CONJUNTOS Y NÚMEROS. Curso 2016-2017. **HOJA 5.**

1) Sabemos que dados dos enteros positivos a y b, existen primos $p_1, \ldots, p_s$ de modo que $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ y $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$ para algunos $\alpha_i, \beta_i \in \mathbb{N}$.
   - a) Expresa el $\mathrm{mcd}(a,b)$ y el $\mathrm{mcm}(a,b)$ en función de estas factorizaciones.
   - b) Demuestra que $ab = \mathrm{mcd}(a,b) \cdot \mathrm{mcm}(a,b)$.
   - c) Halla el máximo común divisor de 1547 y 3059 usando dos procedimientos: el descrito en a) y el algoritmo de Euclides.

2) Encuentra todas las parejas $a, b \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,b) = 10$ y $\mathrm{mcm}(a,b) = 100$.

3) Sea $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ la descomposición de n en factores primos. Utilizando la unicidad de la decomposición en primos, demuestra que n tiene $(n_1+1)(n_2+1)\cdots(n_s+1)$ divisores positivos.

4) Demuestra que hay infinitos enteros primos de la forma $4n-1$ y de la forma $6n-1$. Ayuda: Recordar la demostración de Euclides sobre la existencia de infinitos primos.

5) Sea $S \subset \mathbb{Z}$ un subconjunto no vacío que tiene las siguientes dos propiedades:

$$s_1, s_2 \in S \implies s_1 + s_2 \in S$$
$$s \in S \implies -s \in S.$$

Demuestra que $S = \{0\}$ o bien $S = n\mathbb{Z} = \{nk : \ k \in \mathbb{Z}\}$ para algún entero positivo n.

6) Sean a, b, m números naturales con a y b coprimos (primos entre sí). Demuestra que:

$$\text{Si} \quad a \mid m \quad \wedge \quad b \mid m \implies ab \mid m$$

Encuentra un ejemplo que muestre que esto puede no ser cierto si a y b no son coprimos.

7) Halla el conjunto de soluciones de las siguientes ecuaciones diofánticas:

a) $111x + 36y = 15$, b) $10x + 26y = 1224$, c) $6x + 10y = 20$.

8) a) Probar la identidad

$$x^{2k+1} + 1 = (x+1)\sum_{j=0}^{2k}(-1)^j x^{2k-j}.$$

Utilizar esta identidad para demostrar que si $2^n + 1$ es primo, entonces n es una potencia de 2. Los primos de la forma $2^{2^k} + 1$ se denominan *primos de Fermat.*

b) Probar la identidad

$$x^n - 1 = (x-1)\sum_{j=0}^{n-1} x^j$$

Utilizar esta identidad para demostrar que si $2^n - 1$ es primo, entonces n es primo. Se denominan *primos de Mersenne* los de la forma $2^n - 1$.

9) Un entero positivo es perfecto si es igual a la suma de sus divisores propios (todos menos él mismo). Demostrar que si $2^n - 1$ es primo entonces $2^{n-1}(2^n - 1)$ es un número perfecto.

10) a) Teniendo en cuenta que $10 \equiv 1 \pmod 9$, prueba que $n \equiv s \pmod 9$ si s es la suma de los dígitos de n; deduce que n es múltiplo de 9 si y sólo si lo es s. ¿Cuándo será n múltiplo de 3?

b) Usando la misma idea, y partiendo de que $10 \equiv -1 \pmod{11}$, deduce qué suma s debemos hacer con los dígitos de n para saber si es múltiplo de 11.

c) Si en vez de dígitos tuviésemos los *bits* del desarrollo de n en base 2, usa: $2 \equiv -1 \pmod 3$ y deduce qué debemos hacer con esos *bits* para saber si n es múltiplo de 3. O con las cifras de n en base $b = 8$ para saber si n es múltiplo de 7.

d) Prueba que, para n, m dados, y si s_n, s_m son las respectivas sumas de sus dígitos, se cumple: $nm \equiv s_n s_m \bmod(9)$. Deduce qué utilidad puede tener esto si no tenemos la calculadora a mano.

11) a) Sea $\mathcal{U}(\mathbb{Z}_n)$ el subconjunto de $\mathbb{Z}_n$ formado por las unidades de $\mathbb{Z}_n$. Prueba que

$$\overline{a}\overline{b} = \overline{ab} \in \mathcal{U}(\mathbb{Z}_n) \iff \overline{a} \in \mathcal{U}(\mathbb{Z}_n) \text{ y } \overline{b} \in \mathcal{U}(\mathbb{Z}_n)$$

b) Demuestra que la propiedad anterior vale en cualquier anillo conmutativo A (el conjunto $\mathcal{U}(A)$ de unidades es cerrado por el producto).

