

**Práctico 4**  
**Matemática Discreta I – Año 2023/1**  
**FAMAF**

**Ejercicios resueltos**

- (1) a) Calcular el resto de la división de 1599 por 39 sin tener que hacer la división.

(Ayuda:  $1599 = 1600 - 1 = 40^2 - 1$ ).

*Rta:*  $1599 \equiv 1^2 - 1 \pmod{39}$ , por lo tanto el resto es 0.

- b) Lo mismo con el resto de 914 al dividirlo por 31.

*Rta:*  $914 = 30^2 + 14 \equiv (-1)^2 + 14 \pmod{31}$ , por lo tanto el resto es 15.

- (2) Sea  $n \in \mathbb{N}$ . Probar que todo número de la forma  $4^n - 1$  es divisible por 3.

*Rta:*  $4^n - 1 \equiv 1^n - 1 \equiv 0 \equiv 3 \pmod{3}$  por lo tanto  $3|4^n - 1$ .

- (3) Probar que el resto de dividir  $n^2$  por 4 es igual a 0 si  $n$  es par y 1 si  $n$  es impar.

*Rta:* Si  $n = 2k$ , se tiene  $n^2 = 4k^2$ , por lo tanto  $4|n^2$ . Si  $n = 2k + 1$ , tenemos  $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$  y vale el resultado.

- (4) a) Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.

*Rta:*

*Regla del 2.* Si  $n = \sum_{j=0}^k a_j 10^j$ ,  $n \equiv \sum_{j=1}^k a_j 0^j + a_0 \pmod{2}$  por lo tanto es divisible por 2 si y solo si su dígito de unidades lo es, o sea si termina en 0, 2, 4, 6, 8.

*Regla del 3 y 9.* Como  $10 \equiv 1 \pmod{3}$ ,  $\sum_{j=0}^k a_j 10^j \equiv \sum_{j=0}^k a_j 1^j \pmod{3}$ . Por lo tanto  $3|n$  si y sólo si 3 divide a la suma de sus dígitos. Notar que lo mismo pasa con 9 por ser  $10 \equiv 1 \pmod{9}$ .

*Regla del 4 y 8.*  $10^j \equiv 0 \pmod{4}$  si  $j > 1$  y  $10^j \equiv 0 \pmod{8}$  si  $j > 2$ . Por lo tanto, al tomar congruencia de  $n$  módulo 4 u 8, sólo quedan las dos últimas cifras en el primer caso y las 3 últimas en el segundo. Es decir  $4|n$  si y sólo si  $4|10a_1 + a_0$  y  $8|n$  si y sólo si  $8|100a_2 + 10a_1 + a_0$ .

*Regla del 11.*  $10 \equiv -1 \pmod{11} \Rightarrow n = \sum_{j=0}^k a_j 10^j \equiv \sum_{j=0}^k a_j (-1)^j$ . Entonces  $11|n$  si y sólo si 11 divide a la suma de los dígitos que están en lugar par menos la suma de los dígitos que están en lugar impar.

- b) Decir por cuáles de los números del 2 al 11 son divisibles los siguientes números:

12342

5176

314573

899.

*Rta:*  $12342 = 2 \cdot 3 \cdot 11^2 \cdot 17$ ,  $5176 = 2^3 \cdot 647$ ,  $314573 = 7 \cdot 44939$ , 899 no es divisible por ninguno de ellos.

- (5) Sean  $a, b, c$  números enteros, ninguno divisible por 3. Probar que

$$a^2 + b^2 + c^2 \equiv 0 \pmod{3}.$$

*Rta:* Si ninguno es divisible por 3 tenemos que cada uno de ellos es de la forma  $x \equiv 1 \pmod{3}$  o  $x \equiv 2 \pmod{3}$ , por lo tanto  $x^2 \equiv 1 \pmod{3}$  o  $x^2 \equiv 4 \equiv 1 \pmod{3}$ . Luego  $a^2, b^2, c^2$  son congruentes a 1 módulo 3, y en consecuencia

$$a^2 + b^2 + c^2 \equiv 1 + 1 + 1 \equiv 3 \equiv 0 \pmod{3}:$$

Por lo tanto,  $3|a^2 + b^2 + c^2$ .

- (6) Hallar la cifra de las unidades y la de las decenas del número  $7^{15}$ .

