ARITMÈTICA
Primavera 2021
Exercicis per a la classe de problemes

1. Fixem un nombre natural $b > 1$, que anomenarem base de numeració. Demostreu que per a tot nombre natural $x > 0$ existeix $n \geq 0$ i existeixen nombres $x_0, x_1, \ldots, x_n \in \{0, 1, 2, \ldots, b-1\}$ únics tals que $x_n \neq 0$ i $x = x_0 + x_1 \cdot b + x_2 \cdot b^2 + \cdots + x_n \cdot b^n$. Aquesta expressió s'anomena l'expressió de x en base b; l'expressió en base b del nombre zero és 0.

2. Sigui $b > 1$ una base de numeració i sigui $k \geq 1$ un nombre natural. Demostreu que les xifres de l'expressió en base b^k de qualsevol nombre natural x són els nombres naturals les expressions dels quals en base b s'obtenen en agrupar de k en k les xifres de l'expressió de x en base b, a partir de la xifra de les unitats.

3. (Expressió de polinomis en base g.) Siguin k un cos i $g \in k[X]$ un polinomi no constant. Demostreu que tot polinomi $f \in k[X]$ admet una expressió única de la forma

$$f = a_0 + a_1 \cdot g + \cdots + a_k \cdot g^k,$$

amb $a_0, a_1, \ldots, a_k \in k[X]$, polinomis de grau menor (estrictament) que el grau de g.

4. (Expressió de polinomis en base g.) Sigui $g \in \mathbb{Z}[X]$ un polinomi mònic, no constant. Demostreu que tot polinomi $f \in \mathbb{Z}[X]$ admet una expressió única de la forma

$$f = a_0 + a_1 \cdot g + \cdots + a_k \cdot g^k,$$

amb $a_0, a_1, \ldots, a_k \in \mathbb{Z}[X]$, polinomis de grau menor (estrictament) que el grau de g.

5. Calculeu el quocient i el residu de la divisió del polinomi $f = (1+x)^6$ de $\mathbb{Z}[x]$ entre el polinomi $g = x - 1$.

6. Siguin $a, b \in \mathbb{Z}$ nombres enters tals que $\mathrm{mcd}(a, b) = 1$. Calculeu $\mathrm{mcd}(a+b, a-b)$ en funció de a i b.

7. Demostreu que si n, $n+2$ i $n+4$ són nombres naturals primers, aleshores $n = 3$.

8. (a) Siguin a, m, n nombres naturals, $m \neq n$. Calculeu $\mathrm{mcd}(a^{2^m} + 1, a^{2^n} + 1)$.

(b) Siguin m, n nombres naturals i $d := \mathrm{mcd}(m, n)$. Demostreu que $\mathrm{mcd}(2^m - 1, 2^n - 1) = 2^d - 1$.

9. Demostreu que, per a tot nombre enter k, els nombres $6k-1$, $6k+1$, $6k+2$, $6k+3$, $6k+5$ són primers entre si dos a dos; és a dir, que per a $a, b \in \{6k-1, 6k+1, 6k+2, 6k+3, 6k+5\}$, $a \neq b$, és $\mathrm{mcd}(a, b) = 1$.

10. Observeu que si p, q són nombres naturals primers diferents, els divisors de $p^2 q^3$ coincideixen amb els $3 \cdot 4 = 12$ termes de l'expansió del producte

$$(1 + p + p^2)(1 + q + q^2 + q^3),$$

i que aquest producte és igual a la suma de tots els divisors de $p^2 q^3$.

Donat un enter n, considerem les funcions

$$\sigma_k(n) := \sum_{d \mid n} d^k, \quad k \in \mathbb{Z},\ k \geq 0.$$

Sigui $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ la descomposició de n en factors primers.

(a) Expliqueu el significat de les funcions σ_k, per a $k = 0,\, 1,\, > 1$.

(b) Demostreu la fórmula

$$\sigma_1(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

(c) Demostreu la fórmula

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)k} - 1}{p_i^k - 1},$$

per a tot $k \geq 1$.

