TEMA 3

Aritmética

Ejercicio 1. Encuentra los sistemas o bases de numeración, si existe alguno, para los que se verifica cada una de las siguientes igualdades:

1. $3 \times 4 = 22$,
2. $41 \times 14 = 1224$,
3. $52 \times 25 = 1693$,
4. $25 \times 13 = 51$,
5. $13^4 = 14641$

Ejercicio 2. Da la expresión en bases 4, 8 y 16 de los naturales que en base 2 se escriben:

1. 10110110001001101011,
2. 10001000000100110,
3. 1011101111011111

Ejercicio 3. Sean $x = 48572)_{16}$ e $y = 95883)_{16}$. Expresa el valor de $x + y$ en base 8.

Ejercicio 4. Un número escrito en base b tiene 64 cifras. ¿Cuántas cifras tiene el mismo número expresado en base b^3?.

Ejercicio 5. Dado un número natural $n \geq 10$, definimos el número natural $P(n)$ como el número que resulta de colocar la cifra de las unidades a la izquierda (por ejemplo, si $n = 3148$ entonces $P(n) = 8314$). Calcula un número n que termine en 6 y que verifique que $4n = P(n)$.

Ejercicio 6. Enumera los divisores positivos de 120, y calcula cuántos divisores tiene el número 118800.

Ejercicio 7. Determina la factorización como producto de números primos de $10!$ y $15!$. ¿Cuántos divisores tiene cada uno de ellos?

Ejercicio 8. Encuentra el valor máximo de n tal que 2^n divide a $25!$.

Ejercicio 9. ¿Cuántos ceros tiene al final el número $100!$?.

Ejercicio 10. Encuentra todas las soluciones enteras de $x^2 - y^2 = 32$.

Ejercicio 11. Encuentra todas las parejas de números a, b tales que $\mathrm{mcd}(a, b) = 210$ y $\mathrm{mcm}(a, b) = 840$.

Ejercicio 12. Sean $a, b \in \mathbb{N}$ tal que b es divisor de a y $a + 2$. Demuestra que $b = 1$ ó $b = 2$.

Ejercicio 13. Sean $a, b \in \mathbb{Z}$ primos relativos. Demuestra que si $a|c$ y $b|c$ entonces $ab|c$. Estudia que pasa si $\mathrm{mcd}(a, b) \neq 1$.

Ejercicio 14. Dado un número entero n, demuestra que $mcd(8n+3, 5n+2) = 1$.

Ejercicio 15. Sea $a \in \mathbb{Z}$. Demuestra que el máximo común divisor de $35a+57$ y $45a+76$ vale 1 ó 19. ¿Para que valores de a es este máximo común divisor igual a 19?.

Ejercicio 16. Demuestra que si p es un número primo, entonces $\sqrt{p}$ es un número irracional. Concluye que $\sqrt{75}$ es irracional.

Ejercicio 17. Estudia si las siguientes afirmaciones son verdaderas o falsas. En ellas, a y b denotan un número entero cualquiera, y p un número primo. Razona la respuesta.

1. Si $\mathrm{mcd}(a, p^2) = p$ entonces $\mathrm{mcd}(a^2, p^2) = p^2$.
2. Si $\mathrm{mcd}(a, p^2) = p$ y $\mathrm{mcd}(b, p^2) = p^2$ entonces $\mathrm{mcd}(ab, p^4) = p^4$.
3. Si $\mathrm{mcd}(a, p^2) = p$ y $\mathrm{mcd}(b, p^2) = p$ entonces $\mathrm{mcd}(ab, p^4) = p^2$.
4. Si $\mathrm{mcd}(a, p^2) = p$ entonces $\mathrm{mcd}(a+p, p^2) = p$.

Ejercicio 18. En $\mathbb{Z}_{300}$ realiza, si es posible, los siguientes cálculos:

- $25 \cdot 60$.
- $127 \cdot (-100)$.
- 237^{-1}.
- $13 - 50 \cdot 101^{-1}$.
- Encuentra $x \neq 0$ tal que $111 \cdot x = 0$.
- Encuentra x tal que $13x + 25 = 32x - 50$.
- Encuentra x tal que $11x - 100 = 45x + 12$.

Ejercicio 19. Calcula, si es posible, 1392^{-1} en $\mathbb{Z}_{7585}$.

Ejercicio 20. Calcula el resto de dividir 4225^{1850} entre 1234.

