Hoja 6. Aritmética Modular

Susana Cubillo (2021)

Ejercicios recopilados de los apuntes y Hojas de problemas de los profesores del Dpto. Matemática Aplicada a las TIC (Campus Montegancedo). UPM.

1. Demuestra que si p es primo y $p \geq 5$, entonces $p \equiv 1 (\mathrm{mod}\ 6)$ ó $p \equiv 5 (\mathrm{mod}\ 6)$.

Sol.: Si $p \equiv 0 (\mathrm{mod}\ 6)$, entonces p es múltiplo de 6, y no puede ser primo
Si $p \equiv 2 (\mathrm{mod}\ 6)$, entonces $6/(p-2)$, $6k = p-2$ para algún $k \in \mathbb{Z}$, $p = 6k+2$, p es múltiplo de 2, y no puede ser primo
Si $p \equiv 3 (\mathrm{mod}\ 6)$, entonces p es múltiplo de 3, y no puede ser primo
Si $p \equiv 4 (\mathrm{mod}\ 6)$, entonces p es múltiplo de 2, y no puede ser primo
Por tanto, $p \equiv 1 (\mathrm{mod}\ 6)$ ó $p \equiv 5 (\mathrm{mod}\ 6)$.

2. Sabiendo que $1234567 \equiv 7\ (mod\ 10)$, $90123 \equiv 3\ (mod\ 10)$, $2468 \equiv 18\ (mod\ 25)$, $13579 \equiv 4\ (mod\ 25)$, calcula el valor del menor residuo no negativo a tal que:

a) $1234567 \times 90123 \equiv a\ (mod\ 10)$ b) $2468 \times 13579 \equiv a\ (mod\ 25)$

Sol.: a) $1234567 \times 90123 \equiv (7 \times 3)\ (mod\ 10) \equiv 1 (mod\ 10)$; el menor residuo no negativo es 1
b) $2468 \times 13579 \equiv (18 \times 4) (mod\ 25) \equiv 72\ (mod\ 25) \equiv 22\ (mod\ 25)$

3. Utiliza el método de la regla del nueve para comprobar que dos de las siguientes igualdades son falsas. ¿Qué puede decirse de la otra igualdad?

a) $5783 \times 40162 = 233256846$ c) $9787 \times 1258 = 12342046$
b) $8901 \times 5743 = 52018443$

Sol.:
a) $(5+7+8+3) \times (4+1+6+2) = 23 \times 13 \equiv (5 \times 4)\ (\mathrm{mod}\ 9) \equiv 2 (\mathrm{mod}\ 9)$
$(2+3+3+2+5+6+8+4+6) = 39 \equiv 3 (\mathrm{mod}\ 9)$ FALSA

b) $18 \times 19 = 342 \equiv 0 \pmod 9$; $27 \equiv 0 \pmod 9$. NO SE PUEDE DECIR NADA

c) $31 \times 16 = 496 \equiv 1 \pmod 9$; $22 \equiv 4 \pmod 9$. FALSA

4. Comprueba si 1213141516171819 y 192837465564738291 son divisibles por 11. ¿Qué cifra falta en la igualdad $871782\_1200 = 14!$?

Sol.: 1213141516171819 no es divisible por 11; 192837465564738291 sí lo es.

5. Sea n un número natural y n' el número natural obtenido al permutar dos dígitos consecutivos cualesquiera de n . Demostrar que n y n' son congruentes módulo 9.

Sol.: $n = x_0 + 10\,x_1 + 10^2\,x_2 + \cdots + 10^i\,x_i + 10^{i+1}\,x_{i+1} + \cdots + 10^n\,n$

$n' = x_0 + 10\,x_1 + 10^2\,x_2 + \cdots + 10^i\,x_i + 10^{i+1}\,x_{i+1} + \cdots + 10^n\,n$

Por tanto, $n - n' = 10^i\,x_i + 10^{i+1}\,x_{i+1} - \left(10^i\,x_{i+1} + 10^{i+1}\,x_i\right) =$

$10^i\,x_i\,(1 - 10) + 10^i\,x_{i+1}\,(10 - 1) \equiv 0\ (mod\ 9)$

6. Halla los elementos inversibles de $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ y $\mathbb{Z}_{15}$.

Sol.: $U_6 = \{[1]_6,\ [5]_6\}$ $U_7 = \{[1]_7,\ [2]_7,\ [3]_7,\ [4]_7,\ [5]_7,\ [6]_7\ \}$

$U_8 = \{[1]_8,\ [3]_8,\ [5]_8, [7]_8\ \}$

$U_{15} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\ \}$

7. Halla los inversos de:

a) 6 en $\mathbb{Z}_{17}$ b) 3 en $\mathbb{Z}_{10}$ c) 5 en $\mathbb{Z}_{12}$ d) 7 en $\mathbb{Z}_{16}$ e) 5 en $\mathbb{Z}_{13}$

f) 777 en $\mathbb{Z}_{1009}$ g) 11 en $\mathbb{Z}_{39}$ h) 328 en $\mathbb{Z}_{641}$

Sol.: $[6]_{17}^{-1} = [3]_{17}$ $[3]_{10}^{-1} = [7]_{10}$ $[5]_{12}^{-1} = [5]_{12}$ $[7]_{16}^{-1} = [7]_{16}$

$[5]_{13}^{-1} = [8]_{13}$ $[777]_{1009}^{-1} = [-274]_{1009} = [735]_{1009}$ $[11]_{39}^{-1} = [-7]_{39} = [32]_{39}$

$[328]_{641}^{-1} = [-299]_{641} = [342]_{641}$

8. a) Demuestra que los enteros menores que 11, excepto el 1 y el 10, pueden agruparse de dos en dos de manera que cada uno de ellos es el inverso del otro en $\mathbb{Z}_{11}$.

b) Utiliza el Teorema de Wilson para hallar el resto de dividir $10!$ por 11.

c) Utiliza el Teorema de Wilson para hallar el resto de dividir 15! por 17.

9. Sean a y b números enteros y p primo. Usa el Teorema de Euler para demostrar que $(a+b)^p = (a^p + b^p) \pmod p$

10. ¿Cuál es el último dígito de los números 7^{93}, 23^{189}, 6^{20}?

Sol.: Buscamos x tal que $7^{93} \equiv x\ (mod\ 10)$
$mcd(7,10) = 1$; $7^{\phi(10)} \equiv 1(mod\ 10)$; $7^4 \equiv \mathbf{1}(\boldsymbol{mod\ 10})$
$7^{93} = (7^4)^{23} \cdot 7 \equiv 1 \cdot 7\ (mod\ 10) \equiv 7\ (mod\ 10)$. Por tanto, el último dígito es 7.

$23^{189} \equiv x\ (mod\ 10)$; $23^{189} = (23^4)^{47} \cdot 23 \equiv 1 \cdot 23\ (mod\ 10) \equiv \mathbf{3}\ (\boldsymbol{mod\ 10})$. El último dígito es 3.