*Rta:* Para encontrar dichas cifras tenemos que tomar congruencia módulo 100.

Ahora bien,  $7^{15} = (7^2)^7 \cdot 7 = (50-1)^7 \cdot 7$  y observar que como  $50^k \equiv 0 \pmod{100}$  para  $k > 1$ , por la fórmula binomial,  $(50-1)^7 \cdot 7 \equiv (50 \cdot 7 - 1)7 \pmod{100}$ .

Finalmente

$$(50 \cdot 7 - 1)7 \equiv 350 \cdot 7 - 7 \equiv 50 \cdot 7 - 7 \equiv 350 - 7 \equiv 343 \equiv 43 \pmod{100}.$$

- (7) Hallar el resto en la división de  $x$  por 5 y por 7 para:

a)  $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$ ;

*Rta:* Sabemos que si  $(a, 5) = 1$  y por el teorema de Fermat se tiene  $a^4 \equiv 1 \pmod{5}$ , luego cada sumando salvo  $5^8$  que es congruente a 0 módulo 5. Su suma da entonces  $7 \equiv 2 \pmod{5}$ .

También sabemos que  $a^7 \equiv a \pmod{7}$ ,  $\forall a$ , por lo cual la suma es congruente a  $\sum_{i=1}^8 i^2$  módulo 8. Esto es  $1 + 4 + 2 + 2 + 4 + 1 + 0 + 1 = 15 \equiv 1 \pmod{7}$ .

b)  $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$ .

*Rta:*  $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 1 \cdot 2 \cdot 1 \cdot 1 \equiv 6 \equiv 1 \pmod{5}$

$x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 4 \cdot 3 \cdot 1 \cdot 3 \equiv 108 \equiv 1 \pmod{7}$ .

- (8) Hallar todos los  $x$  que satisfacen:

a)  $x^2 \equiv 1 \pmod{4}$

*Rta:* Resolvemos primero para  $0 \leq x \leq 3$  y luego sumamos un múltiplo de 4. Esto es  $x = 1$  o  $x = 3$  y por lo tanto  $x = 1 + 4k$  o  $x = 3 + 4k$ , lo cual también se puede escribir como  $x = 4k \pm 1$ .

b)  $x^2 \equiv x \pmod{12}$

*Rta:* Soluciones menores que 12:  $x = 0, 1, 4, 9, 11$ . Luego el conjunto solución es  $\{12k, 12k \pm 1, 12k + 4, 12k - 3\}$ .

c)  $x^2 \equiv 2 \pmod{3}$

*Rta:* No tiene soluciones pues  $0^2 = 0, 1^2 = 1, 2^2 \equiv 1 \pmod{3}$ .

d)  $x^2 \equiv 0 \pmod{12}$

*Rta:* Soluciones menores que 12:  $\{0, 6\}$ . Luego las soluciones son  $\{12k, 12k + 6\}$ .

e)  $x^4 \equiv 1 \pmod{16}$

*Rta:* Notemos que  $x$  debe ser impar. Podemos tomar  $-8 \leq x \leq 8$ , es decir  $x \in \{-7, -5, -3, -1, 1, 3, 5, 7\}$ . Los cuadrados son  $\{49, 25, 9, 1, 1, 9, 25, 49\}$  que son congruentes módulo 16 a  $\{1, 9, 9, 1, 1, 9, 9, 1\}$ . A su vez cuando elevamos estos al cuadrado, como  $9^2 = 81 \equiv 1 \pmod{16}$  Tenemos que todo número impar es solución de la ecuación.

Alternativamente podríamos elevar  $2k + 1$  a la cuarta con la fórmula binomial  $\sum_{j=0}^4 \binom{4}{j} (2k)^j 1^{4-j} = 1 + 4 \cdot 2k + 6 \cdot 4k^2 + 4 \cdot 4k^3 + 16k^4 = 1 + 8(k + 3k^2) + 16(k^3 + k^4) \equiv 1 + 8(k + 3k^2) \pmod{16}$ . Si observamos que  $k(1 + 3k)$  siempre es par ya que es uno de los factores es par, tenemos que  $(2k + 1)^4 \equiv 1 + 16(3k + 1)k/2 \equiv 1 \pmod{16}$ .

f)  $3x \equiv 1 \pmod{5}$

*Rta:* Probamos con  $x = 0, 1, 2, 3, 4$  y vemos que  $3 \cdot 2 = 6 \equiv 1 \pmod{5}$ . Luego las soluciones son  $x = 5k + 2$ .