Ejercicio 21. Demuestra que:

1. Un número escrito en base 10 es par si, y sólo si, su última cifra es par.
2. Un número escrito en base 10 es un múltiplo de 3 si, y sólo si, la suma de sus cifras es un múltiplo de 3.
3. Un número escrito en base 10 es múltiplo de 4 si, y sólo si, su última cifra más dos veces la penúltima es múltiplo de 4.
4. Un número escrito en base 10 es un múltiplo de 9 si, y sólo si, la suma de sus cifras es un múltiplo de 9.
5. Un número escrito en base 10 es un múltiplo de 5 si acaba en 0 o en 5.
6. Si $a_n a_{n-1} \cdots a_2 a_1 a_0$ es la expresión decimal de un número x, entonces x es múltiplo de 7 si, y sólo si, el número $y = a_n a_{n-1} \cdots a_2 a_1 - 2 \cdot a_0$ es múltiplo de 7 (es decir, x es múltiplo de 7 si, y sólo si, $(x \text{ quo } 10) - 2 \cdot (x \text{ mód } 10)$ es múltiplo de 7). Comprueba que $x \equiv 3y \pmod{7}$.
7. Un número escrito en hexadecimal es múltiplo de 4 si, y sólo si, termina en 0, 4, 8 ó C.

8. Un número escrito en base 10 es múltiplo de 11 si, y sólo si, la suma de las cifras que ocupan un lugar par menos la suma de las cifras que ocupan posiciones impares es un múltiplo de 11.

9. Un número escrito en base 8 es un múltiplo de 7 si, y sólo si, la suma de sus cifras es un múltiplo de 7.

Ejercicio 22. Un número entero m se dice que está escrito en *forma ternaria equilibrada* si lo tenemos expresado como

$$m = e_n \cdot 3^n + e_{n-1} \cdot 3^{n-1} + \cdots + e_1 \cdot 3 + e_0$$

donde e_i vale -1, 0 ó 1.

1. Calcula una expresión ternaria equilibrada de los números 5, -12, 35, 121, 123456.

2. Demuestra que todo número entero distinto de cero admite una única expresión ternaria equilibrada en la que $e_n \neq 0$.

Ejercicio 23. Sin realizar el cálculo, halla las cifras que faltan en los siguientes números:

1. $2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 = 61 - 4 - 0$

2. $2^5 \cdot 3^3 \cdot 5^3 \cdot 7^3 \cdot 11 = -07 - 84 - 00$

3. $17! = 35 - 6874 - 8096000$

Ejercicio 24. Prueba que dado un número entero cualquiera m se verifica una de las siguientes posibilidades:

1. $m^2 \equiv 0 \pmod{8}$,

2. $m^2 \equiv 1 \pmod{8}$,

3. $m^2 \equiv 4 \pmod{8}$

Concluye que si m es impar, entonces $m^2 - 1$ es múltiplo de 8.

Ejercicio 25. Calcula los números que hay entre 20000 y 30000 que terminen en 39, al escribirlos en base 4 terminan en 33, y al escribirlos en base 8 acaban en 37.

Ejercicio 26. Resuelve las siguientes congruencias:

1. $3x \equiv 2 \pmod{5}$,

2. $17x \equiv 45 \pmod{92}$,

3. $3276x \equiv 1239 \pmod{531}$.

Ejercicio 27. Resuelve los siguientes sistemas de ecuaciones en congruencias:

1. $$\left\{\begin{array}{rl} x \equiv 1 & \pmod{2} \\ 6x \equiv 3 & \pmod{9} \\ 3x \equiv 3 & \pmod{5} \end{array}\right.$$

2. $$\left\{\begin{array}{rl} x \equiv 123 & \pmod{371} \\ x \equiv 331 & \pmod{644} \end{array}\right.$$

3. $$\left\{\begin{array}{rl} 28x \equiv 59 & \pmod{69} \\ 62x \equiv 26 & \pmod{74} \\ 57x \equiv 1 & \pmod{92} \end{array}\right.$$

Ejercicio 28. Resuelve la congruencia $1211^{399}n \equiv 20 \pmod{17}$.

Ejercicio 29. Resuelve el siguiente sistema de congruencias:

$$\left\{\begin{array}{rcll} 17834x & \equiv & 1870 & (\text{mód } 21989) \\ 89710x & \equiv & 10489 & (\text{mód } 8147) \\ 10022x & \equiv & 81984 & (\text{mód } 20984) \\ 20987x & \equiv & 10002 & (\text{mód } 11090) \\ 4094x & \equiv & n & (\text{mód } 56271) \end{array}\right.$$

Donde n es el número formado por las cinco últimas cifras de tu DNI (es decir, si D es tu DNI, entonces $n = D$ mód 100000).