$6^{20} \equiv x\ (mod\ 10)$; 6 y 10 no son primos entre sí
$6^{20} = 2^{20} \cdot 3^{20} = (2^4)^5 \cdot (3^4)^5 \equiv 6^5 \cdot 1\ (mod\ 10) \equiv 6^2 \cdot 6^2 \cdot 6\ (mod\ 10) \equiv \mathbf{6}(\boldsymbol{mod\ 10})$. El último dígito es 6.

11. Calcula el resto de la división de $1! + 2! + 3! + \cdots + n!$ entre 10 , para todo $n \in \mathbb{N}$.

12. ¿Cuántos elementos tienen inverso en $\mathbb{Z}_{25725}$?

13. Calcula los restos de dividir

a) 3^{47} entre 23 b) 6^{592} entre 11 c) 3^{15} entre 17
d) 125^{4577} entre 13 e) 6^{20} entre 23 f) 11^{954} entre 20
g) $(140^{1221} + 28^{753})$ entre 13 h) 5^{28575} entre 57 i) 8^{501} entre 57
j) 17^{158} entre 23 k) 2^{510} entre 17

Sol.: a) $3^{47} \equiv x\ (mod\ 23)$; $mcd(3,23) = 1$; $3^{\phi(23)} \equiv 1\ (mod\ 23)$; $3^{22} \equiv 1\ (mod\ 23)$
$3^{47} = (3^{22})^2 \cdot 3^3 \equiv 1 \cdot 3^3\ (mod\ 23) \equiv \mathbf{4}\ (\boldsymbol{mod\ 23})$

b) $6^{592} \equiv x\ (mod\ 11)$; $6^{592} = (6^{10})^{59} \cdot 6^2 \equiv 6^2\ (mod\ 11) \equiv \mathbf{3}\ (\boldsymbol{mod\ 11})$

c) $3^{15} = 3^{16} \cdot 3^{-1} \equiv 1 \cdot 3^{-1}\ (mod\ 17) \equiv 3^{-1}\ (mod\ 17) \equiv \mathbf{6}\ (\boldsymbol{mod\ 17})$

d) $125^{4577} \equiv x\ (mod\ 13)$; $125^{4577} \equiv 8^{4577}\ (mod\ 13) \equiv (8^{12})^{381} \cdot 8^5 (mod\ 13) \equiv 8^5\ (mod\ 13) \equiv 8^2 \cdot 8^2 \cdot 8\ (mod\ 13) \equiv (-1) \cdot (-1) \cdot 8 (mod\ 13) \equiv \mathbf{8}\ (\boldsymbol{mod\ 13})$

e) $6^{20} \equiv x\ (mod\ 23)$; $6^{22} = 6^{20} \cdot 6^2 \equiv 1 (mod\ 23)$; $6^{20} \equiv (6^{-1})^2 (mod\ 23) \equiv 4^2 \equiv (mod\ 23) \equiv \mathbf{16}\ (\boldsymbol{mod\ 23})$

f) $11^{954} \equiv x\ (mod\ 20)$; $11^{954} = (11^8)^{119} \cdot 11^2 \equiv 11^2\ (mod\ 20) \equiv \mathbf{1}\ (\boldsymbol{mod\ 20})$

g) $140^{1221} \equiv 10^{1221}\ (mod\ 13) \equiv (-3)^{1221}\ (mod\ 13) \equiv ((-3)^{12})^{101} \cdot (-3)^9\ (mod\ 13)$

$\equiv (-3)^9\ (mod\ 13) \equiv (-3)^4 \cdot (-3)^4 \cdot (-3)(mod\ 13) \equiv 3 \cdot 3 \cdot (-3)(mod\ 13)$

$\equiv (-27)(mod\ 13) \equiv \mathbf{12}\ (\boldsymbol{mod\ 13})$

$28^{753} \equiv 15^{1221}\ (mod\ 13) \equiv (-3)^{1221}\ (mod\ 13) \equiv ((-3)^{12})^{101} \cdot (-3)^9\ (mod\ 13)$

14. Demuestra que si a/c, b/c y $mcd(a,b) = 1$, entonces $a \cdot b/c$.

15. Calcula x en la expresión a) $5^{8574} \equiv \mathrm{x}\ (mod\ 13)$ b) $53^{82} \equiv \mathrm{x}\ (mod\ 8)$

16. ¿En qué cifra acaba el número 3^{3658}?

17. Calcula a) 2009^{105} en $\mathbb{Z}_{107}$ b) 19^{191} en $\mathbb{Z}_{221}$

Sol.: a) $2009^{105} \equiv x(mod\ 107)$

$mcd(2009, 107) = 1$; por tanto, $2009^{\phi(107)} \equiv 1(mod\ 107)$; $2009^{106} \equiv 1(mod\ 107)$

$2009^{106} = 2009^{105} \cdot 2009 \equiv 1\ (mod\ 107)$;

Tenemos que buscar el inverso de 2009 en $\mathbb{Z}_{107}$

$2009x - 107y = 1$; $2009 \cdot 49 - 107 \cdot 920 = 1$. Por tanto, $[2009]_{107}^{-1} = [49]_{107}$

Finalmente, $2009^{105} \equiv 49\ (mod\ 107)$;

c) $19^{191} \equiv x\ (mod\ 221)$

$mcd(19, 221) = 1$; por tanto, $19^{\phi(221)} \equiv 1(mod\ 221)$;

$\phi(221) = \phi(13) \cdot \phi(17) = 12 \cdot 16 = 192$; $19^{192} \equiv 1(mod\ 221)$

$19^{192} = 19^{191} \cdot 19 \equiv 1\ (mod\ 221)$;

Tenemos que buscar el inverso de 19 en $\mathbb{Z}_{221}$

$19x - 221y = 1$; $19 \cdot (-93) - 221 \cdot (-8) = 1$. Por tanto, $[19]_{221}^{-1} = [128]_{221}$

Finalmente, $19^{191} \equiv 128\ (mod\ 221)$;

18. Comprueba que $2^{340} \equiv 1\ (mod\ 11)$ y que $2^{340} \equiv 1\ (mod\ 31)$.

Concluye que $2^{340} \equiv 1\ (\mathrm{mod}\ 341)$.

19. Prueba, mediante congruencias, que

a) $3^{405} + 2^{801}$ es divisible por 7

b) $3^{2n+5} + 2^{4n+1}$ es divisible por 7 para todo $n \in \mathbb{N}$.

