ARITMÈTICA
Primavera 2020
Llista per als laboratoris de problemes

Divisibilitat

1. (a) En quina base el nombre (decimal) 136 s'escriu 2 5 3?

(b) En quina base el nombre (decimal) 621 s'escriu 2 5 1 3?

2. (a) Escriviu el nombre $(235\ 678\ 943\ 215)_{1000}$ en base 10 i en base 100.

(b) Escriviu el nombre $(ABCDEF01234)_{16}$ en les bases 2, 4 i 8.

3. (a) Trobeu el màxim comú divisor i el mínim comú múltiple dels nombres enters 2047 i 2225.

(b) Ídem per a 2200 i 2816.

4. (a) Trobeu el màxim comú divisor $d > 0$ de la parella de nombres enters $a = 2795$ i $b = 2314$.

(b) Trobeu nombres enters r, s tals que $d = ra + sb$.

(c) Feu el mateix per a la parella $a = 2842$, $b = 3567$.

5. Calculeu, per a tot nombre enter n, $\mathrm{mcd}(28n - 5, 35n - 8)$.

6. Siguin a, $b \in \mathbb{Z}$ nombres enters tals que $a > 0$, $b > 0$ i $\mathrm{mcd}(a, b) = 1$.

(a) Demostreu que si $ab = c^2$, per a algun nombre enter c, llavors existeixen x, $y \in \mathbb{Z}$ tals que $a = x^2$, $b = y^2$, i $\mathrm{mcd}(x, y) = 1$.

(b) Doneu un exemple que ensenyi que en el cas en què no sigui $\mathrm{mcd}(a, b) = 1$, es pot tenir una igualtat de la forma $ab = c^2$, amb $c \in \mathbb{Z}$, però a i b no quadrats.

7. Siguin a, $b \in \mathbb{Z}$ nombres enters.

(a) Proveu que si $\mathrm{mcd}(a, b) = 1$, llavors $\mathrm{mcd}(a^n, b^n) = 1$, per a tot nombre natural n.

(b) Proveu que si $\mathrm{mcd}(a, b) = d$, llavors $\mathrm{mcd}(a^n, b^n) = d^n$, per a tot nombre natural n.

8. (a) Proveu que, per a tot nombre enter n, és $\mathrm{mcd}(n, n + 1) = 1$.

(b) Sigui $k \in \mathbb{Z}$ un nombre enter tal que, per a tot $t \in \mathbb{N}$, és $\mathrm{mcd}(t, t+k) = 1$. Demostreu que $k = \pm 1$.

(c) Esbrineu per a quins valors de $k \in \mathbb{Z}$ es té que, per a tot $s \in \mathbb{N}$, és $\mathrm{mcd}(s, s + k) = 2$.

Equacions diofantines lineals

9. Per a cadascuna de les equacions diofantines següents, doneu la solució (x, y) tal que x pren el menor valor positiu (i no nul) possible:

(a) $119x + 84y = 7$,

(b) $119x + 84y = 21$,

(c) $104x + 143y = 13$.

10. Heu comprat llapis a $1,01$ euros i retoladors a $1,40$ euros. Si, en total, us heu gastat $29,93$ euros, quants llapis i quants retoladors heu comprat?

11. Calculeu totes les solucions enteres de les equacions

(a) $111x + 81y + 45z = 15$, (b) $21x + 49y + 105z = 147$,
(c) $6x + 10y + 9z = 3$, (d) $165x + 60y + 105z + 30t = 225$.

Polinomis

12. Apliqueu l'algoritme d'Euclides als polinomis $p_1 = 2x^4 + 4x^3 + 7x^2 + 12x + 3$, i $p_2 = x^4 + 2x^3 + 6x^2 + 6x + 9$, per a calcular-ne el màxim comú divisor, d, i una igualtat de Bézout que expressi d com a combinació lineal de p_1 i p_2.

Tot i que el polinomi p_2 és mònic i, per tant, la divisió entera entre p_2 es pot realitzar en $\mathbb{Z}[x]$, els polinomis que proporciona l'algoritme d'Euclides no tenen els coeficients enters. Podríeu donar-ne una explicació?

