb{Z}_{34}$

$34 \mid 12x-14$

$12x = 34k+14$

$6x = 17k+7$

$6x \equiv 7 \bmod 17$

$mcd(6,17)=1$

$[6]_{17}[x]_{17}=[7]_{17}$

$[18]_{17}[x]_{17}=[21]_{17}$

$[x]_{17}=[21]_{17} \longrightarrow x \equiv 21 \bmod 17$

Relación de ejercicios 2

① Expresa el $mcd(a,b)$ como combinación lineal de a,b:

a) $a=16, b=135 \longrightarrow mcd(16,135)=1$

$$135 \underline{|16} \quad 7 \;\; 8 \qquad 16 \underline{|7} \quad 2 \;\; 2 \qquad 7 \underline{|2} \quad 1 \;\; 3$$

$16x+135y=3 \; \forall x,y \in \mathbb{Z} \longrightarrow 16(-59)+135(7)=1$

$$\begin{pmatrix}135\\1\\0\end{pmatrix}-8\begin{pmatrix}16\\0\\1\end{pmatrix}=\begin{pmatrix}7\\1\\-8\end{pmatrix}$$

$$\begin{pmatrix}16\\0\\1\end{pmatrix}-2\begin{pmatrix}7\\1\\-8\end{pmatrix}=\begin{pmatrix}2\\-2\\17\end{pmatrix}$$

$$\begin{pmatrix}7\\1\\-8\end{pmatrix}-3\begin{pmatrix}2\\-2\\17\end{pmatrix}=\begin{pmatrix}1\\7\\-59\end{pmatrix}$$

b/E

b) $a=55, b=34 \longrightarrow mcd(55,34)=1$

$55 \underline{|34}$, resto 21, cociente 1; $34 \underline{|21}$, resto 13, cociente 1; $21 \underline{|13}$, resto 8, cociente 1; $13 \underline{|8}$, resto 5, cociente 1; $8 \underline{|5}$, resto 3, cociente 1; $5 \underline{|3}$, resto 2, cociente 1

$55x+34y=1 \longrightarrow 55(13)+34(-21)=1$

$\begin{pmatrix}55\\1\\0\end{pmatrix}-\begin{pmatrix}34\\0\\1\end{pmatrix}=\begin{pmatrix}21\\1\\-1\end{pmatrix} \longrightarrow \begin{pmatrix}34\\0\\1\end{pmatrix}-\begin{pmatrix}21\\1\\-1\end{pmatrix}=\begin{pmatrix}13\\-1\\2\end{pmatrix}$

$\longrightarrow \begin{pmatrix}21\\1\\-1\end{pmatrix}-\begin{pmatrix}13\\-1\\2\end{pmatrix}=\begin{pmatrix}8\\2\\-3\end{pmatrix} \longrightarrow \begin{pmatrix}13\\-1\\2\end{pmatrix}-\begin{pmatrix}8\\2\\-3\end{pmatrix}=\begin{pmatrix}5\\-3\\5\end{pmatrix}$

$\longrightarrow \begin{pmatrix}8\\2\\-3\end{pmatrix}-\begin{pmatrix}5\\-3\\5\end{pmatrix}=\begin{pmatrix}3\\5\\-8\end{pmatrix} \longrightarrow \begin{pmatrix}5\\-3\\5\end{pmatrix}-\begin{pmatrix}3\\5\\-8\end{pmatrix}=\begin{pmatrix}2\\-8\\13\end{pmatrix}$

$\longrightarrow \begin{pmatrix}3\\5\\-8\end{pmatrix}-\begin{pmatrix}2\\-8\\13\end{pmatrix}=\begin{pmatrix}1\\13\\-21\end{pmatrix}$

c) $a=107, b=23 \longrightarrow mcd(107,23)=1$

$107 \underline{|23}$, resto 15, cociente 4; $23 \underline{|15}$, resto 8, cociente 1; $15 \underline{|8}$, resto 7, cociente 1; $8 \underline{|7}$, resto 1, cociente 1

$107x+23y=1 \longrightarrow 107(-3)+23(14)=1$

$\begin{pmatrix}107\\1\\0\end{pmatrix}-4\begin{pmatrix}23\\0\\1\end{pmatrix}=\begin{pmatrix}15\\1\\-4\end{pmatrix} \longrightarrow \begin{pmatrix}23\\0\\1\end{pmatrix}-\begin{pmatrix}15\\1\\-4\end{pmatrix}=\begin{pmatrix}8\\-1\\5\end{pmatrix}$