20. Demuestra que $\forall\, n \in \mathbb{Z}^+$, las últimas cifras de los números n y n^5 son iguales.

21. Efectúa la siguiente operación en $\mathbb{Z}_{203}$: $[5]+[5]\cdot[4]^{169}\cdot[17]^{-1}$.

Sol.:

$[4]^{169}$: $4^{169}\equiv x\ (mod\ 203)$

$mcd\ (4,203)=1$, por lo que $4^{\phi(203)}\equiv 1\ (mod\ 203)$; $\phi(203)=\phi(7)\cdot\phi(29)=168$

$4^{168}\equiv 1\ (mod\ 203)$; $4^{169}\equiv 4^{168}\cdot 4\equiv 4\ (mod\ 203)$

$[17]^{-1}$: $17\,x-203\,y=1$; $17\cdot 12-203\cdot 1=1$; por tanto, $[17]^{-1}=[12]$

Finalmente, en $\mathbb{Z}_{203}$: $[5]+[5]\cdot[4]^{169}\cdot[17]^{-1}=[5]+[5]\cdot[4]\cdot[12]=[42]$

22. Prueba, mediante congruencias, que $3^{405}+2^{801}$ es divisible por 7.

Sol.: $3^{\phi(7)}=3^6$; $3^{405}=(3^6)^{67}\cdot 3^3\equiv 3^3\ (mod\ 7)\equiv 6\ (mod\ 7)$

$2^{801}=(2^6)^{133}\cdot 2^3\equiv 2^3\ (mod\ 7)\equiv 1\ (mod\ 7)$

Por tanto, $(3^{405}+2^{801})\equiv(6+1)(mod\ 7)\equiv 0\ (mod\ 7)$

23. ¿Cuál es el resto de dividir $1^5+2^5+3^5+\cdots+100^5$ entre 4?

Sol.: $(1^5+2^5+3^5+4^5)\equiv(1+0+(-1)+0)\ (mod\ 4)\equiv 0\ (mod\ 4)$

$(5^5+6^5+7^5+8^5)\equiv(1^5+2^5+3^5+4^5)\ (mod\ 4)\equiv 0\ (mod\ 4)$ ....

Siguiendo el proceso $1^5+2^5+3^5+\cdots+100^5\equiv 0\ (mod\ 4)$

Por tanto, el resto es 0.

24. Un reloj analógico se pone en hora a las 12 en punto de un día determinado. ¿Qué hora marcaría después de transcurridas 5^{100} horas exactas, si no se para nunca y es totalmente preciso?

Sol.: $5^{100}\equiv x(\ mod\ 12)$

$\phi(12)=\phi(2^2)\cdot\phi(3)=4$; $5^4\equiv 1(\ mod\ 12)$; $5^{100}=(5^4)^{25}\equiv 1(\ mod\ 12)$

El resto es 1, y por tanto marcaría la 1.

25. Resuelve las siguientes ecuaciones

a) $21x\equiv 18$ en Z_{30}. b) $27x\equiv 84$ en Z_{120} c) $20x\equiv 8$ en Z_{12}

d) $28x\equiv 77$ en Z_{637} e) $35x\equiv 42$ en Z_{49} $f)$ $66x=42$ en $\mathbb{Z}_{168}$

Sol.:

a) $[21]_{30}\cdot[x]_{30}=[18]_{30}$; $21x\equiv 18\ (\mathrm{mod}\ 30)$; $21x-30y=18$;

$mcd\ (21,30)=3$; por tanto, 3 soluciones en Z_{30} ;

$7x-10\,y=6$; $7\cdot(-2)-10\cdot(-2)=6$; $x=-2+10\,t,\ t\in\mathbb{Z}$

$$[x]_{30}=\{[8]_{30},[18]_{30},[28]_{30}\}$$

b) $[27]_{120}\cdot[x]_{120}=[84]_{120}$; $27x\equiv 84\ (\mathrm{mod}\ 120)$; $27x-120y=84$;

$mcd\ (27{,}120) = 3$; por tanto, 3 soluciones en Z_{120} ;
$9x - 40\,y = 28$; $9 \cdot (252) - 40 \cdot (56) = 28$; $x = 12 + 40\,t,\ t \in \mathbb{Z}$

$$[x]_{120} = \{[12]_{120}, [52]_{120}, [92]_{120}\}$$

c) $[20]_{12} \cdot [x]_{12} = [8]_{12}$; $20\mathrm{x} \equiv 8\ (\mathrm{mod}\ 12)$; $20x - 12y = 8$;

$mcd\ (20{,}12) = 4$; por tanto, 4 soluciones en Z_{12} ;
$5x - 3\,y = 2$; $5 \cdot (1) - 3 \cdot (1) = 2$; $x = 1 + 3\,t,\ t \in \mathbb{Z}$

$$[x]_{12} = \{[1]_{12}, [4]_{12}, [7]_{12}, [10]_{12}\}$$

d) $[28]_{637} \cdot [x]_{637} = [77]_{637}$; $28\mathrm{x} \equiv 77\ (\mathrm{mod}\ 637)$; $28x - 637y = 77$;

$mcd\ (28, 637) = 7$; por tanto, 7 soluciones en Z_{637} ;
$4x - 91\,y = 11$; $4 \cdot (-20) - 91 \cdot (-1) = 11$; $x = -20 + 91\,t,\ t \in \mathbb{Z}$

$$[x]_{637} = \{[71]_{637}, [162]_{637}, [253]_{637}, [344]_{637}, [435]_{637}, [526]_{637}, [617]_{637}\}$$

e) $[35]_{49} \cdot [x]_{49} = [42]_{49}$; $35\mathrm{x} \equiv 42\ (\mathrm{mod}\ 49)$; $35x - 49y = 42$;

$mcd\ (35, 49) = 7$; por tanto, 7 soluciones en Z_{49} ;
$5x - 7\,y = 6$; $5 \cdot (-3) - 7 \cdot (-3) = 6$; $x = -3 + 7\,t,\ t \in \mathbb{Z}$

$$[x]_{49} = \{[4]_{49}, [11]_{49}, [18]_{49}, [25]_{49}, [32]_{49}, [39]_{49}, [46]_{49}\}$$

f) $[66]_{168} \cdot [x]_{168} = [42]_{168}$; $66\mathrm{x} \equiv 42\ (\mathrm{mod}\ 168)$; $66x - 168y = 42$;

$mcd\ (66, 637168) = 6$; por tanto, 6 soluciones en Z_{168} ;
$11x - 28\,y = 7$; $11 \cdot (-5) - 28 \cdot (-2) = 7$; $x = -5 + 28\,t,\ t \in \mathbb{Z}$

$$[x]_{168} = \{[23]_{168}, [51]_{168}, [79]_{168}, [107]_{168}, [135]_{168}, [163]_{168}\}$$

26. Resuelve las siguientes ecuaciones:

a) $5\mathrm{x} \equiv 1(\mathrm{mod}\ 11)$ b) $4\mathrm{x} \equiv 3(\mathrm{mod}\ 7)$ c) $5\mathrm{x} \equiv 7(\mathrm{mod}\ 15)$.

Sol.: a) $\begin{cases} x = -2 + 11t \\ y = -1 + 5t \end{cases}$ $t \in \mathbb{Z}$

b) $\begin{cases} x = 6 + 7t \\ y = 3 + 4t \end{cases}$ $t \in \mathbb{Z}$

c) No tiene solución, al ser $mcd(5,15) = 5$, que no divide a 7

27. a) ¿Qué entero tanto al dividirlo por 2 como al dividirlo por 3 da de resto 1?
b) ¿Qué entero es divisible por 5 pero queda resto 1 al dividirlo por 3?