12) Halla $\mathcal{U}(\mathbb{Z}_7)$ e indica cuál es el inverso multiplicativo de cada uno de sus elementos. Haz lo mismo con $\mathcal{U}(\mathbb{Z}_8)$.

13) a) Demuestra que si $p \in \mathbb{N}$ es primo entonces p divide al número combinatorio $\binom{p}{k}$ para cada $1 \leq k \leq p-1$. ¿Es esto cierto si p no es primo?

b) Probar que si p es primo, en $\mathbb{Z}/p\mathbb{Z}$ se cumple la igualdad $\overline{a}^p + \overline{b}^p = (\overline{a} + \overline{b})^p$.

14) Hallar los inversos de 13 y -15 en $\mathbb{Z}_{23}$ y $\mathbb{Z}_{31}$.

15) Demuestra que la ecuación $13X = 2$ tiene solución única en $\mathbb{Z}_{23}$. Indica cuál es. (Sugerencia: usa el problema anterior).

16) Demuestra que existen infinitos naturales no representables como suma de tres cuadrados. (Sugerencia: estudia los cuadrados módulo 8).

17) Demuestra que si $n > 1$ y $(n-1)! + 1 \equiv 0 \pmod n$ entonces n es primo.

18) Escribe una sola congruencia que sea equivalente al sistema de congruencias: $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 3$ y $x \equiv 3 \pmod 7$.

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \end{cases}$$

19) Demuestra que $2222^{5555} + 5555^{2222}$ es divisible por 7.

20) Prueba que $n^7 - n$ es divisible entre 42, para cualquier entero n.

21) Probar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero para todo n.

22) He comprado bolígrafos a 55 céntimos y rotuladores a 71 céntimos. Si me he gastado en total 20 euros, ¿cuántos he comprado de cada?

23) Calcula el resto que queda al dividir 3^{2011} entre 11.

24) Tengo una bolsa con 30 caramelos y los voy a repartir entre mis sobrinos, dándoles 2 caramelos a cada niño y 7 a cada niña. ¿Cuántos sobrinos tengo si la menor de mis sobrinas se llama Silvia y los mayores de mis sobrinos se llaman Pablo y Julián?

25) Resolver los sistemas de congruencias:

$$a) \begin{cases} x \equiv -5 \pmod 7 \\ x \equiv 17 \pmod{143} \end{cases} \qquad b) \begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 3 \pmod{12} \end{cases}$$

HOJA 5

1. $a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot P_3^{\alpha_3} \cdots P_S^{\alpha_S}$; $b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot P_3^{\beta_3} \cdot \ldots \cdot P_S^{\beta_S}$

a) $mcd(a,b) = P_K^{\gamma_K} \cdots P_j^{\gamma_j}$ donde $P_K \cdots P_j$ pertenecen a la descomposición de factores primos tanto de a como de b. Y $\gamma_K \cdots \gamma_j$ son la mayor potencia común de $P_K \cdots P_j$

$mcm(a,b) = P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdots P_S^{\gamma_S}$ donde $P_1 \ldots P_S$ son todos los factores primos pertenecientes a la descomposición de ambos números y $\gamma_1 \cdots \gamma_S$ es la mayor potencia de $\alpha_i \ldots \alpha_s$ y $\beta_1 \ldots \beta_s$ de tal forma:

$$\gamma_1 = \text{máx}(\alpha_1, \beta_1)$$
$$\gamma_2 = \text{máx}(\alpha_2, \beta_2)$$
$$\vdots$$
$$\gamma_s = \text{máx}(\alpha_s, \beta_s)$$

b) Por una proposición vista en clase sabemos que si M es múltiplo común de a y b $\Longleftrightarrow$ M es múltiplo de $\frac{ab}{mcd(a,b)}$. Por lo tanto podemos denotar los infinitos múltiplos comunes de a y de b así: $M\frac{ab}{mcd(a,b)}$

El mcm (a,b) lo obtenemos cuando M = 1, por lo que:

$$mcm(a,b) = \frac{ab}{mcd(a,b)} \Rightarrow ab = mcm(a,b) \cdot mcd(a,b)$$

qed.

c) FACTORIZACIONES:

$1547 = 7.13.17$

$3059 = 7.19.23$

$mcd(1547, 3059) = \boxed{7}$

$mcm(1547, 3059) =$

$= 7.13.17.19.23 =$

$= \boxed{676039}$

ALGORITMO DE EUCLIDES

$3059 \,\underline{|1547}$
$1512 \quad 1$

$3059 = 1547.1 + 1512$

$1547 \,\underline{|1512}$
$0035 \quad 1$

$1547 = 1512.1 + 35$

$1512 \,\underline{|35}$
$112 \quad 43$
07

$1512 = 35.43 + \textcircled{7}$

mcd(3059,1547

$35 \,\underline{|7}$
$0 \quad 5$

$35 = 7.5$

3 Antes de nada, vamos a demostrar que si a, cuya descomposición en factores primos es: $a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_k^{\alpha_k}$, tiene un divisor que lo llamaremos b, entonces b es uno de los términos del producto:

$$(1 + P_1 + P_1^2 + P_1^3 + \cdots + P_1^{\alpha_1})(1 + P_2 + P_2^2 + \cdots + P_2^{\alpha_2}) \cdots (1 + P_k + P_k^2 + \cdots + P_k^{\alpha_k})$$

En efecto, sea b un divisor de a con la forma:

$b = P_1^i P_2^j \cdots P_K^s$ con $0 \leq i \leq \alpha_1$, $0 \leq j \leq \alpha_2$ $\cdots$ $0 \leq s \leq a_K$

luego b es uno de los términos del producto:

$$(1 + P_1 + P_1^2 + P_1^3 + \cdots + P_1^{\alpha_1})(1 + P_2 + P_2^2 + \cdots + P_2^{\alpha_2}) \cdots (1 + P_k + P_k^2 + \cdots P_k^{\alpha_k})$$

Recíprocamente, cada término del producto anterior es de la de la forma $P_1^i P_2^j \cdots P_K^s$ con $0 \leq i \leq \alpha_1$, $0 \leq j \leq \alpha_2, \ldots, 0 \leq s \leq a_K$ entonces cada término del producto es un divisor de a.

Por lo tanto, según lo que acabamos de demostrar, los divisores de a son los sumandos del producto:

$$(1 + P_1 + P_1^2 + \cdots + P_1^{\alpha_1})(1 + P_2 + P_2^2 + \cdots + P_2^{\alpha_2}) \cdots (1 + P_K + P_K^2 + \cdots + P_K^{\alpha_K})$$

que tienen a su vez $\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_K + 1$ sumandos cada uno, luego el número total de sumandos posibles y, por lo, tanto, de divisores de a es:

Nº divisores: $(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdots (\alpha_K + 1)$

$\boxed{4.}$ a) Supongamos que existe un número finito de primos congruentes con $-1 \pmod 4$ en $C = \{P_1, P_2, \dots, P_n\}$

Antes de nada vamos a probar que si $n \equiv -1 \pmod 4$ entonces hay al menos un número primo p que lo divide de tal forma que $p \equiv -1 \pmod 4$. Para demostrar esto basta con fijarse en la tabla de multiplicación de las clases de restos módulo 4:

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Definimos ahora $N = 4p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} - 1 \; (\alpha_i > 1)$. Se ve que $N \equiv -1$ (mod
Entonces, por la observación anterior existe un $P_i \in C$ tal que $P_i | N$. Resulta evidente que $P_i | 4P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} \Rightarrow P_i | 4P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} - N \Rightarrow$
$\Rightarrow P_i | 1$, lo que es una CONTRADICCIÓN.

b) Supongamos que existe un número finito de primos congruentes con $-1 \pmod 6$ en $C = \{P_1, P_2, \dots, P_n\}$

Antes de nada vamos a probar que si $n \equiv -1 \pmod 6$ entonces existe al menos un número primo p que lo divide de tal forma que $p \equiv -1 \pmod 6$. Para demostrar esto basta con ver la tabla de multiplicación de las clases de los restos módulo 6:

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definimos $N = 6p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} - 1 \; (\alpha_i > 1)$. Se ve que $N \equiv -1$ (mod
Entonces, por la observación anterior existe un $P_i \in C$ tal que $P_i | N$. Resulta evidente que $P_i | 6P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} \Rightarrow P_i | 6P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} - N =$
$\Rightarrow P_i | 1$, lo que es una CONTRADICCIÓN.

4.1 Sabemos que tiene como mínimo dos sobrinas, a las cuales les da siete caramelos a cada una (14 caramelos repartidos; y tiene como mínimo 3 sobrinos, a quienes le da dos caramelos a cada uno (otros 6 caramelos repartidos). Por lo que quedan 10 caramelos por repartir entre sus sobrinos/sobrinas:

$x =$ sobrinos $\qquad y =$ sobrinas

$$\boxed{2x + 7y = 10}$$

De aquí sacamos que no puede tener más sobrinas pues se alcanzaría un número impar (10 es par); por lo que el resto de sobrinos son de género masculino. $2x = 10 \Rightarrow x = 5$

En total: 2 sobrinas y 8 sobrinos

19. $2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$?