11. Siguin $a,\, b \in \mathbb{Z}$ nombres enters tals que $\mathrm{mcd}(a,b) = 1$. Calculeu $\mathrm{mcd}(a^2+b^2, a^2-b^2, 2ab)$ en funció de a i b.

12. Trobeu totes les solucions (x,y), amb $x, y \in \mathbb{Z}_{>0}$, del sistema d'equacions

$$\left.\begin{array}{r} xy = 51840 \\ \mathrm{mcd}(x,y) = 24 \end{array}\right\}$$

13. Demostreu que no hi ha cap nombre primer de la forma $n = a^4 - b^4$, amb $a,\, b \in \mathbb{Z}$.

14. Siguin a, b nombres naturals no nuls, i siguin

$$a = \prod_p p^{v_p(a)}, \qquad b = \prod_p p^{v_p(b)},$$

les descomposicions de a i b com a producte de nombres primers. Proveu que

$$(1) \quad \mathrm{mcd}(a,b) = \prod_p p^{\min\{v_p(a), v_p(b)\}}, \qquad (2) \quad \mathrm{mcm}(a,b) = \prod_p p^{\max\{v_p(a), v_p(b)\}}.$$

15. Demostreu que si p és un nombre natural primer, aleshores, per a $1 \leq k \leq p-1$, p divideix el nombre combinatori $\binom{p}{k}$. És certa aquesta propietat si p no és primer?

16. Siguin $a_1,\, a_2,\, \ldots,\, a_n \in \mathbb{Z}$ nombres enters i $d = \mathrm{mcd}(a_1, a_2, \ldots, a_n)$.

(a) Demostreu que existeixen nombres enters $r_1,\, r_2,\, \ldots,\, r_n$ tals que $r_1a_1 + r_2a_2 + \cdots + r_na_n = d$.

(b) Calculeu nombres enters r, s, t tals que $17r + 51s + 45t = 1$ o bé demostreu que no existeixen.

17. Siguin $n > 1$ un nombre natural i p el menor nombre natural primer que divideix n. Demostreu que si $p^3 > n$, llavors n és primer (i $p = n$) o bé $\dfrac{n}{p}$ és primer.

18. Siguin $K \in \mathbb{N}$ i $N := 4K+3$. Demostreu que, si N no és primer, llavors existeix un divisor primer p de N de la forma $p = 4k+3$, per a algun $k \in \mathbb{N}$. Adapteu la demostració del teorema d'Euclides feta a classe per a demostrar que el conjunt dels nombres naturals primers de la forma $4K+3$, $K \in \mathbb{N}$, conté una infinitat de nombres primers.

19. Establiu criteris de divisibilitat que, donat un nombre enter $n \geq 1$ expressat en base 10, decideixin quan aquest nombres és divisible per un enter d tal que $1 \leq d \leq 11$.

20. Demostreu que no existeix cap polinomi no constant $f(x) \in \mathbb{Z}[x]$ tal que $f(a)$ sigui primer per a tot $a \in \mathbb{Z}$.

21. Calculeu la taula de sumar i la de multiplicar de cadascun dels anells $\mathbb{Z}/5\mathbb{Z}$ i $\mathbb{Z}/6\mathbb{Z}$.

Determineu, mirant les taules, quins són els elements invertibles i quins els divisors de zero de cadascun d'aquests dos anells.

22. Calculeu, si existeixen, els inversos de $6 \pmod{11}$, $6 \pmod{17}$, $6 \pmod{10}$, $7 \pmod{11}$, $7 \pmod{17}$, i $7 \pmod{10}$.

23. (a) Demostreu que per a tot nombre enter a, existeixen nombres enters únics q, r tals que $a = 7q + r$ i $r \in \{0, 3, 6, 9, 12, 15, 18\}$.

(b) Demostreu que per a tot nombre enter a, existeixen nombres enters únics q, r tals que $a = 7q + r$ i $r \in \{0, 3, 6, 9, -3, -6, -9\}$.