Ejercicio 30. Determina el número de enteros entre 1500 y 2500 tales que

(a) sus dos últimas cifras en base dos son 11,

(b) sus dos últimas cifras en base tres son 00 y

(c) sus dos últimas cifras en base cinco son 12.

Ejercicio 31. ¿Cuántos números hay entre 60000 y 90000 que terminen en 45, y que su triple dé resto 97 al dividirlos por 122?

Ejercicio 32. Dado un número natural n, denotaremos por $S(n)$ a la suma de sus cifras.

1. Demuestra que para cualquier n se tiene que $n \equiv S(n)$ (mód 9).
2. Calcula los divisores de 2010.
3. Enuentra todos los números naturales para los que $n(S(n) - 1) = 2010$.

Ejercicio 33. Calcula las soluciones enteras de cada una de las siguientes ecuaciones diofánticas:

1. $2x + 3y = 7$.
2. $6x + 10y = 16$.
3. $232x - 341y = 17$.

Ejercicio 34. ¿Cuántas soluciones tiene la ecuación diofántica

$$210x - 91y = 77$$

que verifiquen que $-500 \leq x, y \leq 500$?

Ejercicio 35. Calcula 5 soluciones enteras de la ecuación

$$3761373923x + 472926384y = 382734927$$

Ejercicio 36.
1. Calcula una solución entera de la ecuación

$$79257x + 78610y = 1$$

2. Encuentra el inverso (para el producto) de 79257 en $\mathbb{Z}_{78610}$.
3. Encuentra 78610^{-1} en $\mathbb{Z}_{79257}$.
4. Calcula todas las soluciones de la ecuación

$$79257x + 78610y = 10$$

Ejercicio 37. Calcula todas las soluciones en $\mathbb{Z}$ de las ecuaciones:

1. $6x + 9y + 15z = 7$.
2. $6x + 10y + 15z = 7$.
3. $35x + 45y + 55z = 60$.

Ejercicio 38. Encuentra $a, b, c \in \mathbb{Z}$ tales que 31 sea múltiplo de $5a + 7b + 11c$. Demuestra que si x, y, z son números enteros tales que $5x + 7y + 11z$ es múltiplo de 31, también lo son $21x + 17y + 9z$ y $6x + 27y + 7z$.

Ejercicio 39. Calcula el cociente y el resto de dividir $2x^4 + 3x^3 + x^2 + 6x + 1$ entre $3x^2 + 1$ en $\mathbb{Z}_7[x]$ y en $\mathbb{Z}_{10}[x]$.

Ejercicio 40. Comprueba que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para $p = 2, 3, 5, 7, 11, 13, 17$.

En general se tiene que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para cualquier número primo.

- Si a es tal que $a^2 \equiv -1 \pmod{p}$ entonces $(x^2 + a)(x^2 - a)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv 2 \pmod{p}$ entonces $(x^2 + ax + 1)(x^2 - ax + 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv -2 \pmod{p}$ entonces $(x^2 + ax - 1)(x^2 - ax - 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.

Y se tiene que para cualquier primo p, hay en $\mathbb{Z}_p$ una raíz cuadrada de -1, de 2 o de -2.

Ejercicio 41. Sean $p(x) = x^4 + 2x^2 + 2x + 1$, y $q(x) = x^3 + 2x^2 + x + 2$ dos polinomios con coeficientes en $\mathbb{Z}_3$. Sean $r(x) = p(x) \bmod q(x)$ y $s(x) = q(x) \bmod r(x)$.

- Calcula todos los divisores de $p(x)$ (hay 8 en total, cuatro de ellos mónicos), de $q(x)$ (también hay 8) de $r(x)$ (en total 6) y $s(x)$ (hay 4).
- Calcula todos los divisores comunes de $p(x)$ y $q(x)$; de $q(x)$ y $r(x)$; y de $r(x)$ y $s(x)$.
- Calcula el mínimo común múltiplo de $p(x)$ y $q(x)$.

Ejercicio 42. Calcula un máximo común divisor de $a(x)$ y $b(x)$ en los siguientes casos:

1. $a(x) = x^4 + 2x^2 + 1, b(x) = x^4 - 1$ en $\mathbb{Z}_5[x]$.
2. $a(x) = x^4 + 2x^2 + 1, b(x) = x^2 + 2$ en $\mathbb{Z}_3[x]$.

Ejercicio 43. Calcula las raíces en $\mathbb{Z}_5$ del polinomio $x^2 + x + 4$.

Ejercicio 44. Calcula en $\mathbb{Z}_7[x]$ el resto de dividir

1. $x^7 + x^2 + 1$ entre $x - 1$,
2. $x^n + 1$ entre $x - 1$.