Sol.: a) $\begin{cases} x \equiv 1\ (mod\ 2) \\ y \equiv 1\ (mod\ 3) \end{cases}$ $x = 1 \cdot 3 \cdot (3)_2^{-1} + 1 \cdot 2 \cdot (2)_3^{-1} + 6t = 3 - 2 + 6t = 1 + 6t\,, t \in \mathbb{Z}$

b) $\begin{cases} x \equiv 0\ (mod\ 5) \\ y \equiv 1\ (mod\ 3) \end{cases}$ $x = 0 + 1 \cdot 5 \cdot (5)_3^{-1} + 15t = 5 \cdot (-1) + 15t = 10 + 15t\,, t \in \mathbb{Z}$

28. Halla un número natural cuyos restos al dividirlo por 3, 4, 5 y 6 sean, respectivamente 2, 3, 4 y 5.

Sol.:

$\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 4) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 6) \end{cases}$ $\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 2^2) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 2) \\ x \equiv 5\ (mod\ 3) \end{cases}$ $\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 2^2) \\ x \equiv 4\ (mod\ 5) \end{cases}$

$x = 2 \cdot 20 \cdot (20)_3^{-1} + 3 \cdot 15 \cdot (15)_4^{-1} + 4 \cdot 12 \cdot (12)_5^{-1} + 60t =$
$= 40 \cdot (-1) + 45 \cdot (-1) + 48 \cdot 3 + 60t = 59 + 6t\,, t \in \mathbb{Z}$

29. Resuelve el sistema de congruencias
$x \equiv 2 (\mathrm{mod}\ 5)$, $2x \equiv 1 (\mathrm{mod}\ 7)$, $3x \equiv 4 (\mathrm{mod}\ 11)$.

Sol.: $\begin{cases} x \equiv 2\ (mod\ 5) \\ 2x \equiv 1\ (mod\ 7) \\ 3x \equiv 4\ (mod\ 11) \end{cases}$ $\begin{cases} x \equiv 2\ (mod\ 5) \\ x \equiv 4\ (mod\ 7) \\ x \equiv 5\ (mod\ 11) \end{cases}$

$x = 2 \cdot 77 \cdot (77)_5^{-1} + 4 \cdot 55 \cdot (55)_7^{-1} + 5 \cdot 35 \cdot (35)_{11}^{-1} + 387\,t =$
$= 154 \cdot 3 + 220 \cdot (-1) + 175 \cdot 6 + 385\,t = 137 + 385\,t\,, t \in \mathbb{Z}$

30. Halla los números enteros n tales que $n + 1$ es múltiplo de 3, $n + 3$ es múltiplo de 4 y $n + 5$ es múltiplo de 7.

Sol.: $\begin{cases} (n+1) \equiv 0\ (mod\ 3) \\ (n+3) \equiv 0\ (mod\ 4) \\ (n+5) \equiv 0\ (mod\ 7) \end{cases}$ $\begin{cases} n \equiv 2\ (mod\ 3) \\ n \equiv 1 (mod\ 4) \\ n \equiv 2\ (mod\ 7) \end{cases}$

$$n = 2 \cdot 28 \cdot (28)_3^{-1} + 1 \cdot 21 \cdot (21)_4^{-1} + 2 \cdot 12 \cdot (12)_7^{-1} + 84\,t = \\ = 56 \cdot 1 + 21 \cdot 1 + 24 \cdot 3 + 84\,t = 65 + 84\,t\,, t \in \mathbb{Z}$$

31. Resuelve el sistema de congruencia $\begin{cases} 4x \equiv 11 (\mathrm{mod}\ 15) \\ 10x \equiv 8\ (\mathrm{mod}\ 12) \end{cases}$

Sol.: $\begin{cases} x \equiv 44 (\mathrm{mod}\ 15) \\ 5x \equiv 4\ (\mathrm{mod}\ 6) \end{cases}$ $\begin{cases} x \equiv 14 (\mathrm{mod}\ 15) \\ x \equiv 2\ (\mathrm{mod}\ 6) \end{cases}$ $\begin{cases} x \equiv 14\ (mod\ 3) \\ x \equiv 14\ (mod\ 5) \\ x \equiv 2\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \end{cases}$ $\begin{cases} x \equiv (-1)\ (mod\ 5) \\ x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \end{cases}$

$$x = (-1) \cdot 6 \cdot (6)_5^{-1} + 0 \cdot 15 \cdot (15)_2^{-1} + 2 \cdot 10 \cdot (10)_3^{-1} + 30\,t\ = -6 + 20 + 30\,t = \\ 14 + 30\,t = [14]_{30}$$

32. Sabiendo que $mcd(b, 561) = 1$, justificar las siguientes afirmaciones:

a) $b^2 \equiv 1 (\mathrm{mod}\ 3)$ b) $b^{10} \equiv 1 (\mathrm{mod}\ 11)$ c) $b^{16} \equiv 1 (\mathrm{mod}\ 17)$
d) $b^{500} \equiv 1 (mod\ 3)$ e) $b^{560} \equiv 1 (mod\ 11)$ f) $b^{560} \equiv 1 (mod\ 17)$

g) $b^{560} \equiv 1 (\mathrm{mod}\ 561)$

33. Una banda de 17 piratas se reúne para repartirse un cofre con más de cien monedas de oro. Efectuado equitativamente el reparto sobra una moneda. En la pelea resultante para adjudicarla muere un pirata y vuelven a realizar el reparto sobrando una moneda. ¿Cuál es el mínimo número de monedas que puede contener el cofre?
Supongamos que la solución anterior es el número real de monedas que contenía el cofre y que la historia continúa: siempre que sobran monedas en el reparto hay pelea y muere un pirata. ¿Cuántos piratas quedarán vivos cuando en el reparto no sobre ninguna moneda?

Sol.: a) $x = nº\ monedas > 100$

$$\begin{cases} x \equiv 1 (\mathrm{mod}\ 17) \\ x \equiv 1\ (\mathrm{mod}\ 16) \end{cases}$$

$$x = 1 \cdot 16 \cdot (16)_{17}^{-1} + 1 \cdot 17 \cdot (17)_{16}^{-1} + 272\,t\ = -16 + 17 + 272\,t = 1 + 272\,t$$

Por lo tanto, el mínimo número de monedas es 273

b) 273 ha de ser múltiplo del número de piratas que quedarán vivos.
Al ser $273 = 3 \cdot 7 \cdot 13$, el mayor múltiplo menos de 16 es 13. Quedarán 13 piratas.

34. Se reparten cuatro bolsas iguales de caramelos entre tres grupos de niños. En el primer grupo, que consta de cinco niños, se reparten dos bolsas y sobra un caramelo. En el segundo grupo, de seis niños, se reparte una bolsa y sobran dos caramelos. En el tercer grupo, de siete niños, se reparte una bolsa y sobran tres caramelos. Sabiendo que, en total, el número de caramelos no llegaba a 500, ¿cuántos caramelos había en cada bolsa?