$\longrightarrow \begin{pmatrix}15\\1\\-4\end{pmatrix}-\begin{pmatrix}8\\-1\\5\end{pmatrix}=\begin{pmatrix}7\\2\\-9\end{pmatrix} \longrightarrow \begin{pmatrix}8\\-1\\5\end{pmatrix}-\begin{pmatrix}7\\2\\-9\end{pmatrix}=\begin{pmatrix}1\\-3\\14\end{pmatrix}$

2 Considere las ecuaciones diofánticas:

1 $312x+42y=834$, 2 $144x+702y=9$

a) Indique si tienen solución:

Una ecuación diofántica tiene solución entera solo si $mcd(x,y)|c$

1 $312x+42y=834$

$mcd(312,42)=6 \longrightarrow 6|834$, por lo que tiene solución

2 $144x+702y=9$

$mcd(144,702)=18 \longrightarrow 18\nmid 9$, por lo que no tiene soluciones

b) Encuentre la solución general de la ecuación o ecuaciones con solución:

① $312x + 42y = 834$

$mcd(312, 42) = 6$

$312x + 42y = 6 \longrightarrow 312(-2) + 42(15) = 6$

$$\begin{pmatrix} 312 \\ 1 \\ 0 \end{pmatrix} - 7\begin{pmatrix} 42 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 18 \\ 1 \\ -7 \end{pmatrix} \longrightarrow \begin{pmatrix} 42 \\ 0 \\ 1 \end{pmatrix} - 2\begin{pmatrix} 18 \\ 1 \\ -7 \end{pmatrix} = \begin{pmatrix} 6 \\ -2 \\ 15 \end{pmatrix}$$

$(312x + 42y) \cdot 139 = 6 \cdot 139$

$312 \cdot 139x + 42 \cdot 139y = 834$

$312\underbrace{(-2 \cdot 139)}_{x_0} + 42 \cdot \underbrace{(139 \cdot 15)}_{y_0} = 834$

$-(312x + 42y = 834)$

$312(-2 \cdot 139) - 312x + 42(139 \cdot 15) - 42y = 0$

$\frac{312}{6}(-2 \cdot 139 - x) + \frac{42}{6}(139 \cdot 15 - y) = \frac{0}{6}$

$52(-278 - x) + 7(139 \cdot 15 - y) = 0$

$52(278 + x) = 7(139 \cdot 15 - y)$

$52 \cdot \frac{278 + x}{7} = -y + (139 \cdot 15)$ $\left\{ \frac{278 + x}{7} = k, \forall k \in \mathbb{Z} \right.$

$52k = -y + (139 \cdot 15)$

$$\boxed{\begin{aligned} y &= (139 \cdot 15) - 52k \\ x &= 7k - 278 \end{aligned}}$$

c) Encuentra las soluciones positivas de la ecuación:

$139 \cdot 15 - 52k \geq 0 \longrightarrow 15 \cdot 139 \geq 52k \longrightarrow k \leq \frac{15 \cdot 139}{52}$

$7k - 278 \geq 0 \longrightarrow 7k \geq 278 \longrightarrow k \geq \frac{278}{7}$

$k \leq \frac{15 \cdot 139}{52}$, $k \geq \frac{278}{7}$, por lo que $k = 40$

③ Para tender un tramo de vía de 122 m, se dispone de barras de 30 m y 16 m. ¿Es posible cubrir el tramo usando solo estas barras?

④ Dete...

$30x + 16y = 122$

$mcd(30,16) = 2$

$30x + 16y = 2$

$\begin{pmatrix} 30 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 16 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 14 \\ 1 \\ -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 16 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 14 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix}$

$30(-1) + 16(2) = 2$

$30(-61) + 16(2 \cdot 61) = 122$

$-30x \quad - 16y = -122$

$\frac{30}{2}(-x-61) + \frac{16}{2}(122-y) = 0$

$-15(x+61) + 8(122-y) = 0$

$15(x+61) = 8(122-y) \longrightarrow \frac{x+61}{8} = k \longrightarrow x = 8k - 61$

$x + 61 = 8 \cdot \frac{122-y}{15} \longrightarrow \frac{122-y}{15} = k \longrightarrow y = -15k + 122$

⊙ De ser posible, indique el número de barras de cada tipo que habría que usar:

$8k - 61 \geq 0 \longrightarrow k \geq \frac{61}{8}$

$-15k + 122 \geq 0 \longrightarrow k \leq \frac{122}{15}$

$7'6 < k < 8'13, \; k = 8$

$x_0 = 3$ barras de 30 m

$y_0 = 2$ barras de 16 m

④ Determina los valores $c \in \mathbb{Z}, 10 < c < 20$, para los cuales, no tiene solución entera la ecuación $84x + 990y = c$. ~~Resuelve los que tengan solución.~~

$\boxed{84x + 990y = c}$ es resolvible si $mcd(84, 990) \mid c$

$mcd(84, 990) = 6$

$990 = 84 \cdot 11 + 66 \qquad 84 = 66 \cdot 1 + 18 \qquad 66 = 18 \cdot 3 + 12 \qquad 18 = 12 \cdot 1 + 6 \qquad 12 = 6 \cdot 2 + 0$

La ecuación tiene solución $\forall c \in \mathbb{Z}, 10 < c < 20, 6 \mid c$, es decir, para $c = 18, c = 12$

⑤ Resuelve la ecuación diofántica $4x + 6y + 7z = 12$ con $u = 2x + 3y$:

$2(2x + 3y) + 7z = 12$

$2u + 7z = 12$

$mcd(2, 7) = 1$

$2u + 7z = 1 \longrightarrow 2(-3) + 7(1) = 1$

$\begin{pmatrix} 7 \\ 0 \end{pmatrix} - 3 \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -3 \end{pmatrix}$

$2(-3 \cdot 12) + 7(1 \cdot 12) = 12$

$2u + 7z = 12$

$-2(-36) + 7(12) = 12$

$2u - 2(-36) + 7z - 7(12) = 0$

$2(u + 36) + 7(z - 12) = 0$

$2(u + 36) = 7(-z + 12)$

$\begin{cases} \frac{u+36}{7} = k \longrightarrow u = 7k - 36 \\ \frac{-z+12}{2} = k \longrightarrow z = 12 - 2k \end{cases}$

Obtenemos una nueva ecuación diofántica de 2 valores, en función

$u = -36 + 7k$

$2x + 3y = -36 + 7k$

$mcd(2, 3) = 1$

$2x + 3y = 1$

$2 \cdot (-1) + 3 \cdot (+1) = 1$

$+2(7k - 36) + 3(36 - 7k) = +36 - 7k$

$2x + 3y = -36 + 7k$

$2(7k - 36 + x) + 3(36 - 7k + y) = 0$

$2(7k - 36 + x) = 3(-y + 7k - 36)$

$\begin{cases} \frac{7k - 36 + x}{3} = \alpha \longrightarrow x = 3\alpha - 7k + 36 \\ \frac{-y + 7k - 36}{2} = \alpha \longrightarrow y = -2\alpha + 7k - 36 \end{cases}$

Solución: $(x, y, z) = (3\alpha - 7k + 36, -2\alpha + 7k - 36, -2k + 12) \; \forall \alpha, k \in \mathbb{Z}$

⑥ Utiliza la identidad de Bezout para demostrar que, si $d = mcd(a,b)$, entonces $\underbrace{mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1}_{\text{tesis}}$

$\underbrace{mcd(a,b) = d}_{\text{hipótesis}} \longrightarrow ax + by = d$

$\underbrace{mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1}_{\text{tesis}} \longleftrightarrow \left(\frac{a}{d}\right)x' + \left(\frac{b}{d}\right)y' = 1$

$$\left.\begin{array}{l} \frac{ax}{d} + \frac{by}{d} = \frac{d}{d} \\ \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1 \end{array}\right\} \begin{array}{l} x = x' \\ y = y' \end{array}$$

⑦ Sean a, b enteros coprimos y sea $k \in \mathbb{Z}$. Usa la identidad de Bezout para deducir:

a) Si $\underbrace{b \text{ es divisor de } ak}_{\text{hipótesis}}$, entonces $\underbrace{b \text{ es divisor de } k}_{\text{tesis}}$:

$mcd(a,b) = 1$ $\qquad\qquad k = b(?)$

$ar + bs = 1 \longrightarrow ark + bsk = k$ $\qquad k = b(qr + sk)$ ✓

$b|ak \longrightarrow ak = bq$

$ark + bsk = k$

$bqr + bsk = k$

$k = b(qr + sk)$

b) Si a y b son divisores de k, entonces $a \cdot b$ también es divisor de k:

$ar + bs = 1 \longrightarrow ark + bsk = k$ $\qquad k = ab(?)$

$k = bt$ $\qquad k = ab(rt + sk)$

$k = ax$

$arbt + bsax = k$

$k = ab(rt + sx)$

1) Resolver si es posible, las siguientes congruencias lineales:

a) $3x \equiv 1 \pmod{12}$

No es posible pues $mcd(3,12) = 3 \nmid 1$

c) $64x + 11 = 43 \pmod{84}$

$64x = 32 \pmod{84} \longleftrightarrow 16x = 8 \pmod{21}$

$mcd(64,84) = 4 \mid 32$

$64x + 84y = 4 \longrightarrow 64(4) + 84(-3) = 4$

$\begin{pmatrix} 84 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 64 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 20 \\ 1 \\ -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 64 \\ 0 \\ 1 \end{pmatrix} - 3\begin{pmatrix} 20 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ 4 \end{pmatrix}$

$\longrightarrow \begin{pmatrix} 20 \\ 1 \\ -1 \end{pmatrix} - 5\begin{pmatrix} 4 \\ -3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 16 \\ -21 \end{pmatrix}$

$64x + 84y = 32$

$64(-32) + 84(24) = -32$

$64x + 64(-32) + 84y + 84(24) = 0$

$\frac{64}{4}(x-32) + \frac{84}{4}(y+24) = 0$

$16(x-32) + 21(y+24) = 0$

$16(x-32) = 21(-y-24)$

$\begin{cases} x - 32 = 21 \cdot q \longrightarrow x = 21q + 32 \\ -y - 24 = 16q \longrightarrow y = -16q - 24 \end{cases}$

$\boxed{\begin{array}{l} x_1 = 32 \\ x_2 = 21 + 32 = 53 \\ x_3 = 74 \\ x_4 = 95 \end{array}}$ El número de soluciones me lo da el $mcd(64,84) = 4$

② Encuentra el conjunto de enteros x que verifican el siguiente sistema de congruencias:

$x \equiv -2 \bmod (5) \longrightarrow \cancel{x \equiv 3 (\text{mód } 5)}$

$2x \equiv 1 (\text{mód } 7)$

$x \equiv 3 (\text{mód } 8)$

Los 3 módulos son coprimos 2 a 2, por lo que hay solución

$x \equiv -2 (\text{mód } 5) \longrightarrow x = 5k - 2$

$2(5k-2) = 1 (\text{mód } 7)$

$10k - 4 = 1 (\text{mód } 7)$

$10k = 5 (\text{mód } 7)$

$3k = 5 (\text{mód } 7)$

$\text{mcd}(3,7) = 1 \mid 5$

$3k + 7y = 1 \longrightarrow 3(-2) + 7(1) = 1$

$\begin{pmatrix} 7 \\ 0 \end{pmatrix} - 2\begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$

$3k + 7y = 5$

$3(5 \cdot 2) + 7(-5) = -5$

$3k + 3(10) + 7y + 7(-5) = 0$

$3(k+10) + 7(-5+y) = 0$

$3(k+10) = 7(5-y)$

$k = 7q - 10$

$\boxed{x = 5(7q-10) - 2 = 35Q - 52}$

$35Q - 52 = 3 (\text{mód } 8)$

$35Q = +55 (\text{mód } 8)$

$7Q = 11 (\text{mód } 8)$

$-Q = 3 (\text{mód } 8)$

$Q = -3 (\text{mód } 8) \longrightarrow Q = 8h - 3$

$x = 35(8h-3) - 52$

$x = 35 \cdot 8h - 157 \longrightarrow x = 280h - 157$

$x = -157 (\text{mód } 280)$

$x = 123 (\text{mód } 280)$

③ Resuelve cuando sean posibles los sistemas:

a) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 3 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases}$

$\text{mcd}(10,6) = 2 \longrightarrow 2 \mid 5-3$ ✓

$\text{mcd}(10,15) = 5 \longrightarrow 5 \mid 8-3$ ✓

$\text{mcd}(6,15) = 3 \longrightarrow 3 \mid 8-5$ ✓

Como los módulos de los sistemas no son coprimos 2 a 2, para comprobar si hay solución hay que hacer caso a la regla: el mcd de cada pareja de módulos, debe dividir a la diferencia de sus respectivos coeficientes.