- (9) Sean  $a, b, m \in \mathbb{Z}$ ,  $d > 0$  tales que  $d \mid a$ ,  $d \mid b$  y  $d \mid m$ . Probar que la ecuación  $a \cdot x \equiv b \pmod{m}$  tiene solución si y sólo si la ecuación

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

tiene solución.

*Rta:* La ecuación  $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$  tiene solución si y sólo si  $\frac{m}{d} \mid \frac{a}{d} \cdot x - \frac{b}{d}$  si y sólo si  $\frac{a}{d} \cdot x - \frac{b}{d} = \frac{m}{d}q$  como  $d \neq 0$  multiplicando por  $d$ , esto ocurre si y sólo si  $m \mid a \cdot x - b$ , es decir,  $a \cdot x \equiv b \pmod{m}$ .

- (10) Resolver las siguientes ecuaciones:

a)  $2x \equiv -21 \pmod{8}$

Como el módulo es par, no hay solución pues el miembro de la derecha es par y el de la izquierda es impar.

b)  $2x \equiv -12 \pmod{7}$

*Rta:*  $-12 \equiv 2 \pmod{7}$ , por lo tanto la ecuación es equivalente a  $2x \equiv 2 \pmod{7}$ . Evidentemente 1 es solución de la ecuación y como  $1 = (2, 7)$  todas las soluciones son de la forma  $x = 1 + 7k, k \in \mathbb{Z}$ .

c)  $3x \equiv 5 \pmod{4}$ .

*Rta:*  $5 \equiv 1 \pmod{4}$ , por lo tanto la ecuación es equivalente a  $3x \equiv 1 \pmod{4}$ . Probando se encuentra que 3 es solución y como  $1 = (4, 3)$ , todas las soluciones son de la forma  $x = 3 + 4k, k \in \mathbb{Z}$ .

- (11) Resolver la ecuación  $221x \equiv 85 \pmod{340}$ . Hallar todas las soluciones  $x$  tales que  $0 \leq x < 340$ .

*Rta:* Notemos que 221, 85 y 340 son divisibles por 17. Sus respectivos cocientes son 13, 5 y 20. Por el ejercicio 9 podemos entonces resolver  $13x \equiv 5 \pmod{20}$ . Las soluciones de esta ecuación deben ser múltiplos de

5 y menores que 20. Comprobamos que 5 es la única solución menor que 20. las restantes son de la forma  $20k + 5$ . Tenemos que el conjunto buscado es:  $\{5, 25, 45, \dots, 305, 325\} = \{5 + 20k, \}_{k=1}^{20}$ .

- (12) a) Encontrar todas las soluciones de la ecuación en congruencia

$$36x \equiv 8 \pmod{20}$$

usando el método visto en clase.

*Rta:*

$$36 = 20 \times 1 + 16 \Rightarrow 16 = 36 - 20$$

$$20 = 16 \times 1 + 4 \Rightarrow 4 = 20 - 16$$

$$16 = 4 \times 4 + 0.$$

Luego  $4 = (36, 20)$ . Como  $4|8$  la ecuación tiene solución. Ahora bien,

$$4 = 20 - 16 = 20 - (36 - 20) = (-1) \cdot 36 + 2 \cdot 20,$$

por lo tanto, multiplicando por 2 la ecuación, tenemos que  $8 = (-2) \cdot 36 + 4 \cdot 20$ . Luego,

$$8 \equiv (-2) \cdot 36 \pmod{20},$$

y entonces  $-2$  es solución y todas la soluciones son de la forma  $x = -2 + (20/4)k = -2 + 5k$ , con  $k$  entero.

- b) Dar todas las soluciones  $x$  de la ecuación anterior tales que  $-8 < x < 30$ .

*Rta:* Como todas las soluciones son de la forma  $x = -2 + 5k$ , con  $k$  entero, tomamos valores consecutivos de  $k$  y observamos cuando  $x = -2 + 5k$  se encuentra en el rango  $-8 < x < 30$ . Si empezamos por  $k = -3$ , la solución es  $x = -17$  y las soluciones para ese  $k$  y los siguientes son

$$-17, -12, -7, -2, 3, 8, 13, 18, 23, 28, 33$$

Por lo tanto la respuesta es  $-7, -2, 3, 8, 13, 18, 23, 28$ .