$$\begin{array}{l|l} 2222 & 7 \\ \hline 12 & 317 \\ 52 & \\ 3 & \end{array} \qquad \begin{array}{l|l} 5555 & 7 \\ \hline 65 & 793 \\ 25 & \\ 4 & \end{array} \Rightarrow \begin{cases} 2222 \equiv 3 \pmod 7 \\ 5555 \equiv 4 \pmod 7 \end{cases}$$

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7$$

El pequeño teorema de Fermat dice que $3^6 \equiv 1 \pmod 7$ y $4^6 \equiv 1 \pmod 7$.

$$\begin{array}{l|l} 5555 & 6 \\ \hline 15 & 925 \\ 35 & \\ 5 & \end{array} \qquad \begin{array}{l|l} 2222 & 6 \\ \hline 42 & 37 \\ 02 & \end{array} \Rightarrow \begin{cases} 5555 \equiv 5 \pmod 6 \\ 2222 \equiv 2 \pmod 6 \end{cases}$$

$$2222^{5555} + 5555^{2222} \equiv 3^5 + 4^2 \pmod 7$$

$$3^5 + 4^2 = 259$$

$$\begin{array}{l|l} 259 & 7 \\ \hline 49 & 37 \\ 0 & \end{array} \Rightarrow 7 \mid 259 \Rightarrow 7 \mid 2222^{5555} + 5555^{2222}$$

qed.

$\boxed{23.}$ Resto de 3^{2011} al dividirlo con 11 !

Por el pequeño teorema de Fermat sabemos que $3^{10} \equiv 1 \pmod{11}$

$$\boxed{\begin{array}{l|l} 2011 & 10 \\ \cline{2-2} 011 & 201 \\ \ \ 1 & \end{array}} \quad 2011 \equiv 1 \pmod{10}$$

$$3^{2011} \equiv 3^1 \pmod{11} \Rightarrow 3^{2011} \equiv 3 \pmod{11} \Rightarrow \boxed{\text{RESTO} = \overset{3}{\cancel{11}}}$$

$\boxed{20.}$ $42 | n^7 - n \quad \forall n$?

$42 = 2.3.7$; por lo que $n^7 - n$ será divisible entre 42 si es divisible por 2, por 3 y por 7 para todo n.

i) $2 | n^7 - n \quad \forall n$?

- CASO 1 : n par
  Sabemos que todo nº par menos otro número par tiene como resultado un número par. Entonces en $n^7 - n$ obtenemos un nº par, por lo que será divisible entre 2.

- CASO 2: n impar
  Sabemos que todo nº impar menos otro número impar tiene como resultado un número par. Entonces en $n^7 - n$ obtenemos un número par, por lo que será divisible entre 2.

$$\boxed{2 | n^7 - n \quad \forall n}$$

ii) $3 | n^7 - n \quad \forall n$?

- CASO 1 : n divisible entre 3 ⇒ demostrado
- CASO 2: el pequeño teorema de Fermat nos asegura que $n^2 \equiv 1 \pmod 3 \Rightarrow n^6 \equiv 1 \pmod 3 \Rightarrow n^6 - 1 \equiv 0 \pmod 3$

$\Rightarrow 3 | n^6 - 1 \Rightarrow 3 | n(n^6 - 1) \Rightarrow 3 | n^7 - n$

$$\boxed{3 | n^7 - n \quad \forall n}$$

iii) $7 | n^7 - n \quad \forall n$?

- CASO 1: n divisible entre 7 ⇒ demostrado
- CASO 2: el pequeño teorema de Fermat nos asegura que $n^6 \equiv 1 \pmod 7 \Rightarrow n^6 - 1 \equiv 0 \pmod 7 \Rightarrow 7 | n^6 - 1 \Rightarrow$

$\Rightarrow 7 | n(n^6 - 1) \Rightarrow 7 | n^7 - n \quad \boxed{7 | n^7 - n \quad \forall n}$

QUEDA DEMOSTRADO QUE $42 | n^7 - n$ PARA TODO ENTERO N.

17. $\forall n>1 \quad (n-1)!+1 \equiv 0 \pmod{n} \implies n$ es primo

$(n-1)!+1\equiv 0 \pmod{n} \implies (n-1)! \equiv -1 \pmod{n}$

$$\boxed{\forall n>1 \quad (n-1)! \equiv -1 \pmod{n} \implies n \text{ es primo}}$$

~~Vamos a demostrar lo anterior con el contrarrecíproco, enseñan que si n es compuesto entonces $(n-1)! \not\equiv -1 \pmod{n}$.~~

~~Si n es compuesto entonces $\exists k<n$ tal que $k|n$, por lo que entonces $k|(n-1)!$ y $k\equiv 1 \pmod{n}$. Esto significa que k necesita divi~~

Si n es compuesto entonces $\exists k<n$ tal que $k|n$, por lo que entonces $k|(n-1)!$ y $k\equiv 1 \pmod{n}$. Esto significa que k necesita dividir a 1, por lo que <u>n debe ser primo</u>.