Por lo que este sistema, sí que tiene solución:

$x \equiv 5 \pmod 6$

$x = 6q + 5$

$6q + 5 = 3 \pmod{10}$

$6q = -2 \pmod{10}$

$3q = -1 \pmod 5$

$2 \cdot (3q) = -1(2) \pmod 5$

$q = -2 \pmod 5$

$q = 5k - 2$

$x = 6(5k-2) + 5$

$x = 30k - 7$

$30k - 7 = 8 \pmod{15}$

$30k = 15 \pmod{15}$

$0k = 0 \pmod{15}$

Como nos da una solución trivial, todos los valores de k son válidos

$x = 30k - 7$

$x = -7 \pmod{30}$

$x = 23 \pmod{30}$

b) $\begin{cases} x \equiv 2 \pmod{14} \\ x \equiv 10 \pmod{30} \\ x \equiv 6 \pmod{21} \end{cases}$

$\text{mcd}(14,30) = 2 \mid 10-2$ ✓

$\text{mcd}(14,21) = 7 \nmid 6-2$ ✗

$\text{mcd}(30,21) = 3 \nmid 10-6$ ✗

Por lo que este sistema de congruencias no tiene ninguna solución

④ Encuentra el menor entero positivo cuyo resto cuando se divide por 11 es 8, que tiene el último dígito igual a 4 y es divisible por 27:

$x = 11q+8 \longrightarrow x \equiv 8 (\text{mód } 11)$

$x = 10k+4 \longrightarrow x \equiv 4 (\text{mód } 10)$

$x = 27m+0 \longrightarrow x \equiv 0 (\text{mód } 27)$

los 3 módulos son coprimos 2 a 2, por lo que el sistema tiene solución

---

$x = 27m \longrightarrow x = 270t+54$

$27m \equiv 4 (\text{mód } 10)$

$3(27)m \equiv 12 (\text{mód } 10)$

$71m \equiv 2 (\text{mód } 10)$

$m \equiv 2 (\text{mód } 10)$

$m = 10t+2$

$270t+54 \equiv 8 (\text{mód } 11)$

$270t \equiv -46 (\text{mód } 11)$

$6t \equiv -2 (\text{mód } 11)$

$12t \equiv -4 (\text{mód } 11)$

$t \equiv -4 (\text{mód } 11)$

$t = 11q-4$

$x = 270t+54 \quad \forall t \in \mathbb{Z}$

$x = 270(11q-4)+54$

$x = 2970q-1026$

$2970q-1026 \geq 0$

$2970q \geq 1026$

$q \geq 1$

$x = 1944$

5) Un tesoro escondido de monedas de oro pasa a "ser propiedad" de una banda de 15 piratas. Cuando empiezan a repartirse las monedas, les sobran 3. La discusión por el reparto se "anima" y sólo quedan 7 piratas, pero cuando se reparten las monedas entre ellos sobran 2. La discusión continua y el número de piratas se reduce a 4, que sí consiguen repartirse todas las monedas. ¿Cuál es el mínimo número de monedas que podía haber en el tesoro?

$x=15q+3 \longrightarrow x\equiv 3 \pmod{15}$

$x=7k+2 \longrightarrow x\equiv 2 \pmod{7}$

$x=4t+0 \longrightarrow x\equiv 0 \pmod{4}$

Los 3 módulos son coprimos entre sí, por lo que el sistema sí tiene soluciones

$4t\equiv 2 \pmod{7}$

$2t\equiv 1 \pmod{7}$

$8t\equiv 4 \pmod{7}$

$t\equiv 4 \pmod{7}$

$t=7h+4 \longrightarrow x=4(7h+4)=28h+16$

$28h+16\equiv 3 \pmod{15}$

$28h\equiv -13 \pmod{15}$

$13h\equiv -13 \pmod{15}$

$h\equiv -1 \pmod{15}$

$h=15k-1 \longrightarrow x=28(15k-1)+16$

$x=420k-12$

$x\geq 0$

$420k\geq 12$

$k\geq 1$

Solución: Como mínimo habían 408 monedas en el tesoro

⑥ Calcula el menor entero positivo x que verifique la relación:

a) $3^{201} \equiv x \text{ mód}(11)$

Aplicando el teorema de Euler:

$3^{\phi 11} = 3^{10} \equiv 1 \text{ mód}(11)$

$201 = 20 \cdot 10 + 1$

$3^{201} = (3^{10})^{20} \cdot 3$

$(3^{10})^{20} \cdot 3 \equiv x \text{ mód}(11)$

$1^{20} \cdot 3 \equiv x \text{ mód}(11)$

$3 \equiv x \text{ mód}(11)$? $\longrightarrow x = 11k + 3$, para $k = 0 \longrightarrow \boxed{x = 3}$

b) $2^{11} \cdot 3^{13} = x (\text{mód } 7)$

$2^{\phi 7} = 2^6 \equiv 1(7) \longrightarrow 11 = 2 \cdot 5 + 1 \longrightarrow 2^{11} = 2^{6+5}$