*Rta:* (alternativa) Si queremos ser más sistemáticos planteamos las inequaciones  $-8 < -2 + 5k < 30$ . Sumando 2 y dividiendo por 5 en las inequaciones, obtenemos  $-6/5 < k < 32/5$  o equivalentemente  $-1.2 < k < 6.4$ , es decir que  $k$  debe tomar los valores  $-1, 0, 1, 2, 3, 4, 5, 6$  y por lo tanto  $x = -2 + 5k$  toma valores  $-7, -2, 3, 8, 13, 18, 23, 28$ .

- (13) a) Encontrar todas las soluciones de la ecuación en congruencia

$$21x \equiv 6 \pmod{30}$$

usando el método visto en clase.

*Rta:*  $3 = (21, 30)$  y  $3 = (-7) \cdot 21 + 5 \cdot 30$ , por lo tanto  $6 = (-14) \cdot 21 + 10 \cdot 30$ . Haciendo congruencia módulo 30 obtenemos:  $6 \equiv (-14) \cdot 21 \equiv 6 \cdot 21 \pmod{30}$ . Luego la ecuación tiene como soluciones  $x = 6 + (30/10)k = 6 + 3k$ , con  $k$  entero.

- b) Dar todas las soluciones  $x$  de la ecuación anterior tales que  $0 < x < 35$ .

*Rta:* En base al punto anterior,  $0 < x < 35$ , es equivalente a  $0 < 6 + 10k < 35$ . Restando 6 y luego dividiendo por 10 las inecuaciones, obtenemos  $-6/10 < k < 29/10$  o bien  $-0.6 < k < 2.9$ , por lo tanto  $k$  toma valores 0, 1, 2 y las soluciones son 6, 16, 26.

(14) Encontrar todas las soluciones de los siguientes sistemas de ecuaciones en congruencia

a) 
$$\begin{aligned} 4x &\equiv 7 \pmod{11} \\ 7x &\equiv 8 \pmod{12} \end{aligned}$$

*Rta:* Para resolver la ecuación  $4x \equiv 7 \pmod{11}$  observemos que  $-1$  es solución. Como  $1 = (4, 11)$  todas las soluciones de  $4x \equiv 7 \pmod{11}$  son de la forma  $x = -1 + 11k$ , para  $k$  entero. Ahora, debemos encontrar los  $k \in \mathbb{Z}$  soluciones de la ecuación

$$7(-1 + 11k) \equiv 8 \pmod{12}.$$

Expandiendo el lado izquierdo de la ecuación obtenemos

$$7 \times (-1) + 7 \times 11k \equiv -7 + 77k \equiv 5 + 5k \pmod{12}.$$

Luego, debemos resolver  $5 + 5k \equiv 8 \pmod{12}$  o equivalentemente,  $5k \equiv 3 \pmod{12}$ . Una solución a esta ecuación es 3. Como  $1 = (5, 12)$ , todas las soluciones son de la forma  $k = 3 + 12h$  con  $h \in \mathbb{Z}$ .

La solución al sistema entonces será  $x = -1 + 11k = -1 + 11(3 + 12h)$ . Es decir  $x = 32 + 132h$  para  $h \in \mathbb{Z}$ .

b) 
$$\begin{aligned} x &\equiv -1 \pmod{7} \\ x &\equiv 3 \pmod{10} \\ x &\equiv -2 \pmod{11}. \end{aligned}$$

*Rta:* Las soluciones de la primera ecuación son  $x = -1 + 7k$  para  $k \in \mathbb{Z}$ . Especializando estas soluciones en la segunda ecuación obtenemos  $-1 + 7k \equiv 3 \pmod{10}$ , lo que es equivalente a  $7k \equiv 4 \pmod{10}$ , cuyas soluciones son  $k = 2 + 10h$  para  $h \in \mathbb{Z}$ . Luego las soluciones para el sistema que forman las dos primeras ecuaciones son  $x = -1 + 7k = -1 + 7(2 + 10h) = 13 + 70h$  para  $h \in \mathbb{Z}$ .