18. En general, sabemos que el sistema de congruencias:

$$\begin{cases} x\equiv a \pmod{m} \\ x\equiv b \pmod{n} \\ x\equiv c \pmod{\bar{n}} \end{cases} \text{ es equivalente al siguiente: } \begin{cases} n\bar{n}x\equiv n\bar{n}a \pmod{mn\bar{n}} \\ m\bar{n}x\equiv m\bar{n}b \pmod{mn\bar{n}} \\ mnx\equiv mnc \pmod{mn\bar{n}} \end{cases};$$

por lo que lo aplicaremos a continuación:

$$\begin{cases} x\equiv 1 \pmod{4} \\ x\equiv 2 \pmod{3} \\ x\equiv 3 \pmod{7} \end{cases} \text{ es equivalente a:}$$

$$\begin{cases} 7.3.x\equiv 7.3.1 \pmod{3.4.7} \\ 7.4.x\equiv 7.4.2 \pmod{3.4.7} \\ 3.4.x\equiv 3.4.3 \pmod{3.4.7} \end{cases} \implies \begin{cases} 21x\equiv 21 \pmod{84} \\ 28x\equiv 56 \pmod{84} \\ 12x\equiv 36 \pmod{84} \end{cases}$$

$\boxed{25.}$

$$a)\ \begin{cases} x \equiv -5 \ (\text{mod } 7) \\ x \equiv 17 \ (\text{mod } 143) \end{cases} \longrightarrow \quad x = 7k - 5$$

$$[x]_{143} = [7k-5]_{143} = [17]_{143} \Longrightarrow [7k]_{143} = [22]_{143} \Longrightarrow$$

$$\Longrightarrow [k]_{143} = [7]^{-1}_{143}\ [22]_{143}$$

$$\boxed{\begin{aligned} &[7]^{-1}_{143} = [7^{\phi(143)-1}]_{143} \\ &\quad \phi(143) = \phi = (11.13) = (11-1)(13-1) = 10.12 = 120 \\ &\qquad\qquad [7]^{-1}_{143} = [7^{120-1}]_{143} = [7^{119}]_{143} \end{aligned}}$$

$$\Longrightarrow [k]_{143} = [7^{119}]_{143}\ [22]_{143} = [7^{119}.22]_{143} \Longrightarrow k = 7^{119}.22 + 143q$$

$$x = 7(7^{119}.22 + 143q) = 7^{120}.22 + 7.143q = 7^{120}.22 + 1001q$$

$$\boxed{x \equiv 7^{120}.22 \ (\text{mod } 1001)}$$

$$b)\ \begin{cases} x \equiv 7 \ (\text{mod } 8) \\ x \equiv 3 \ (\text{mod } 12) \longrightarrow \ x = 3 + 12K \end{cases}$$

17. | HALLAR INVERSOS

a.1) de 13 en $\mathbb{Z}_{23}$

- TEOREMA DE EULER: $[13]_{23}^{-1} = [13^{\phi(23)-1}]_{23}$

$$\phi(23) = 22$$

$$[13^{\phi(23)-1}]_{23} = [13^{21}]_{23}$$

- IDENTIDAD DE BEZOUT:

$\exists [13]_{23}^{-1} \Longleftrightarrow mcd(13, 23) = 1$ (se cumple)

$\begin{array}{r|l} 23 & 13 \\ \hline 10 & 1 \end{array}$ $\quad \underline{23} = \underline{13} + 10 \longrightarrow 10 = \underline{23} - \underline{13}$

$\begin{array}{r|l} 13 & 10 \\ \hline 3 & 1 \end{array}$ $\quad \underline{13} = 10 + 3 \longrightarrow 3 = \underline{13} - 10 \Rightarrow 3 = \underline{13} - (\underline{23} - \underline{13}) \Rightarrow$

$\Rightarrow 3 = 2.\underline{13} - \underline{23}$

$\begin{array}{r|l} 10 & 3 \\ \hline 1 & 3 \end{array}$ $\quad 10 = 3.3 + 1$

$\Downarrow 1 = 10 - 3.3 \Rightarrow 1 = (\underline{23} - \underline{13}) - 3(2.\underline{13} - \underline{23})$

$1 = \underline{23} - \underline{13} - 6.\underline{13} + 3.\underline{23} \Rightarrow 1 = \underset{\alpha}{\overset{\shortparallel}{4}}.23 - \underset{\beta}{\overset{\shortparallel}{7}}.13$

Por lo tanto, $[13]_{23}^{-1} = [-7]_{23} = [16]_{23}$ $\quad \begin{array}{l} \alpha = 4 \\ \beta = -7 \end{array}$

a.2) de 13 en $\mathbb{Z}_{31}$.