$3^{\phi 7} = 3^6 \equiv 1(7) \longrightarrow 13 = 2 \cdot 6 + 1 \longrightarrow 3^{13} = 3^{6+6+1}$

$2^{6+5} \cdot 3^{6+7} \equiv x \text{ mód}(7)$

$2^6 \cdot 2^5 \cdot 3^{6 \cdot 2} \cdot 3^1 \equiv x \text{ mód}(7)$

$2^5 \cdot 3^1 \equiv x \text{ mód}(7)$

$\cancel{2^3} \cdot 2^2 \cdot 3 \equiv x \text{ mód}(7)$

$12 \equiv x \text{ mód}(7)$

$5 \equiv x \text{ mód}(7)$? $\longrightarrow \boxed{x = 5}$

⑦ Calcula el resto de dividir 100^{101} entre 7:

$100^{101} = 7q + R$

$100^{101} \equiv R \text{ mód}(7)$

$(2^2 \cdot 5^2)^{101} \equiv R \text{ mód}(7)$

$2^{202} \cdot 5^{202} \equiv R \text{ mód}(7)$

$2^{\phi 7} = 2^6 \longrightarrow 202 = (6 \cdot 33) + 4 \longrightarrow 2^{202} = (2^6)^{33} \cdot 2^4 = 2^4 \cdot 1^{33}$

$5^{\phi 7} = 5^6 \longrightarrow 202 = (6 \cdot 33) + 4 \longrightarrow 5^{202} = (5^6)^{33} \cdot 5^4 = 5^4 \cdot 1^{33}$

$2^4 \cdot 5^4 \equiv R \text{ mód}(7)$

$\cancel{2^3} \cdot 2 \cdot 5^4 \equiv R \text{ mód}(7)$

$\cancel{2 \cdot 5^2} \cdot 5^2 \equiv R \text{ mód}(7)$

$4 \equiv R (\text{mód } 7)$

Resto de la división: 3

$7 \,|\, 4$

$3 \quad 1$

⑧ Sea p un número primo. Demuestra que $n^p \equiv n \pmod{p}$ $\forall n \geq 0, \in \mathbb{Z}$:

Según el teorema de Euler $\longrightarrow n^{\phi m} \equiv 1 \pmod{m}$ $\begin{cases} n = n \\ m = p \end{cases}$

$n^{p-1} \equiv 1 \text{ mód}(p)$, ya que $mcd(n,p) = 1$

$n \cdot n^{p-1} \equiv n \text{ mód}(p)$

$n^p \equiv n \pmod{p}$

Sin embargo, no sabemos si $mcd(n,p)=1$, por lo que esto solo es válido si $nx + py = 1$

Si el $mcd(p,n) \neq 1$, sin embargo, como p es un número primo, necesariamente, $n = kp$ (múltiplo de p) $\longrightarrow n \equiv 0 \text{ mód}(p)$
$n^p \equiv 0 \text{ mód}(p)$
$n^p \equiv n \text{ mód}(p)$

⑩ Determine la máxima potencia de 2 que divide a cada uno de estos enteros:

a) $1423408 = 10^6 + 4 \cdot 10^5 + 2 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10^1 + 8$

$\boxed{10 = 2 \cdot 5}$

N es múltiplo de 2^n si y solo si el número formado con los n primeros dígitos (desde la derecha) es múltiplo de $2n$:

$1423408 = 2\dot{}$, ya que $8 = 2\dot{}$
$1423408 = 4\dot{}$, ya que $08 = 4\dot{}$
$1423408 = 8\dot{}$, ya que $408 = 8\dot{}$
$1423408 = 16\dot{}$, ya que $3408 = 16\dot{}$
$1423408 \neq 32\dot{}$, ya que $23408 \neq 32\dot{}$

En este caso $x = 2^4$

b) $41578912246 = 2\dot{}$, ya que $6 = 2\dot{}$
$41578912246 \neq 4\dot{}$, ya que $46 \neq 4\dot{}$

En este caso $x = 2^1$

9) Utiliza la congruencia módulo 9 para encontrar el dígito x en el producto: $89878 \cdot 58965 = 5299x56270$.

b) $2\alpha 0$ [

$[89878]_9 \cdot [58965]_9 = [5299x56270]_9$

$[10]_9 = 1$

$[8+\cancel{9}+8+7+8]_9 \cdot [5+8+\cancel{9}+6+5]_9 = [\cancel{8}+\cancel{2}+\cancel{9}+\cancel{9}+x+\cancel{8}+\cancel{6}+\cancel{2}+7+0]$