13. Trobeu totes les arrels i les multiplicitats corresponents dels polinomis següents i; per a cadascun d'ells, escriviu el conjunt de les arrels racionals, el conjunt de les arrels reals no racionals, i el conjunt de les arrels complexes:

(a) $q_1 = 2x^3 - 4x^4 + x^5$,

(b) $q_2 = 2 - 8x + 11x^2 - 6x^3 + x^4$,

(c) $q_3 = -2x + 2x^2 + 5x^3 - 3x^4 - 3x^5 + x^6$.

14. Proporcioneu les descomposicions de tots els polinomis de l'enunciat de l'exercici anterior com a producte de polinomis irreductibles en $\mathbb{C}[x]$, en $\mathbb{R}[x]$ i en $\mathbb{Q}[x]$.

15. Sigui p un polinomi de coeficients reals i sigui z un nombre complex. Demostreu que $p(z) = 0$ si, i només si, $p(\overline{z}) = 0$.

Congruències

16. Calculeu totes les solucions de les congruències següents:

(a) $30x \equiv 3 \pmod 7$,

(b) $15x \equiv 5 \pmod{26}$,

(c) $1224x \equiv 31 \pmod{335}$,

(d) $1984x \equiv 666 \pmod{2001}$,

(e) $154x \equiv 112 \pmod{280}$,

(f) $525x \equiv 735 \pmod{1000}$,

(g) $55x \equiv 77 \pmod{121}$,

(h) $68x \equiv 153 \pmod{170}$,

(i) $45x \equiv 105 \pmod{120}$,

(j) $45x \equiv 105 \pmod{100}$.

17. Resoleu el sistema de congruències

$$x \equiv 1 \pmod{6}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 3 \pmod{17};$$

doneu-ne la solució positiva més petita.

18. Resoleu el sistema de congruències

$$3x \equiv 2 \pmod{4}, \quad 4x \equiv 7 \pmod{15}, \quad 5x \equiv -1 \pmod{17}.$$

19. Resoleu el sistema de congruències

$$3x \equiv 6 \pmod{12}, \quad 10x \equiv 15 \pmod{25};$$

doneu-ne totes les solucions positives menors que 300.

20. Resoleu el sistema de congruències

$$x \equiv 1 \pmod{5}, \quad x \equiv 3 \pmod{8}, \quad x \equiv 3 \pmod{12}.$$

21. *Tenim certs objectes, no sabem en quin nombre.*
Si el dividim per 3*, el residu és* 2*;*
per 5*, el residu és* 3*;*
i per 7*, el residu és* 2*.*
Quin és el nombre?
Aquest problema va ésser plantejat per Sun Tsu, en el segle IV, en el llibre Sunzi Suanjing.

22. Determineu la xifra que manca en el NIF següent:

`4697649?-G.`

Comproveu la correcció del vostre NIF.

23. Determineu quins dels codis següents són ISBN:

`0-394-38049-5, 1-09-231221-3, 0-8218-0123-6,`
`0-404-50874-X, 90-6191-705-2, ?-261-05073-X.`

Nombres complexos

24. Calculeu: $(1+5i)(12-17i)$, $(19+4i)(19-4i)$, $(-4+19i)(19-4i)$, $\dfrac{8+3i}{7-11i}$.

25. Sigui $\alpha \in [0, 2\pi]$. Demostreu que $\cos\alpha = \dfrac{e^{i\alpha}+e^{-i\alpha}}{2}$, i que $\sin\alpha = \dfrac{e^{i\alpha}-e^{-i\alpha}}{2i}$.

26. Escriviu en forma binòmica els nombres complexos $3e^{\frac{3\pi}{4}i}$, $12e^{\frac{-22\pi}{3}i}$, $19e^{\frac{14\pi}{2}i}$, i $(-\sqrt{3}+i)^8$.

27. Escriviu en forma polar els nombres complexos $\dfrac{\sqrt{2}}{2}+i\dfrac{\sqrt{2}}{2}$, $5\sqrt{2}-5i\sqrt{2}$, $\dfrac{i}{2}$.