Finalmente, especificando estas soluciones en la tercera ecuación obtenemos  $13 + 70h \equiv -2 \pmod{11}$  o equivalentemente  $70h \equiv -15 \pmod{11}$  o bien  $4h \equiv 7 \pmod{11}$ , cuyas soluciones son  $h = -1 + 11t$  para  $t \in \mathbb{Z}$ . Luego,  $x = 13 + 70h = 13 + 70(-1 + 11t) = -57 + 770t$ .

Concluyendo: las soluciones del sistema son  $x = -57 + 770t$  para  $t \in \mathbb{Z}$ .

c) 
$$\begin{aligned} x &\equiv -1 \pmod{2} \\ x &\equiv 5 \pmod{9} \\ x &\equiv -3 \pmod{7}. \end{aligned}$$

*Rta:* Las soluciones de la primera ecuación son  $x = 1 + 2k$  para  $k \in \mathbb{Z}$ . Especializando estas soluciones en la segunda ecuación obtenemos  $1 + 2k \equiv 5 \pmod{9}$ , lo que es equivalente a  $2k \equiv 4 \pmod{9}$ , cuyas soluciones son  $k = 2 + 9h$  para  $h \in \mathbb{Z}$ . Luego las soluciones para el sistema que

forman las dos primeras ecuaciones son  $x = 1 + 2k = 1 + 2(2 + 9h) = 5 + 18h$  para  $h \in \mathbb{Z}$ .

Finalmente, especificando estas soluciones en la tercera ecuación obtenemos  $5 + 18h \equiv -3 \pmod{7}$  o equivalentemente  $18h \equiv -8 \pmod{7}$  o bien  $4h \equiv 6 \pmod{7}$ , cuyas soluciones son  $h = 5 + 7t$  para  $t \in \mathbb{Z}$ . Luego,  $x = 5 + 18h = 5 + 18(5 + 7t) = 95 + 126t$ .

Concluyendo: las soluciones del sistema son  $x = 95 + 126t$  para  $t \in \mathbb{Z}$ .

- (15) Dado  $t \in \mathbb{Z}$ , decimos que  $t$  es *invertible módulo  $m$*  si existe  $h \in \mathbb{Z}$  tal que  $th \equiv 1 \pmod{m}$ .

a) ¿Es 5 invertible módulo 17?

Rta: Si,  $5 \cdot 7 \equiv 1 \pmod{17}$

b) Probar que  $t$  es invertible módulo  $m$ , si y sólo si  $(t, m) = 1$ .

Rta: Si  $t$  es invertible módulo  $m$  sea  $h$  tal que  $th \equiv 1 \pmod{m}$ . Esto es  $th - 1 = mq$ , y por lo tanto  $1 = th - mq$ , lo cual dice que  $(t, m) = 1$ . Recíprocamente si  $(t, m) = 1$  existen enteros  $h$  y  $q$  tales que  $1 = th + mq$  y esto nos dice que  $m$  divide a  $1 - th$  o sea  $th \equiv 1 \pmod{m}$ .

c) Determinar los invertibles módulo  $m$ , para  $m = 11, 12, 16$ .

Rta:  $\{1, 2, 3, \dots, 9, 10\}, \{1, 5, 7, 11\}, \{1, 3, 5, 7, 9, 11, 13, 15\}$ .

- (16) Encontrar los enteros cuyos cuadrados divididos por 19 dan resto 9.

Rta: Si resolvemos  $x^2 \equiv 9 \pmod{19}$  vemos que 3 y 16 son los únicos restos que son solución. Luego, todas las soluciones buscadas son  $19k \pm 3$ .

- (17) Probar que todo número impar  $a$  satisface:  $a^4 \equiv 1 \pmod{16}$ ,  $a^8 \equiv 1 \pmod{32}$ ,  $a^{16} \equiv 1 \pmod{64}$ .

¿Se puede asegurar que  $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ ?

Rta: Si  $n = 1$ ,  $a^2 - 1$  es divisible por 8 ya que  $a^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1)$  y  $2|k(k + 1)$ .

Si  $a^{2^n} \equiv 1 \pmod{2^{n+2}}$  entonces  $2^{n+2}$  divide a  $a^{2^n} - 1$  multiplicando por  $a^{2^n} + 1$ , que es par, tenemos que  $2^{n+1+2}$  divide a  $(a^{2^n} - 1)(a^{2^n} + 1) = a^{2^{n+1}} - 1$ .