35. Un distribuidor de equipos informáticos efectuó un pedido de entre 1000 y 1500 equipos a un fabricante que se los envió en contenedores completos con capacidad para 68 equipos cada uno. El distribuidor los repartió a los diferentes puntos de venta usando furgonetas con capacidad para 20 equipos y quedando 32 equipos sin repartir en el almacén. ¿Cuántos equipos pidió el distribuidor a la fábrica?

36. De un determinado número natural n se sabe que es el mínimo número impar que si se divide por 3 su resto es 1, si se divide por 5 su resto es 4, y si se divide por 7 su resto es 3.
a) Halla dicho número n.
b) ¿Es n un número primo? Justifica la respuesta enunciando la propiedad utilizada.

37. Halla todos los números enteros n tales que:

a) $n+1$ es múltiplo de 7, $n+4$ es múltiplo de 6 y $n+4$ es múltiplo de 5.
b) $n+1$ es múltiplo de 3, $n+3$ es múltiplo de 4 y $n+5$ es múltiplo de 7.
c) $7n+1$ es múltiplo de 3, y $6n+6$ es múltiplo de 8.

38. Resuelve, si es que tienen solución, los siguientes sistemas de congruencias.

a) $\begin{cases} 21x \equiv 15 \pmod{30} \\ 6x \equiv 5 \pmod{25} \end{cases}$ b) $\begin{cases} x \equiv 1139^{502} \pmod{25} \\ x+17 \equiv 14 \pmod{4} \end{cases}$ c) $\begin{cases} 9!\, x \equiv 9^{21} \pmod{11} \\ x \equiv 47^{111} \pmod{6} \end{cases}$

d) $\begin{cases} 15x \equiv 2 \pmod{58} \\ 24x \equiv 32 \pmod{80} \end{cases}$ e) $\begin{cases} 120x \equiv 180 \pmod{450} \\ 24x \equiv 76 \pmod{100} \end{cases}$ f) $\begin{cases} 168x \equiv 24 \pmod{220} \\ 56x \equiv 40 \pmod{68} \end{cases}$

g) $\begin{cases} x \equiv 2 \ (mod\ 5) \\ 2x \equiv 1 \ (mod\ 7) \\ 3x \equiv 4 \ (mod\ 11) \end{cases}$ h) $\begin{cases} 4x \equiv 11 \pmod{15} \\ 10x \equiv 8 \pmod{12} \end{cases}$ i) $\begin{cases} 160x \equiv 180 \pmod{390} \\ 24x \equiv 76 \pmod{100} \end{cases}$

j) $\begin{cases} x \equiv 2\ (mod\ 30) \\ x \equiv 3\ (mod\ 77) \\ x \equiv 14\ (mod\ 99) \end{cases}$ k) $\begin{cases} 3x \equiv 6\ (mod\ 12) \\ 2x \equiv 5\ (mod\ 7) \\ 3x \equiv 1\ (mod\ 5) \end{cases}$ l) $\begin{cases} 2x \equiv 5 (mod\ 7) \\ 4!\, x \equiv 3\ (mod\ 5) \\ 6x \equiv 8\ (mod\ 20) \end{cases}$

m) $\begin{cases} 6x \equiv 10 (mod\ 16) \\ 4!\, x \equiv 3\ (mod\ 5) \\ 5x \equiv 7\ (mod\ 12) \end{cases}$

Sol.:

a) $\begin{cases} 21x \equiv 15\ (\mathrm{mod}\ 30) \\ 6x \equiv 5\ (\mathrm{mod}\ 25) \end{cases}$ $\begin{cases} 7x \equiv 5\ (\mathrm{mod}\ 10) \\ 6x \equiv 5\ (\mathrm{mod}\ 25) \end{cases}$ $\begin{cases} 7x \equiv 5\ (mod\ 2) \\ 7x \equiv 5 (mod\ 5) \\ 6x \equiv 5\ (mod\ 5^2) \end{cases}$ $\begin{cases} x \equiv 5\ (\mathrm{mod}\ 2) \\ x \equiv 21 \cdot 5\ (\mathrm{mod}\ 5^2) \end{cases}$

$\begin{cases} x \equiv 5\ (\mathrm{mod}\ 2) \equiv 1 (mod\ 2) \\ x \equiv 5\ (\mathrm{mod}\ 5^2) \end{cases}$

$x = 25 \cdot (25)_2^{-1} + 5 \cdot 2 \cdot (2)_{25}^{-1} + 50\, t = 25 \cdot 1 + 10 \cdot 13 + 50\, t = 5 + 50\, t = [5]_{50}$

b) $\begin{cases} x \equiv 1139^{502}\ (\mathrm{mod}\ 25) \\ x + 17 \equiv 14\ (\mathrm{mod}\ 4) \end{cases}$ $\begin{cases} x \equiv 14^{502}\ (\mathrm{mod}\ 25) \\ x \equiv 1\ (\mathrm{mod}\ 4) \end{cases}$

$\phi(25) = 20 \quad 14^{502} = (14^{20})^{25} \cdot 14^2 \equiv 14^2\ (mod\ 25) \equiv 21 (mod\ 25)$

$\begin{cases} x \equiv 21\ (\mathrm{mod}\ 25) \\ x \equiv 1\ (\mathrm{mod}\ 4) \end{cases}$

$x = 21 \cdot 4 \cdot (4)_{25}^{-1} + 1 \cdot 25 \cdot (25)_4^{-1} + 100\, t = 84 \cdot 19 + 25 \cdot 1 + 100\, t = 21 + 100\, t = [21]_{100}$

c) $\begin{cases} 9!\, x \equiv 9^{21}\ (\mathrm{mod}\ 11) \\ x \equiv 47^{111}\ (\mathrm{mod}\ 6) \end{cases}$ $\phi(11) = 10 \quad 9^{21} = (9^{10})^2 \cdot 9 \equiv 9\ (mod\ 11)$

$\begin{cases} x \equiv 9\ (\mathrm{mod}\ 11) \\ x \equiv (-1)\ (\mathrm{mod}\ 6) \end{cases}$

$x = 9 \cdot 6 \cdot (6)_{11}^{-1} + (-1) \cdot 11 \cdot (11)_6^{-1} + 66\, t = 54 \cdot 2 - 11 \cdot (-1) + 66\, t = 53 + 66\, t$

d) $\begin{cases} 15x \equiv 2\ (\mathrm{mod}\ 58) \\ 24x \equiv 32\ (\mathrm{mod}\ 80) \end{cases}$ $\begin{cases} 15x \equiv 2\ (mod\ 2) \\ 15x \equiv 2\ (mod\ 29) \\ 3x \equiv 4\ (mod\ 10) \end{cases}$ $\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 4 (mod\ 29) \\ 3x \equiv 4\ (mod\ 2) \\ 3x \equiv 4\ (mod\ 5) \end{cases}$ $\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 4\ (mod\ 29) \\ x \equiv 3\ (mod\ 5) \end{cases}$