$[4]_9 [6]_9 = [x]_9$

$[4 \cdot 6]_9 = [x]_9 \longrightarrow [x]_9 = [6]_9 \longrightarrow \boxed{x=6}$

10) La letra asociada al DNI en el NIF indica la clase del número módulo 23, teniendo en cuenta esto:

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

En cada apartado, determina si existe un dígito α que haga que el NIF resultante sea válido:

a) $24\alpha 67890$ A

$[24\alpha 67890]_{23} = [2\cdot 10^7 + 4\cdot 10^6 + \alpha\cdot 10^5 + 6\cdot 10^4 + 7\cdot 10^3 + 8\cdot 10^2 + 9\cdot 10]_{23}$

$2\cdot 10^7 + 4\cdot 10^6 + \alpha\cdot 10^5 + 6\cdot 10^4 + 7\cdot 10^3 + 8\cdot 10^2 + 9\cdot 10^1 \equiv 3 \text{ mód } (23)$

$10^2 = 100 = 4\cdot 23 + 8 \equiv 8 \text{ mód } (23)$

$[10^3]_{23} = [8\cdot 10]_{23} = [11]_{23}$

$[10^4]_{23} = [11\cdot 10]_{23} = [18]_{23} = [-5]_{23}$

$[10^5]_{23} = [-5\cdot 10]_{23} = [-4]_{23}$

$[10^6]_{23} = [10(-4)]_{23} = [6]$

$[10^7]_{23} = [10\cdot 6]_{23} = [-9]_{23}$

$[24\alpha 67890]_{23} = [-18+24-4\alpha-30+77+64+90]_{23}$

$\Rightarrow [-4\alpha]_{23} = [3]_{23}$

$\Rightarrow [-4\cdot 5]_{23} = [3]_{23}$

$\Rightarrow [3]_{23} = [3]_{23} \longrightarrow \boxed{\alpha = 5}$

b) $2\alpha 041327 4$

$[2\alpha0413274]_{23} = [2\cdot10^7 + \alpha\cdot10^6 + 4\cdot10^4 + 10^3 + 3\cdot10^2 + 2\cdot10^1 + 7]_{23}$

$[10^2]_{23} = [8]_{23}$

$[10^3]_{23} = [10\cdot8]_{23} = [11]_{23}$

$[10^4]_{23} = [-5]_{23}$

$[10^5]_{23} = [-4]_{23}$

$[10^6]_{23} = [6]_{23}$

$[10^7]_{23} = [-9]_{23}$

$[2\alpha0413274]_{23} = [-18 + 6\alpha - 20 + 11 + 24 + 20 + 7]_{23}$

$= [\cancel{5} + 6\alpha + \cancel{3} + \cancel{11} + 1 - \cancel{3} + \cancel{7}]_{23} = [6\alpha + 1]_{23}$

$[6\alpha + 1]_{23} = [6]_{23}$

$[6\alpha]_{23} = [5]_{23}$

$[6(-3)]_{23} = [5]_{23} \longrightarrow [-18]_{23} = [5]_{23} \longrightarrow [5]_{23} = [5]_{23}$

$\boxed{\alpha = -3}$, pero el dígito debe ser $0 \leq \alpha \leq 9$, por lo que $\nexists \alpha \in \mathbb{Z}$ que cumpla las condiciones

c) $4459\alpha 203 D$

$[4459\alpha203D]_{23} = [4\cdot10^7 + 4\cdot10^6 + 5\cdot10^5 + 9\cdot10^4 + \alpha\cdot10^3 + 2\cdot10^2 + 3]_{23}$

$= [-36 + 24 - 20 - 45 + 11\alpha + 16 + 3]_{23} = [10 + 1 + 3 + 1 + 11\alpha - 7 + 3]_{23}$

$\Rightarrow [11\alpha + 11]_{23} = [9]_{23} \longrightarrow [11\alpha]_{23} = [-2]_{23}$

$[11\cdot4]_{23} = [-2]_{23} \longrightarrow [44]_{23} = [-2]_{23} \longrightarrow [-2]_{23} = [-2]_{23}$

$\boxed{\alpha = 4}$

④ Un agente de Bolsa tiene dinero invertido en acciones de azucarera y Repsol. Las de azucarera se cotizan en 89 € y las de Repsol a 614 €. Necesita hacer una transacción para disponer de 1000 €. ¿Puede hacerlo comprando acciones de Repsol y vendiendo azucarera? ¿Cuántas de cada tipo como mínimo, comprará y venderá?