- (18) Encontrar el resto en la división de  $a$  por  $b$  en los siguientes casos:

a)  $a = 11^{13} \cdot 13^8$ ;  $b = 12$ ; Rta:  $11^{13} \cdot 13^8 \equiv (-1)^{13} \cdot 1^8 \equiv -1 \pmod{12}$ .

b)  $a = 4^{1000}$ ;  $b = 7$ ; Rta:  $4^{1000} = (4^6)^{166} 4^4 \equiv (4^2)^2 \equiv 2^2 \pmod{7}$ .

c)  $a = 123^{456}$ ;  $b = 31$ ; Rta:  $123^{456} \equiv (-1)^{456} \equiv 1 \pmod{31}$ .

d)  $a = 7^{83}$ ;  $b = 10$ . Rta:  $7^{83} = (7^4)^{20} 7^3 \equiv 1^{20} 3^3 \equiv 3 \pmod{10}$ .

- (19) Obtener el resto en la división de  $2^{21}$  por 13; de  $3^8$  por 5 y de  $8^{25}$  por 127.

*Rta:*  $2^{21} = 2^{13}2^8 \equiv 2 \cdot 2^8 \pmod{13}$  Como  $2^32^9 = 2^{12} \equiv 1 \pmod{13}$ , se tiene  $82^9 \equiv 1 \pmod{13}$  y esto dice que  $2^9 \equiv 5 \pmod{13}$  ya que  $8 \cdot 5 = 3 \cdot 13 + 1$ .

$$3^8 = 3^4 \cdot 3^4 \equiv 1 \cdot 1 \pmod{13}.$$

$8^{25} = 2^{75}$  como  $2^7 = 128 \equiv 1 \pmod{127}$ ; tenemos que  $2^{75} = (2^7)^{10}2^5 \equiv 2^5 \pmod{127}$ . Por lo tanto  $8^{25} \equiv 32 \pmod{127}$

- (20) a) Probar que no existen enteros no nulos tales que  $x^2 + y^2 = 3z^2$ .

*Rta:* Si  $x, y, z$  fuesen solución y tuvieran un factor común  $t$  es claro que también  $x/t, y/t, z/t$  cumpliría las condiciones. Luego podemos asumir que  $x, y, z$  no tienen factor en común salvo  $\pm 1$ .

Ahora bien,  $0^2 \equiv 0 \pmod{3}$ ,  $1^2 \equiv 1 \pmod{3}$  y  $2^2 \equiv 1 \pmod{3}$ . Por lo tanto, si tomamos congruencia módulo 3 en ambos miembros vemos que la suma de dos cuadrados módulo 3 sólo puede ser 0 si ambos números son divisibles por 3. Luego  $x = 3a, y = 3b$ , y por lo tanto  $x^2 = 9a^2, y^2 = 9b^2$ . Podemos simplificar la ecuación y obtenemos  $3a^2 + 3b^2 = z^2$ . Tomando congruencia módulo 3 nuevamente tenemos que 3 divide a  $z^2$  y por lo tanto divide a  $z$ . Esto contradice el hecho que  $x, y, z$  no tenían factor común.

- b) Probar que no existen números racionales no nulos  $a, b, r$  tales que  $3(a^2 + b^2) = 7r^2$ .

*Rta:* Aquí también podemos asumir que  $a, b, r$  no tienen factores en común. Tomando congruencia módulo 3 vemos que 3 divide a  $r$  o sea  $r = 3t, r^2 = 9t^2$ . Reemplazando y simplificando tenemos  $a^2 + b^2 = 3t^2$ , que sabemos por el inciso anterior que no tiene solución.

- (21) Probar que si  $(a, 1001) = 1$  entonces 1001 divide a  $a^{720} - 1$ .

*Rta:* Notemos que  $1001 = 7 \cdot 11 \cdot 13$ . Por lo tanto  $(a, 1001) = 1$  implica  $(a, 7) = (a, 11) = (a, 13) = 1$ . Entonces  $a^6 \equiv 1 \pmod{7}$ ;  $a^{10} \equiv 1 \pmod{11}$  y  $a^{12} \equiv 1 \pmod{13}$ . Por lo tanto  $a^{720} = ((a^6)^{10})^{12} \equiv 1 \pmod{7 \cdot 11 \cdot 13}$ .

- (22) Sea  $p$  primo impar.