$x = 4 \cdot 10 \cdot (10)_{29}^{-1} + 3 \cdot 58 \cdot (58)_5^{-1} + 290\, t = 40 \cdot 3 + 174 \cdot 2 + 290\, t = 178 + 290\, t = [178]_{290}$

e) $\begin{cases}120x \equiv 180 \pmod{450} \\ 24x \equiv 76 \pmod{100}\end{cases}$ $\begin{cases}4x \equiv 6 \pmod{15} \\ 6x \equiv 19 \pmod{25}\end{cases}$ $\begin{cases}4x \equiv 6 \pmod{3} \\ 4x \equiv 6 \pmod{5} \\ 6x \equiv 19 (mod\ 5^2)\end{cases}$

$\begin{cases}x \equiv 0 \pmod{3} \\ 6x \equiv 19 \pmod{25}\end{cases}$ $\begin{cases}x \equiv 0 \pmod{3} \\ x \equiv 21 \cdot 19 \pmod{25}\end{cases}$ $\begin{cases}x \equiv 0 \pmod{3} \\ x \equiv (-1) \pmod{25}\end{cases}$

$$x = (-1) \cdot 3 \cdot (3)_{25}^{-1} + 75\,t = (-3) \cdot 17 + 75\,t = 24 + 75\,t = [24]_{75}$$

f) $\begin{cases}168x \equiv 24 \pmod{220} \\ 56x \equiv 40 \pmod{68}\end{cases}$ $\begin{cases}42x \equiv 6 \pmod{55} \\ 14x \equiv 10 \pmod{17}\end{cases}$ $\begin{cases}42x \equiv 6 \pmod{5} \\ 42x \equiv 6 \pmod{11} \\ x \equiv 11 \cdot 10 (mod\ 17)\end{cases}$

$\begin{cases}2x \equiv 1 \pmod{5} \\ 9x \equiv 6 \pmod{11} \\ x \equiv 8 (mod\ 17)\end{cases}$ $\begin{cases}x \equiv 3 \pmod{5} \\ x \equiv 8 \pmod{11} \\ x \equiv 8 (mod\ 17)\end{cases}$

$$x = 3 \cdot 187 \cdot (187)_5^{-1} + 8 \cdot 85 \cdot (85)_{11}^{-1} + 8 \cdot 55 \cdot (55)_{17}^{-1} + 935\,t =$$
$$561 \cdot 3 + 680 \cdot 7 + 440 \cdot 13 + 935\,t = 12163 + 935\,t = 108 + 935\,t = [108]_{935}$$

g) $\begin{cases}x \equiv 2 (mod\ 5) \\ 2x \equiv 1 (mod\ 7) \\ 3x \equiv 4 (mod\ 11)\end{cases}$ $\begin{cases}x \equiv 2 (mod\ 5) \\ x \equiv 4 (mod\ 7) \\ x \equiv 5 (mod\ 11)\end{cases}$

$$x = 2 \cdot 77 \cdot (77)_5^{-1} + 4 \cdot 55 \cdot (55)_7^{-1} + 5 \cdot 35 \cdot (35)_{11}^{-1} + 385\,t =$$
$$154 \cdot 3 + 220 \cdot (-1) + 175 \cdot 6 + 385\,t = 1292 + 385\,t = [137]_{385}$$

h) $\begin{cases}4x \equiv 11 \pmod{15} \\ 10x \equiv 8 \pmod{12}\end{cases}$ $\begin{cases}x \equiv 44 \pmod{15} \\ 5x \equiv 4 \pmod{6}\end{cases}$ $\begin{cases}x \equiv 14 \pmod{15} \\ x \equiv (-4) \pmod{6}\end{cases}$ $\begin{cases}x \equiv (-1) \pmod{3} \\ x \equiv (-1) \pmod{5} \\ x \equiv (-4) (mod\ 2) \\ x \equiv (-4) (mod\ 3)\end{cases}$

$$x = (-1) \cdot 10 \cdot (10)_3^{-1} + 4 \cdot 6 \cdot (6)_5^{-1} + (-4) \cdot 15 \cdot (15)_2^{-1} + 30\,t =$$
$$(-10) \cdot 1 + 24 \cdot 1 - 60 \cdot 1 + 30\,t = 14 + 30\,t = [14]_{30}$$

i) $\begin{cases}160x \equiv 180 \pmod{390} \\ 24x \equiv 76 \pmod{100}\end{cases}$ $\begin{cases}8x \equiv 9 \pmod{39} \\ 6x \equiv 19 \pmod{25}\end{cases}$ $\begin{cases}8x \equiv 9 \pmod{3} \\ 8x \equiv 9 \pmod{13} \\ x \equiv 21 \cdot 19 (mod\ 25)\end{cases}$

$\begin{cases}8x \equiv 9 \pmod{3} \\ 8x \equiv 9 \pmod{13} \\ x \equiv 21 \cdot 19 (mod\ 25)\end{cases}$ $\begin{cases}x \equiv 0 \pmod{3} \\ x \equiv 6 \pmod{13} \\ x \equiv (-1) (mod\ 25)\end{cases}$

$$x = 6 \cdot 75 \cdot (75)_{13}^{-1} + (-1) \cdot 39 \cdot (39)_{25}^{-1} + 975\, t =$$
$$450 \cdot 4 - 39 \cdot (-16) + 975\, t = 474 + 975\, t = [474]_{975}$$

39. Dado el sistema de congruencias $\begin{cases} x \equiv 4\ (mod\ 8) \\ x \equiv \mathrm{k}\ (mod\ 6) \\ x \equiv -1\ (mod\ 15) \end{cases}$

a) Determina los valores enteros de k para que el sistema tenga solución

b) Determina las soluciones del sistema anterior para los valores de k hallados en el apartado anterior.