- TEOREMA DE EULER

$[13]_{31}^{-1} = [13^{\phi(31)-1}]_{31} =$

$\phi(31) = 30 \quad ; [13^{30-1}]_{31} = [13^{29}]_{31} = [13]_{31}^{-1}$

- IDENTIDAD DE BEZOUT:

$\exists [13]_{31}^{-1} \Longleftrightarrow mcd(13, 31) = 1$ (se cumple)

$\begin{array}{r|l} 31 & 13 \\ \hline 5 & 2 \end{array}$ $\quad \underline{31} = \underline{13}.2 + 5 \rightarrow 5 = \underline{31} - 2.\underline{13}$

$\begin{array}{r|l} 13 & 5 \\ \hline 3 & 2 \end{array}$ $\quad \underline{13} = 5.2 + 3 \rightarrow 3 = \underline{13} - 2.5 \rightarrow 3 = 13 - 2.(31 - 2.13) = 5.\underline{13} + 2.\underline{31}$

$\begin{array}{r|l} 5 & 3 \\ \hline 2 & 1 \end{array}$ $\quad 5 = 3 + 2 \rightarrow 2 = 5 - 3 \rightarrow 2 = (\underline{31} - 2.\underline{13}) - (5.\underline{13} + 2.\underline{31}) \rightarrow$

$\rightarrow 2 = -1.\underline{31} - 7.\underline{13}$

$\begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array}$ $\quad 3 = 2 + ① \rightarrow ① = 3 - 2 \rightarrow ① = (5.\underline{13} + 2.\underline{31}) - (-1.\underline{31} - 7.\underline{13}) =$

~~6.13 + 8~~ $= \underset{\alpha}{\overset{\shortparallel}{\underbrace{12}}}.13 + \underset{\beta}{\overset{\shortparallel}{\underbrace{3}}}.31$

$$[13]_{31}^{-1} = [12]_{31}$$

$\boxed{25.}$

b)

$$\mathbb{Z}/_{12}\mathbb{Z} \xrightarrow[\text{del resto}]{\text{T}^{\text{a}}\text{ chino}} \mathbb{Z}/_{4}\mathbb{Z} \times \mathbb{Z}/_{3}\mathbb{Z}$$

$$[n]_{12} \longrightarrow \left([n]_4 \ , \ [n]_3\right)$$

$$[3]_{12} \longrightarrow \left([3]_4 , \ [0]_3\right)$$

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 3 \pmod{12} \end{cases} \longleftrightarrow \begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 0 \pmod 3 \end{cases}$$

$$\hookrightarrow [3]_{12} \longrightarrow \left([3]_4 , \ \underbrace{[0]_3}\right)$$

$\updownarrow$ redundante con $7 \pmod 8$

$x \equiv 7 \pmod 8$

$\boxed{5.}$ $S \subset \mathbb{Z}$, $S \neq \phi$

$s_1 + s_2 \in S \Rightarrow s_1 + s_2 \in S$

$s \in S \Rightarrow -s \in S$.

- Si $s_1 = 0 \Rightarrow S = \{0\}$
- Si $s_1 \neq 0 \Rightarrow \exists -s_1 \Rightarrow s_1 + (-s_1) = 0 \Rightarrow 0$ siempre está.
- Si $s_1 \neq 0$ (supongamos s_1 el mínimo de S^+).
  $\hookrightarrow s_1 = n$.

Supongamos que hay un elemento que no es múltiplo de $s_1 = n$. $\Rightarrow s_2 = an + b \Rightarrow s_2 = as_1 + b$

Cogemos $s_2 - n$, y lo realizamos hasta que $s_2 - an < s_1$, por lo que llegamos a una contradicción por lo que $\forall s \in S$ son múltiplos de algún n.