$89x - 614y = 1000$

$mcd(89, 614)$

$$\begin{pmatrix} 614 \\ 1 \\ 0 \end{pmatrix} - 6\begin{pmatrix} 89 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 80 \\ 1 \\ -6 \end{pmatrix}$$

$$\begin{pmatrix} 89 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 80 \\ 1 \\ -6 \end{pmatrix} = \begin{pmatrix} 9 \\ -1 \\ 7 \end{pmatrix} \longrightarrow \begin{pmatrix} 80 \\ 1 \\ -6 \end{pmatrix} - 8\begin{pmatrix} 9 \\ -1 \\ 7 \end{pmatrix} = \begin{pmatrix} 8 \\ 9 \\ -62 \end{pmatrix}$$

$$\begin{pmatrix} 9 \\ -1 \\ 7 \end{pmatrix} - \begin{pmatrix} 8 \\ 9 \\ -62 \end{pmatrix} = \begin{pmatrix} 1 \\ -10 \\ 69 \end{pmatrix}$$

$614 \,|\underline{89}$
$80 \quad 6$

$89 \,|\underline{80}$
$9 \quad 1$

$80 \,|\underline{9}$
$8 \quad 8$

$9 \,|\underline{8}$
$1 \quad 1$

$8 \,|\underline{1}$
$0 \quad 8$

$89(69) + 614(-10) = 1$

$89x - 614y = 1000$

$-1000(89 \cdot 69) + 1000(614 \cdot 10) = -1000$

$89(x - 69000) + 614(10000 - y) = 0$

$$\left.\begin{aligned} x &= k + 69000 \\ y &= 10000 - k \end{aligned}\right\} \begin{aligned} &k + 69000 \geq 0 \longrightarrow k \geq -69000 \\ &10000 - k \geq 0 \longrightarrow k \leq 10000 \end{aligned}$$

5) Estudia si estos sistemas de congruencia tienen solución y resuélvelos:

a) $\begin{cases} 3x+9 \equiv 8x+12 \pmod{16} \\ x \equiv 11^{954} \pmod{20} \end{cases} \longrightarrow \begin{cases} x \equiv 9 \pmod{16} \\ x \equiv 1 \pmod{20} \end{cases}$

$\boxed{\begin{matrix} mcd(16,20)=4 \\ 4 \mid 9-1 \checkmark \end{matrix}}$

$x \equiv 11^{954} \pmod{20}$

$20 = 2^2 \cdot 5$

$\phi_{20} = (2^2-2^1)(5^1-5^0) = (2)(4) = 8$

$11^8 \equiv 1 \pmod{20}$

$954 = (119 \cdot 8) + 2$

$11^{954} = (11^8)^{119} \cdot 11^2$

$x = 20q+1$

$20q+1 \equiv 9 \pmod{16}$

$20q \equiv 8 \pmod{16}$

$160q \equiv 64 \pmod{16}$

$0 \equiv 0 \pmod{16}$

$x \equiv (11^8)^{119} \cdot 11^2\ (20)$

$x \equiv 11^2\ (20) \longrightarrow x \equiv 121\ (20) \longrightarrow x \equiv 1\ (20)$

$3x+9 \equiv 8x+12 \pmod{16}$

$-5x \equiv 3 \pmod{16}$

$-15x \equiv 9 \pmod{16}$

$x \equiv 9 \pmod{16}$

$x = 20q+1 \quad \forall q \in \mathbb{Z}$

Como no hay restricción de la segunda congruencia q puede tomar cualquier valor

b) $\begin{cases} 3x \equiv 4 \pmod{7} \\ 5x \equiv 9 \pmod{11} \\ 8x \equiv 12 \pmod{13} \end{cases} \longrightarrow \begin{cases} x \equiv -1 \pmod{7} \\ x \equiv 4 \pmod{11} \\ x \equiv 8 \pmod{13} \end{cases}$

7, 11, 13 son coprimos, por lo que el sistema es resoluble

$3x \equiv 4 \pmod{7}$

$6x \equiv 8 \pmod{7} \longrightarrow x \equiv -1 \pmod{7}$

$5x \equiv 9 \pmod{11}$

$10x \equiv 18 \pmod{11}$

$x \equiv -7 \pmod{11} \longrightarrow x \equiv 4 \pmod{11}$

$8x \equiv 12 \pmod{13}$

$64x \equiv 12(8) \pmod{13}$

$-x \equiv 5 \pmod{13} \longrightarrow x \equiv 8 \pmod{13}$