Ejercicio 45. Calcula en $\mathbb{Z}_5[x]$ el resto de dividir $x^n + 2$ entre $x + 4$.

Ejercicio 46. Calcula el resto de dividir el polinomio $x^{1321} + 5$ por el polinomio $x + 3$ en el anillo $\mathbb{Z}_7[x]$.

Ejercicio 47. Calcula el cociente y el resto de la división para las siguientes parejas de polinomios considerados en los anillos, $\mathbb{Z}_5[x]$ y $\mathbb{Z}_7[x]$.

1. $p(x) = x^4 - x^2 + 1$, $q(x) = 2x^2 + 1$.
2. $p(x) = x^5 - x^3 + 3x - 5$, $q(x) = x^2 + 5$.
3. $p(x) = x^8 + x^4 + 1$, $q(x) = x^2 - x + 1$.

4. $p(x) = x^5 - x^3 + 3x - 5$, $q(x) = x^2 + 7$.

Ejercicio 48. Encuentra todos los números primos p tales que $x^2 + 2$ sea un divisor de $x^5 - 10x + 12$ en $\mathbb{Z}_p[x]$.

Ejercicio 49. Halla un máximo común divisor y un mínimo común múltiplo en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$ de las siguientes parejas de polinomios:

1. $p(x) = x^2 - 1$, $q(x) = x^3 - 3x^2 + 6x - 4$.
2. $p(x) = x^2 + 2x + 1$, $q(x) = x^3 + 7x^2 + 15x + 9$.
3. $p(x) = x^5 +^5 x^4 + 4x^3 + 3x^2 + 2x - 1$, $q(x) = x^3 - 3x^2 + 2x - 1$.

Encuentra en cada caso polinomios $u(x)$ y $v(x)$ tales que

$$p(x) \cdot u(x) + q(x) \cdot v(x) = mcd(p(x), q(x)).$$

Ejercicio 50. Encuentra todas las raíces de $x^2 - 1 \in \mathbb{Z}_8[x]$. Da dos factorizaciones distintas de $x^2 - 1$ como producto de polinomios mónicos.

Ejercicio 51. Comprueba que los polinomios $x^3 + x^2 + x + 1$ y $x^2 + 2x + 1$ determinan la misma aplicación $f : \mathbb{Z}_3 \to \mathbb{Z}_3$.

Ejercicio 52. El polinomio $x^4 - 1$ puede factorizarse en factores lineales en $\mathbb{Z}_5[x]$. Encuentra dicha factorización.

Ejercicio 53. Descompón como producto de irreducibles el polinomio $x^6 - 1$ en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$ y $\mathbb{Z}_7[x]$.

Ejercicio 54. Sea $A = \mathbb{Z}_2[x]_{x^3+1}$.

1. Calcula las unidades de A, y da, en cada caso, su inverso. ¿Es la suma de dos unidades una unidad? ¿Y el producto?
2. Calcula los divisores de cero. Para cada uno de ellos, encuentra un elemento no nulo de A que al multiplicarlo por él de cero. ¿Es la suma de dos divisores de cero un divisor de cero? ¿Y el producto?.

Ejercicio 55. Sea $A = \mathbb{Z}_5[x]_{x^3+3}$, y $\alpha = [x] \in A$.

- Comprueba que $3\alpha^2 + 4\alpha + 1$ y $2\alpha + 3$ son unidades y calcula sus inversos.
- Comprueba que $3\alpha^2 + 3$ y $4\alpha^3 + \alpha^2 + 3\alpha + 1$ son divisores de cero. Multiplícalos por un elemento no nulo de A para que de cero.

Ejercicio 56. ¿Cuántos elementos tiene $\mathbb{Z}_3[x]_{x^4+x^2+x+1}$? ¿Cuántos de ellos tienen inverso?

Ejercicio 57. Sean $K_1 = \mathbb{Z}_2[x]_{x^4+x+1}$ y $K_2 = \mathbb{Z}_2[x]_{x^4+x^3+x^2+x+1}$. Sean $\alpha = [x]$ y $\beta = [x]$, tomadas respectivamente en K_1 y K_2.

Calcula todas las potencias de α y β, y encuentra un isomorfismo $K_2 \to K_1$.

Ejercicio 58. Demuestra que $x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$ y que $x^3 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$. Describe todos los elementos, y la aritmética de $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_2[x]_{x^3+x+1}$.