22. Bolígrafos 55 cent.
Rotuladores 71 cent. $\Big\} \Rightarrow 20$ €

$$1 = -24 \cdot \underline{71} + 31 \cdot \underline{55}$$

$$2000 = -48000 \cdot \underline{71} + 62000 \cdot \underline{55}$$

$$(\alpha, \beta) = (-48000, 62000) + (55, -71)T$$

$$\frac{62000}{71} \geq T \geq \frac{48000}{55} \qquad \boxed{T = 873}$$

$\frac{62000}{71} = 873'\ldots \qquad \frac{48000}{55} = 872'\ldots$

21. $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero $\forall n$.

$$\frac{3n^5 + 5n^3 + 7n}{15} \in \mathbb{Z}$$

$\boxed{7.}$

a) $111x + 36y = 15$

$$\begin{array}{r|l} 111 & 3 \\ 37 & 37 \\ 1 & \end{array} \qquad \begin{array}{r|l} 36 & 3 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$\text{mcd}(111,36) = 3$

$111\alpha + 36\beta = 5$

$\Updownarrow$

$37\alpha + 12\beta = 1$

$\begin{array}{r|l} 37 & 12 \\ \hline 1 & 3 \end{array}$ $\quad 37 = 3.12 + 1 \rightarrow 1 = \underline{37} - 3.\underline{12}$

$\alpha = 1 \quad \beta = -3$

$\alpha = 1 \Rightarrow x = 5$

$\beta = -3 \Rightarrow y = -15$ UNA SOLUCIÓN

$(x,y) = (5,-15) + \cancel{(111,-3)}\ (-36,111)\,T$

CONJUNTO DE SOLUCIONES

$(x,y) = (5,-15) + (-36,111)\,T \iff \begin{array}{l} x = 5 - 36T \\ y = -15 + 111T \end{array}$

---

b) $10x + 26y = 1224$

$$\begin{array}{r|l} 10 & 5 \\ 2 & 2 \\ 1 & \end{array} \qquad \begin{array}{r|l} 26 & 2 \\ 13 & 13 \\ 1 & \end{array}$$

$\text{mcd}(10,26) = 2$

$10\alpha + 26\beta = 2 \iff 5\alpha + 13\beta = 1$

$\begin{array}{r|l} 13 & 5 \\ \hline 3 & 2 \end{array}$ $\quad \underline{13} = 2.\underline{5} + \underline{3} \rightarrow 3 = \underline{13} - 2.\underline{5}$

$\begin{array}{r|l} 5 & 3 \\ \hline 2 & 1 \end{array}$ $\quad \underline{5} = \underline{3} + \underline{2} \rightarrow 2 = \underline{5} - 3 \rightarrow 2 = 5 - (\underline{13} - 2.\underline{5}) = 3.\underline{5} - \underline{13}$

$\begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array}$ $\quad 3 = 2 + 1 \rightarrow 1 = 3 - 2 \rightarrow 1 = \underline{13} - 2.\underline{5} - (3.\underline{5} - \underline{13}) \Rightarrow$

$\Rightarrow 1 = 2.\underline{13} + [illegible] - 5.\underline{5}$

$\beta = 2 \quad \alpha = \cancel{6} -5$

$\beta = 2 \Rightarrow y = 1224$

$\alpha = \cancel{6}\ -5 \Rightarrow x = \cancel{3672}\ -3060$ UNA SOLUCIÓN

$(x,y) = (-3060, 1224) + (-26, 10)\,T$

CONJUNTO DE SOLUCIONES

$(x,y) = (-3060,1224) + (-26,10)\,T \iff \begin{array}{l} x = -3060 - 26T \\ y = 1224 + 10T \end{array}$

c) $6x + 10y$

$$6\alpha + 10\beta = 2$$
$$\Updownarrow$$
$$3\alpha + 5\beta = 1$$

10	2
5	5
1	

6	2
3	3
1	

$\text{mcd}(10,6) = 2$

$5 \,\underline{|3}$ $5 = 3 + 2 \rightarrow 2 = \underline{5} - \underline{3}$

$2 \quad 1$

$3 \,\underline{|2}$ $3 = 2 + 1 \rightarrow 1 = \underline{3} - 2 \Rightarrow 1 = \underline{3} - (\underline{5} - \underline{3}) = 2.\underline{3} - \underline{5}$

$1 \quad 1$

$$1 = 2.3 - 5$$

$\alpha = 2 \; ; \; \beta = -1$

$$\boxed{x = 20 \qquad y = -10}$$

UNA SOLUCIÓN

$$(x,y) = (20,-10) + (10,-6)T$$

CONJUNTO DE SOLUCIONES:

$$\boxed{(x,y) = (20,-10) + (10,-6)T \iff \begin{array}{l} x = 20 + 10T \\ y = -10 - 6T \end{array}}$$

~~21~~ $\boxed{22}$ ~~2~~ bolígrafos a 55 cent. / rotuladores a 71 cent. $\Rightarrow$ Gasto = 20 €

x = bolígrafos
y = rotuladores

$$55x + 71y = 2000$$
$$55\alpha + 71\beta = 1$$

55	5
11	11
1	

71	71
1	

$\text{mcd}(55,71) = 1$

$71 \,\underline{|55}$ $\underline{71} = \underline{55} + 16 \rightarrow 16 = \underline{71} - \underline{55}$