Sol.:

a)

$mcd(8,6) = 2$, por lo que ha de verificarse $2/(4-k)$

$mcd(6,15) = 3$, por lo que ha de verificarse $3/(k+1)$

$\begin{cases} 2m = 4 - k \\ 3p = k + 1 \end{cases}$; $k = 4 - 2m = 3p - 1$; $3p + 2m = 3$;

resolviendo esta ecuación diofántica, nos queda $p = 1 + 2t,\ t \in \mathbb{Z}$,

$k = 3\,(1 + 2t) - 1 = 2 + 6t\,,\ t \in \mathbb{Z}$. Por tanto k = 2

b)

$$\begin{cases} x \equiv 4\ (mod\ 8) \\ x \equiv \mathrm{k}\ (mod\ 6) \\ x \equiv -1\ (mod\ 15) \end{cases} \qquad \begin{cases} x \equiv 4\ (mod\ 2^3) \\ x \equiv 2\ (mod\ 2) \\ \cancel{x \equiv 2\ (mod\ 3)} \\ x \equiv -1 (mod\ 3) \\ \cancel{x \equiv -1 (mod\ 5)} \end{cases} \qquad \begin{cases} x \equiv 4\ (mod\ 8) \\ x \equiv 2\ (mod\ 3) \\ x \equiv -1\ (mod\ 5) \end{cases}$$

$$x = 4 \cdot 15 \cdot (15)_8^{-1} + 2 \cdot 40 \cdot (40)_3^{-1} - 24 \cdot (24)_5^{-1} + 120\, t =$$
$$60 \cdot (-1) + 80 \cdot 1 - 24 \cdot (-1) + 120\, t = 44 + 120\, t = [44]_{120}$$

40. Se tiene una cantidad par de monedas, menor que 600, que se quieren disponer en filas. Si se ordenan, de manera contigua, completando filas de 17 monedas cada una, sobran 8 monedas. Si se consideran únicamente la mitad de las monedas iniciales y se ordenan en filas de 7 monedas, sobran 3 monedas. Averigua la posible cantidad inicial de monedas. ¿Es única la solución?

Sol.: Sea y el número de monedas. Como es par, $y = 2x$.

$\begin{cases} 2x \equiv 8 \pmod{17} \\ x \equiv 3 \pmod{7} \end{cases}$ $\begin{cases} x \equiv 72 \pmod{17} \\ x \equiv 3 \pmod{7} \end{cases}$ $\begin{cases} x \equiv 4 \pmod{17} \\ x \equiv 3 \pmod{7} \end{cases}$

$x = 4 \cdot 7 \cdot (7)_{17}^{-1} + 3 \cdot 17 \cdot (17)_{73}^{-1} + 119\,t =$

$28 \cdot 5 + 51 \cdot 5 + 119\,t = 395 + 119\,t = 38 + 119\,t$

$y = 2 \cdot x = 2 \cdot 38 + 119\,t = 76 + 238\,t$. Al ser $y < 600$, y puede tomar los siguientes valores $y = \{76,\ 314,\ 552\}$

41. Una determinada empresa desea emitir un anuncio en dos cadenas de televisión con el objetivo de que sea visto diariamente por 910 personas. Al realizar un estudio de audiencia se sabe que cada vez que se emite en CTV1 va a ser visto por 325 personas, mientras que en CTV2 sólo será visto por 26. ¿Cuántas veces al día debe emitirse en cada una de las cadenas para cumplir, con un coste mínimo, el objetivo previsto de las exactamente 910 personas teniendo en cuenta que CTV1 cobra 10.000 euros por cada emisión y CTV2 sólo 1.000 euros?

42. Un grupo de menos de 300 turistas viaja en 5 autocares iguales completos y llega a un hotel. Las mesas del comedor del hotel son de 9 personas y de 4 personas. Los turistas de los dos primeros autocares se sientan alrededor de la mesas de 9 personas resultando 3 personas sin acomodar; éstas, junto con los turistas de los 3 autocares restantes completos, se sientan alrededor de las mesas de 4 personas, quedando todos acomodados para la cena. Al día siguiente, van a realizar una visita a un museo donde deben entrar en grupos de 24 personas. Si al hacer la distribución en grupos de 24 personas, el último grupo es de tan sólo 15 personas, ¿cuántos turistas viajan en total?

Sol.: Sea x = número de turistas en cada autocar. Por tanto, nº turistas = $5x$

$$\begin{cases} 2x \equiv 3\ (mod\ 9) \\ 3x + 3 \equiv 0\ (mod\ 4) \\ x \equiv 15\ (mod\ 24) \end{cases}$$

Resolvemos el sistema

$\begin{cases} x \equiv 15 (mod\ 9) \\ 3x \equiv 1\ (mod\ 4) \\ x \equiv 15\ (mod\ 24) \end{cases}$ $\begin{cases} x \equiv 6\ (mod\ 9) \\ x \equiv (-1)\ (mod\ 4) \\ x \equiv 15\ (mod\ 24) \end{cases}$ $\begin{cases} x \equiv 6\ (mod\ 3^2) \\ x \equiv (-1)\ (mod\ 2^2) \\ x \equiv 15\ (mod\ 2^3 \cdot 3) \end{cases}$

43. (examen abril 2011) Se presentan 800 manuscritos a un concurso literario. Después de una primera selección, en la que se eliminan más de 300 manuscritos, se

pretende almacenar los manuscritos eliminados en cajas de la misma capacidad y que todas las cajas estén completas, para que no se extravíe ningún manuscrito. En principio, se eligen cajas con capacidad para 6 manuscritos, pero sobran 3; si se eligen cajas para que contengan 7 manuscritos cada una sobran 5, y si se eligen cajas para que contengan 11 manuscritos cada una, no sobra ningún manuscrito. ¿Cuántos manuscritos quedan en concurso después de la primera selección?

44. (examen julio 2013)

a) Obtén la solución general de la ecuación diofántica $172x + 36y = 4$. ¿Cuántas de las soluciones particulares verifican $10 \leq x \leq 30$? Descríbelas.
b) Halla el valor de x sabiendo que es el menor múltiplo de 4, no inferior a 250, que da de resto 4 al dividirlo tanto por 6 como por 9.
c) Realiza las siguientes operaciones: $\overline{9} \cdot \overline{47}^{79993} + \overline{-7}^{-1}$ en Z_{11}.

45. Dada la ecuación en congruencias $[54]_{21}[x]_{21} = [m]_{21}$
a) Obtén los valores de m para los que la ecuación tiene solución.
b) Para dichos valores, ¿cuál es el número de soluciones no congruentes?
c) Resuelve la ecuación para $m = 12$.

Sol.: a) $mcd(54,21) = 3$ debe dividir a m . Por tanto $m = \{0, 3, 6, 9, 12, 15, 18\}$

b) El número de soluciones no congruentes es $mcd(54,21) = 3$

c) $[54]_{21}[x]_{21} = [12]_{21}$; $54x \equiv 12\ (mod\ 21)$; $21/(12 - 54x)$; por tanto, debe existir $y \in \mathbb{Z}$, tal que $21y = 12 - 54x$; $54x + 21y = 12$, y ésta es la ecuación que debemos resolver.

Simplificamos dividiendo por 3 : $18x + 7y = 4$.