- a) Probar que las únicas raíces cuadradas de 1 módulo  $p$ , son 1 y  $-1$  módulo  $p$ . Es decir, probar que  $x^2 \equiv 1 \pmod{p}$ , entonces  $x \equiv \pm 1 \pmod{p}$ .

*Rta:*  $x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 \equiv 0 \pmod{p}$ , como  $x^2 - 1 = (x - 1)(x + 1)$ , obtenemos  $(x - 1)(x + 1) \equiv 0 \pmod{p}$ . Esto quiere decir que  $p \mid (x - 1)(x + 1)$ . Como  $p$  es primo,  $p \mid x - 1$  o  $p \mid x + 1$ , es decir

$$\begin{aligned} x - 1 \equiv 0 \pmod{p} \quad \vee \quad x + 1 \equiv 0 \pmod{p} & \Leftrightarrow \\ x \equiv 1 \pmod{p} \quad \vee \quad x \equiv -1 \pmod{p}. \end{aligned}$$

- b) Probar que  $p = 2^s \cdot d + 1$  con  $d$  impar.

*Rta:* Como  $p$  es impar  $p - 1$  es par, por la descomposición única en factores primos tenemos que  $p - 1 = 2^s \cdot d$  con  $d$  impar. Luego  $p = 2^s \cdot d + 1$ .

- c) Probar que  $a^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{p}$ .

*Rta:* Por el teorema de Fermat,  $a^{2^s \cdot d} = a^{n-1} \equiv 1 \pmod{n}$ . Luego  $(a^{2^{s-1} \cdot d})^2 \equiv 1 \pmod{n}$  y por lo tanto  $a^{2^{s-1} \cdot d}$  es una raíz cuadrada de 1 módulo  $n$ . Por el lema anterior obtenemos que  $a^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{n}$ .

d) Sea  $p = d \cdot 2^s + 1$  donde  $d$  es impar. Dado  $a$  entero tal que  $0 < a < p$ , probar que

◦  $a^d \equiv 1 \pmod{p}$ , o

◦  $a^{2^r \cdot d} \equiv -1 \pmod{p}$  para algún  $r$  tal que  $0 \leq r < s$ .

*Rta:* Consideremos la sucesión  $a^{2^s \cdot d}, a^{2^{s-1} \cdot d}, \dots, a^{2^2 \cdot d}, a^d$ . La demostración la haremos usando el teorema de Fermat, los resultados anteriores y observando que cada término de la sucesión es el cuadrado del siguiente.

◦ Por c),  $a^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{p}$ .

◦ Si  $a^{2^{s-1} \cdot d} \equiv -1 \pmod{p}$ , listo, en caso contrario  $a^{2^{s-1} \cdot d} \equiv 1 \pmod{p}$ , luego  $(a^{2^{s-2} \cdot d})^2 \equiv 1 \pmod{p}$  y por lo tanto  $a^{2^{s-2} \cdot d}$  es una raíz cuadrada de 1 módulo  $p$ . Luego por a) tenemos que  $a^{2^{s-2} \cdot d} \equiv \pm 1 \pmod{p}$ .

◦ Iterando el razonamiento anterior concluimos que alguno de los términos de la sucesión  $a^{2^r \cdot d}$  es congruente a  $-1$  módulo  $p$  o bien todos los términos son congruentes a 1, en particular  $a^d \equiv 1 \pmod{p}$ .

**§ Ejercicios de repaso.** Los ejercicios marcados con (\*) son de mayor dificultad.

(23) Dada la ecuación de congruencia

$$14x \equiv 10 \pmod{26},$$

hallar todas las soluciones en el intervalo  $[-20, 10]$ . Hacerlo con el método usado en la teórica.

(24) Dada la ecuación de congruencia

$$21x \equiv 15 \pmod{39},$$

hallar todas las soluciones en el intervalo  $[-10, 30]$ . Hacerlo con el método usado en la teórica.

(25) Hallar todos los enteros que satisfacen simultáneamente:

$$x \equiv 1 \pmod{3}; \quad x \equiv 1 \pmod{5}; \quad x \equiv 1 \pmod{7}.$$

(26) (\*) ¿Para qué valores de  $n$  es  $10^n - 1$  divisible por 11?