Preguntas test

Ejercicio 59. Dado el sistema de congruencias

$$\begin{cases} 23x \equiv 54 \pmod{60} \\ 12x \equiv 21 \pmod{35} \end{cases}$$

a) Tiene una solución en el intervalo $[1000, 2000]$.

b) Tiene más de una solución en el intervalo $[1000, 2000]$.

c) Tiene infinitas soluciones, pero ninguna en el intervalo $[1000, 2000]$.

d) No tiene solución, pues $\mathrm{mcd}(60, 35) \neq 1$.

Ejercicio 60. La clase del 28 módulo 75

a) Tiene un inverso.

b) No tiene inverso porque ni 4 ni 15 son primos.

c) Tiene dos inversos.

d) Es un divisor de cero.

Ejercicio 61. Las dos últimas cifras del número $37129373222227^{524525273010}$ son

a) 27.

b) 49.

c) 91.

d) 63.

Ejercicio 62. Sea p un número primo. La congruencia $ax \equiv 1 \pmod{p^2}$

a) No tiene solución, pues p^2 no es primo.

b) Tiene solución si, y sólo si, $ax \equiv 1 \pmod{p}$ tiene solución.

c) Tiene solución, ya que $\mathrm{mcd}(a, 1)|p^2$.

d) Tiene solución salvo que a sea múltiplo de p^2.

Ejercicio 63. El número de unidades de $\mathbb{Z}_{123}$ es

a) 0

b) 40

c) 80

d) 122

Ejercicio 64. Disponemos de 45 billetes de 20 euros, y 18 billetes de 50 euros. ¿De cuántas formas distintas podemos conseguir 1110 euros?

(a) 7.

(b) 11.

(c) 9.

(d) 5.

Ejercicio 65. Sea $a = 24^{1234}$. La congruencia $ax \equiv 6$ mód 11 tiene como solución a:

1. $x = 3$.
2. $x = 7$.
3. $x = 10$.
4. $x = 2$.

Ejercicio 66. ¿Cuál de los siguientes anillos es un cuerpo?

a) $\mathbb{Z}_7[x]$.

b) $\mathbb{Z}_5[x]_{x^2-1}$.

c) $\mathbb{Z}_2[x]_{x^2+1}$.

d) $\mathbb{Z}_3[x]_{x^2+1}$.

Ejercicio 67. ¿Cuál de los siguientes grupos de polinomios de $\mathbb{Z}_7[x]$ es múltiplo de $x^2 - 1$?

a) $x^{2n} + 1$ para $n \geq 1$.

b) $x^{4n} + x^{2n} - 2$ para $n \geq 1$.

c) $x^{2n} - x^n - 1$ para $n \geq 1$.

d) $x^{2n} - 2x^n + 1$ para $n \geq 1$.

Ejercicio 68. Dados $p(x) = x^4 + x^3 + x^2 + x$ y $q(x) = x^5 + x^2 + x + 1$ dos polinomios con coeficientes en $\mathbb{Z}_2$, el máximo común divisor de $p(x)$ y $q(x)$ vale:

a) $x^2 + 1$.

b) $x^2 + x$.

c) $x^4 + x^3 + x^2 + x$.

d) 1.

Ejercicio 69. Sea $A = \mathbb{Z}_5[x]_{x^4+3x^3+3x^2+x+2}$, y sea $p(x) = x^2 + 1 \in A$. Entonces:

a) $p(x)$ no tiene inverso en A, pues $x^4 + 3x^3 + 3x^2 + x + 2$ tiene a $x = 1$ como raíz.

b) $p(x)$ no tiene inverso en A, pues $x^2 + 1$ no es irreducible.

c) $p(x)$ tiene inverso en A y vale $2x^3 + x^2 + 4x + 1$.

d) $p(x)$ tiene inverso en A y vale $x^3 + x^2 + 4x + 2$.

Ejercicio 70. Determina cuál de los siguientes anillos es un cuerpo:

1. $\mathbb{Z}_3[x]_{x^2+1}$.
2. $\mathbb{Z}_5[x]_{x^2+1}$.
3. $\mathbb{Z}_{11}[x]_{x^2+1}$.
4. $\mathbb{Z}_{13}[x]_{x^2+1}$.

Ejercicio 71. Sea $A = \mathbb{Z}_2[x]_{x^4+x+1}$, y $p(x) = x^3 + x^2 + x + 1 \in A$. Entonces:

a) $p(x)$ no tiene inverso, ya que no es irreducible.

b) $p(x)$ tiene inverso, y vale $x^3 + x + 1$.

c) $p(x)$ no tiene inverso, pues $p(1) = 0$.

d) $p(x)$ tiene inverso y vale x^3.