Una posible solución es: $18(1) + 7(-2) = 4$. Por tanto $x = 1 + 7t,\ t \in \mathbb{Z}$.

$$x = 1, 8, 15, 22, 29, \ldots.$$

Y las tres soluciones: $[x]_{21} = \{[1]_{21}, [8]_{21}, [15]_{21}\}$

46. (examen julio 2010)
a) Sabiendo que 13331 es primo, resolver la ecuación $2x \equiv 4^{13329}$ en Z_{13331} , con $0 \leq x \leq 13331$.
b) Resolver, si tiene solución, el sistema de congruencias $\begin{cases} 7x \equiv 6\ (mod\ 12) \\ 5x \equiv 5\ (mod\ 7) \\ 4x \equiv 1\ (mod\ 5) \end{cases}$

Sol.: a) Por el Teorema de Euler, $4^{13330} \equiv 1\ (mod\ 13331)$.

$$4 \cdot 2x \equiv 4 \cdot 4^{13329} \equiv 1\ (mod\ 13331)$$
$$8x \equiv 1\ (mod\ 13331)$$

Y por tanto, sólo falta hallar el inverso de 8 en Z_{13331}, para lo que se utilizará en Algoritmo de Euclides. Resulta ser $[8]^{-1}{}_{13331} = [8332]_{13331}$

b)

$$\begin{cases} 7x \equiv 6\ (mod\ 12) \\ 5x \equiv 5\ (mod\ 7) \\ 4x \equiv 1\ (mod\ 5) \end{cases} \qquad \begin{cases} 7x \equiv 6\ (mod\ 2^2) \\ 7x \equiv 6\ (mod\ 3) \\ x \equiv 1\ (mod\ 7) \\ x \equiv 4\ (mod\ 5) \end{cases} \qquad \begin{cases} 3x \equiv 2\ (mod\ 2^2) \\ x \equiv 0\ (mod\ 3) \\ x \equiv 1\ (mod\ 7) \\ x \equiv 4\ (mod\ 5) \end{cases}$$

47. (examen noviembre 2011)

a) Calcular $8!\ (mod\ 11)$ y $21^{18}(mod\ 11)$
b) Comprobar si 299 es primo
c) Calcular el inverso de 28 en Z_{299}
d) Calcular 28^{527} en Z_{299}

Sol.: a) Por el Teorema de Wilson $10! \equiv 10\ (mod\ 11)$, y multiplicando por el inverso de 10, nos queda $9! \equiv 1\ (mod\ 11)$. Por tanto, $9 \cdot 8! \equiv 1\ (mod\ 11)$. Sólo falta obtener el inverso de 9 módulo 11, que resulta ser 5.

Finalmente, $8! \equiv 5\ (mod\ 11)$.

Por otra parte, $21^{18}(mod\ 11) \equiv 10^{18}\ (mod\ 11)$

Podemos utilizar el Teorema de Euler, pero observemos que $10^2 = 100 \equiv 1(mod\ 11)$, ya que 99 es múltiplo de 11. Por tanto,

$$10^{18}\ (mod\ 11) \equiv (10^2)^9(mod\ 11) \equiv 1(mod\ 11)$$

b) $\sqrt{299} = 17, \ldots$. Por tanto, debemos buscar los divisores entre los números primos menores o iguales que 17.

299 no es múltiplo de 2, ni de 3, ni de 5, ni de 7, ni de 11. Pero sí es múltiplo de 13, ya que $299 = 13 \cdot 23$. Por tanto no es un número primo.

c) Para calcular el inverso, planteamos la ecuación $28\,x \equiv 1\ (mod\ 299)$

$28x + 299\,y = 1$. Buscamos una solución por el algoritmo de Euclides, quedando

$28\ (-32) + 299\ (3) = 1$. Por tanto, el inverso será $x = -32 + 299\,t = 267 + 299\,t, t \in \mathbb{Z}$.

$[28]_{299}^{-1} = [267]_{299}$

d) Al ser $299 = 13 \cdot 23$, se tiene que $\phi(299) = \phi(13) \cdot \phi(23) = 12 \cdot 22 = 264$. Por tanto, por el Teorema de Euler, resulta $28^{264} \equiv 1\ (mod\ 299)$.

Por otra parte, $527 = 264 + 263$, y $28^{527} = 28^{264} \cdot 28^{263} \equiv 28^{263}\ (mod\ 299)$.

Además, $28 \cdot 28^{263} = 28^{264} \equiv 1\ (mod\ 299)$. Por tanto, basta multiplicar por el inverso de 28 para despejar 28^{263}. Pero en el apartado anterior ya obtuvimos este inverso. Por tanto, $28^{263} \equiv 267\ (mod\ 299)$.
Finalmente, y $28^{527} \equiv 28^{263}\ (mod\ 299) \equiv 267\ (mod\ 299)$

48. (examen enero 2012)

a) Hallar el resto de dividir 7^{11715} entre 120.
b) Hallar las soluciones enteras, no congruentes de la ecuación $75x = 6$ en Z_{24}
c) La empresa PizzaNet tiene la siguiente oferta: Las pizzas de 4 ingredientes cuestan 3 €, las pizas de 6 ingredientes cuestan 4 € y las pizas de 7 ingredientes cuestan 5 €. Tres amigos quedan para tomar pizza. Con el dinero que tienen (entre 90 y 150 €), si compraran sólo pizzas de 4 ingredientes les sobraría 1€, si compraran sólo pizzas de 6 ingredientes les sobrarían 2€, y si compraran sólo pizzas de 7 ingredientes les sobrarían 3 €. ¿Cuánto dinero tienen?

Sol.: a) Hallamos $\phi(120) = \phi(2^3 \cdot 3 \cdot 5) = \phi(2^3) \cdot \phi(3) \cdot \phi(5) = (2^3 - 2^2) \cdot 2 \cdot 4 = 32$. Por el Teorema de Euler, $7^{32} \equiv 1\ (mod\ 120)$. Dividiendo 11715 entre 32, obtenemos que $7^{11715} = (7^{32})^{366} \cdot 7^3 \equiv 7^3\ (mod\ 120) \equiv 343\ (mod\ 120) \equiv 103\ (mod\ 120)$.

b) $75x \equiv 6\ (mod\ 24)$. La ecuación tiene solución, ya que $mcd(75,24) = 3$ divide a 24. Además, sabemos que tiene 3 soluciones no congruentes en $\mathbb{Z}_{24}$.
Primeramente, podemos simplificar la ecuación dividiendo por 3.
$25x \equiv 2\ (mod\ 8)$; al resolver, nos queda la ecuación: $25x + 8y = 2$. Una posible solución, es $25(2) + 8(-3) = 2$. Por tanto, $x = 2 + 8t,\ t \in \mathbb{Z}$, por lo que las tres soluciones no congruentes módulo 24, son $\{2, 10, 18\}$.

c) Llamamos x al dinero que tienen. Obtenemos el siguiente sistema de ecuaciones en congruencias:

$$\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 2(mod\ 4) \\ x \equiv 3(mod\ 5) \end{cases}$$

Una solución particular $x = 1 \cdot (20) \cdot (20)_3^{-1} + 2 \cdot (15) \cdot (15)_4^{-1} + 3 \cdot (12) \cdot (12)_5^{-1} =$
$= 20 \cdot (-1) + 30 \cdot (-1) + 36 \cdot (3) = 58$

La solución general es $x = 58 + 60\,t,\ t \in \mathbb{Z}$. Por tanto $x = 58, 118, 178, \ldots$.

Como el dinero que tienen está entre 90 y 150, necesariamente ha de ser 118.