*Rta:* Como  $10 \equiv -1 \pmod{11}$ , se tiene  $10^n - 1 \equiv (-1)^n - 1 \pmod{11}$ . Entonces  $10^n - 1$  es divisible por 11 si y solo si  $n$  es par.



- (27) (\*) Probar que para ningún  $n \in \mathbb{N}$  se puede partir el conjunto  $\{n, n+1, \dots, n+5\}$  en dos partes disjuntas no vacías tales que los productos de los elementos que las integran sean iguales.

*Rta:* Notemos que si fuera posible dicha partición. el  $n+2$  dividiría a ambos productos y uno de ellos no lo contiene. Entonces  $n+2$  debe dividir a  $(n+2-2)(n+2-1)(n+2+1)(n+2+2)(n+2+3)$ . Esto nos dice que  $n+2$  debe dividir a  $(-1)(-2) \cdot 1 \cdot 2 \cdot 3 = 12$ . Las posibilidades para  $n+2$  son entonces: 1, 2, 3, 4, 6, 12. Pero 1 y 2 dan  $n \leq 0$  y las restantes dan  $n \in \{1, 2, 4, 10\}$ . La primera no puede ser pues en el conjunto  $\{1, 2, 3, 4, 5, 6\}$  hay un único elemento divisible por 5, que debería ser divisor de ambos productos de la partición. La misma razón dice que  $n$  no puede ser 2 ni 4. Finalmente si  $n = 10$ , el conjunto sería  $\{10, 11, 12, 13, 14, 15\}$  que posee un único elemento divisible por 7 (el 14) y vale el mismo razonamiento que antes con 7 en lugar de 5.

Alternativamente: Notemos que 7 divide a lo sumo a uno de los 6 números. Si  $\prod_{i=0}^5 (n+i) = u_1 u_2$  con  $u_1 = u_2$ , entonces 7 no divide a ninguno de los factores ya que si divide a un factor de  $u_1$  divide a un factor de  $u_2$ . Tenemos así que las congruencias módulo 7 dan los 6 restos posibles y su producto 720 es congruente a 6 módulo 7. Pero entonces  $u_1^2 = u_1 u_2 \equiv 720 \equiv 6 \pmod{7}$  se tendría que 6 es un cuadrado módulo 7 lo cual es falso.

- (28) (\*) El número  $2^{29}$  tiene nueve dígitos y todos son distintos. ¿Cuál dígito falta? (No está permitido el uso de calculadora).

*Rta:* Primero nos planteamos la siguiente pregunta, ¿Cuánto suman sus dígitos? Si  $2^{29} = \sum_{i=0}^8 a_i 10^i$ , entonces  $\sum_{i=0}^8 a_i = \sum_{i=0}^9 i - d$ , donde  $d$  es el dígito que falta. Esto es  $\sum_{i=0}^8 a_i = 45 - d$ . Además  $2^{29} = \sum_{i=0}^8 a_i 10^i \equiv \sum_{i=0}^8 a_i \pmod{9}$ . Entonces si calculamos esta congruencia podemos obtener  $d$ :  $2^{29} = (2^6)^4 2^5 \equiv 2^5 \pmod{9}$  y  $2^5 \equiv 5 \pmod{9}$  por lo tanto  $d \equiv -5 \pmod{9}$  o sea  $d = 4$  es el dígito faltante.

- (29) (\*) Cinco hombres recogieron en una isla un cierto número de cocos y resolvieron repartirlos al día siguiente. Durante la noche uno de ellos decidió separar su parte y para ello dividió el total en cinco partes y dió un coco que sobraba a un mono y se fue a dormir. Enseguida otro de los hombres hizo lo mismo, dividiendo lo que había quedado por cinco, dando un coco que sobraba a un mono y retirando su parte, se fue a dormir. Uno tras otro los tres restantes hicieron lo mismo, dándole a un mono el coco que sobraba. A la mañana siguiente repartieron los cocos restantes, dándole a un mono el coco sobrante. ¿Cuál es el número mínimo de cocos que se recogieron?

*Rta:*

- (30) (\*) La producción diaria de huevos en una granja es inferior a 75. Cierta día el recolector informó que la cantidad de huevos recogida era tal que contando

de a 3 sobraban 2, contando de a 5 sobraban 4 y contando de a 7 sobraban 5. El capataz, dijo que eso era imposible. ¿Quién tenía razón? Justificar.

*Rta:*