$16 \quad 1$

$55 \,\underline{|16}$ $\underline{55} = 16.3 + 7 \rightarrow 7 = \underline{55} - 3(\underline{71} - \underline{55}) \rightarrow$

$7 \quad \mathbf{3}$ $\rightarrow 7 = \mathbf{4}.\underline{55} - 3.\underline{71}$

$16 \,\underline{|7}$ $16 = 7.2 + 2 \rightarrow 2 = 16 - 2.7 \Rightarrow 2 = \underline{71} - \underline{55} - 2(\mathbf{4}.\underline{55} - 3.\underline{71}) \rightarrow$

$2 \quad 2$ $\rightarrow$ ~~$2 = 4.71 - 5.55$~~ $2 = 7.\underline{71} - 9.\underline{55}$

~~$= 4.55 - 3.71 - 3.(4.71 - 5.55)$~~ $\Rightarrow$

$7 \,\underline{|2}$ $7 = 3.2 + 1 \rightarrow$ ~~$1 = 7 - 3.2 =$~~

$1 \quad 3$

~~$1 = 23.55 - 15.71$~~ ~~$\alpha = 23$~~ ~~$\beta = -15$~~ $\Rightarrow$ ~~$x = 46000$~~ ~~$y = -3000$~~

$$\Rightarrow 1 = 4.\underline{55} - 3.\underline{71} - 3(7.\underline{71} - 9.\underline{55}) = 31.\underline{55} - 24.\underline{71}$$

$\alpha = 31 \Rightarrow x = 62000$

$\beta = -24 \Rightarrow y = -48000$

$$\boxed{(x,y) = (62000, -48000) + (-71, 55)T}$$

C

~~para~~ $62000 - 71T \geq 0 \rightarrow T \leq \frac{62000}{71}$

$-48000 + 55T \geq 0 \rightarrow T \geq 48000/55$

$T = 873$

$\rightarrow$ despéjam

x e y

$\downarrow$ bolis $\quad \downarrow$ rot

$\boxed{2.}$ $a, b \in \mathbb{Z}$

$$\begin{array}{r|l} 1000 & 2 \\ 500 & 2 \\ 250 & 2 \\ 125 & 5^3 \end{array}$$

$\text{mcd}(a,b) = 10$

$\text{mcm}(a,b) = 100 = 2^2 . 5^2$

$\text{mcd}(a,b) \cdot \text{mcm}(a,b) = ab = 1000$

$a = 2.5.2.5 \longleftrightarrow b = 2.5$

$a = 2.5.2 \longleftrightarrow b = 2.5.5$

$a = 2.5.5 \longleftrightarrow b = 2.5.2$

$a = 2.5 \longleftrightarrow b = 2.5.2.5$

4 parejas (o 2 si no importa el orden)

$\boxed{13.}$ a) $p \in \mathbb{N}$ si p es primo $p \mid \binom{p}{k}$ $1 \leq k \leq p-1$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!} \Rightarrow p \mid \binom{p}{k}$$

$$\binom{p}{k} = \binom{p-1}{k-1} + \binom{p-1}{k} = [\dots] = \binom{0}{0} = 1 \in \mathbb{Z}$$

b) $\mathbb{Z}/p\mathbb{Z}$

$$[a]^p + [b]^p = ([a] + [b])^p \pmod{p}$$

$$([a] + [b])^p = [a]^p \underbrace{+ \binom{p}{1}[b]^1 . [a]^{p-1} + \dots + \binom{p}{p-1}[a]^1 . [b]^{p-1} +}_{\overset{\equiv}{0} \pmod{p}} [b]^p$$

$2 - 1$ es primo, entonces

$$x^n - 1 = (x-1)\cdot\sum_{j=0}^{n-1} x^j \Rightarrow (x-1)\left(x^0 + x^1 + x^2 + x^3 + \dots + x^{n-1}\right) \Rightarrow$$

$$\Rightarrow \cancel{x^1} + \cancel{x^2} + \cancel{\dots} + x^n - \left(x^0 + \cancel{x^1} + \cancel{x^2} + \cancel{\dots} + \cancel{x^{n-1}}\right) \Rightarrow x^n - 1$$

$$2^n - 1 = (2-1)\sum_{j=0}^{n-1} 2^j$$

Si n no es primo $\Rightarrow$ $n = a.b$

$$2^{a.b} - 1 = \underbrace{(2^a - 1)}_{\substack{\downarrow \\ >1}} \underbrace{\sum_{j=0}^{b-1} 2^{aj}}_{\substack{\downarrow \\ >1}}$$

Hemos demostrado que si n no es primo, entonces $2^n - 1$ no es primo (el contrarrecíproco).