28. Trobeu quatre nombres complexos diferents z_1, z_2, z_3, z_4, tals que $z_j^4 = 1$, per a $j = 1, 2, 3, 4$.

Nombres de Mersenne, nombres de Fermat, nombres perfectes

29. Comproveu que els nombres de Mersenne M_2, M_3, M_5, M_7 són primers, però que el nombre de Mersenne M_{11} no ho és. Sabeu trobar algun altre nombre de Mersenne que sigui primer? I algun altre que sigui compost?

30. El nombre $p := 57885161$ és primer (demostreu-ho); per tant, podem pensar en el nombre de Mersenne M_p. Quantes xifres té l'expressió decimal de M_p?
Observació. Se sap que el nombre de Mersenne M_p és primer des del dia 25 de gener de 2013; els dos anteriors nombres primers de Mersenne que es coneixen corresponen a $p = 43112609$ (se sap que és primer des del dia 23 d'agost de 2008) i a $p = 42643801$ (se sap que és primer des del dia 12 d'abril de 2009).

31. Comproveu que els nombres de Fermat F_0, F_1, $\dots$, F_4 són primers, i que 641 és un divisor propi de F_5, de manera que F_5 és compost. Sabeu trobar algun altre nombre de Fermat que sigui primer? I algun altre que sigui compost?

32. Un nombre enter positiu es diu que és *perfecte* quan és igual a la suma de tots els seus divisors, llevat d'ell mateix. És a dir, quan $\sigma_1(n) = 2n$.

(a) Comproveu que 6, 28, 496, 8128 són els quatre primers nombres perfectes.

(b) Cerqueu informació sobre nombres perfectes parells.

(c) Cerqueu informació sobre nombres perfectes senars.

33. Demostreu que $2^{p-1}(2^p - 1)$ és un nombre perfecte quan $M_p = 2^p - 1$ és un nombre primer de Mersenne. (*Teorema d'Euclides*)

34. Demostreu que tot nombre perfecte parell és del tipus donat per Euclides. *Indicació:* Sigui $2^{n-1}q$ perfecte, on q és senar i $n > 1$. Aleshores $2^n q = (2^n - 1)s$, on s és la suma dels divisors de q. Escriviu $s = q + d$. Aleshores $q = d(2^n - 1)$, i d és un divisor de q. Per tant, $d \neq q$. Així, q, d són els únics divisors de q. Deduïu que $d = 1$ i q és un nombre primer de Mersenne.

Arrels primitives

35. Per a cadascun dels nombres enters $2 \leq N \leq 25$, calculeu una arrel primitiva mòdul N, o bé comproveu que no existeix.

36. Siguin g una arrel primitiva mòdul un nombre enter $N \geq 2$ i $D \geq 2$ un divisor de N. Demostreu que la reducció mòdul D de g és una arrel primitiva mòdul D.

37. Comproveu que 2, 5, 18 i 32 són arrels primitives mòdul 37. Comproveu que 2, 5, i 32 ho són mòdul 37^{15}, però que 18 no ho és, i que només 5 ho és mòdul $2 \cdot 37^{15}$.

Congruències quadràtiques

38. Calculeu totes les solucions de les congruències:

(a) $x^2 + x + 1 \equiv 0 \pmod 7$.

(b) $x^2 + 5x + 1 \equiv 0 \pmod 7$.

(c) $x^2 + 3x + 1 \equiv 0 \pmod 7$.

39. Calculeu totes les solucions de la congruència: $x^2 + 6x - 31 \equiv 0 \pmod{72}$.

40. Calculeu els símbols de Jacobi següents: $\left(\frac{3}{53}\right)$, $\left(\frac{31}{641}\right)$, $\left(\frac{7}{79}\right)$, $\left(\frac{111}{991}\right)$, $\left(\frac{15}{101}\right)$, $\left(\frac{105}{1009}\right)$, $\left(\frac{5}{21}\right)$, $\left(\frac{1009}{2307}\right)$, $\left(\frac{27}{101}\right)$, $\left(\frac{2663}{3299}\right)$, $\left(\frac{111}{1001}\right)$, $\left(\frac{10001}{20003}\right)$.

41. En general, fixat un nombre enter a, sigui p un nombre primer per al qual a no sigui un quadrat en $\mathbb{Z}/p\mathbb{Z}$. Demostreu que si n és un nombre enter divisible per p, llavors a no és un quadrat en $\mathbb{Z}/n\mathbb{Z}$.