(c) Demostreu que per a tot nombre enter a, existeixen nombres enters únics q, r tals que $a = 7q + r$ i $r \in \{0, 3, 9, 27, 81, 243, 729\}$.

24. *Una dona va al mercat i un cavall trepitja el seu cistell i li trenca els ous. El cavaller s'ofereix a pagar-li els danys i pregunta quants ous portava. La dona no recorda el nombre exacte, però sap que en agafar-los de dos en dos li'n sobrava un, el mateix li passava quan els agafava de tres en tres, de quatre en quatre, de cinc en cinc i de sis en sis. En canvi, quan els agafava de set en set, li quedava just. Quants ous portava com a mínim?*
Aquest problema es troba en un text de l'Índia del segle VI.

25. Demostreu que $3^n + 2 \cdot 17^n$ no és un quadrat perfecte per a cap valor de $n \in \mathbb{Z}_{>0}$. (Pista: podeu considerar congruències mòdul 16).

26. La masovera se'n va al mercat. És dijous i, per tant, compra nous. En tornar cap a casa, es dedica a comptar-les. Si les compta de 2 en 2, n'hi sobra 1; si les compta de 3 en 3, n'hi sobren 2; i així, fins que les compta de 7 en 7, i no n'hi sobra cap. Quantes nous ha comprat? (Informació extra: la masovera va al mercat cada dijous i a la seva família no els agraden les nous.)

27. Sigui $n \geq 2$ un nombre enter. Demostreu que n és primer si, i només si, n divideix $(n-1)! + 1$. (*Teorema de Wilson.*)

28. Calculeu, "a mà", les potències següents: $5^{2010} \pmod{11}$, $6^{40} \pmod{33}$, $7^{135} \pmod{10}$, $30^{45} \pmod{15}$.

29. Siguin p, q dos nombres naturals primers diferents. Demostreu que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

30. Demostreu que per a tot nombre natural primer p se satisfà que

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}.$$

Pista: podeu utilitzar el problema 15.

31. Els enters de la forma $M_n := 2^n - 1$ s'anomenen *nombres de Mersenne.* Un primer de Mersenne és un nombre de Mersenne que, a més a més, és primer. Demostreu que si M_p és primer, aleshores p és primer.

32. Sigui $k \geq 2$ un nombre natural. Demostreu que si $2^k + 1$ és un nombre primer, llavors existeix $n \geq 1$ tal que $k = 2^n$. Els nombres $F_n := 2^{2^n} + 1$, per a $n \geq 0$, s'anomenen nombres de Fermat.

33. Sigui $F_n = 2^{2^n} + 1$ el n-èsim nombre de Fermat, on n és un enter no negatiu. Demostreu que

$$F_0 \, F_1 \cdots F_{n-1} = F_n - 2,$$

per a tot $n \geq 1$.

34. Demostreu que, per a tot parell m, n de nombres enters diferents no negatius, els nombres de Fermat F_m, F_n són relativament primers. Deduïu una demostració alternativa a la donada per Euclides sobre l'existència d'una infinitat de nombres primers.

35. Determineu totes les congruències de grau 2 mòdul 2 i totes les seves solucions.

36. Sigui p un nombre natural primer senar. Demostreu que a $\mathbb{Z}/p\mathbb{Z}$ hi ha exactament $\dfrac{p+1}{2}$ elements que són quadrats i $\dfrac{p-1}{2}$ elements que no ho són. Succeeix el mateix si p no és primer?

37. Trobeu totes les solucions de les congruències següents:

(a) $X^2 \equiv 4 \pmod{p}$, per a tots els nombres primers p;

(b) $X^2 \equiv 31 \pmod{75}$;

(c) $X^2 \equiv 46 \pmod{231}$;

(d) $X^2 \equiv 16 \pmod{105}$;

(e) $X^2 \equiv 1156 \pmod{3^2 \cdot 5^3 \cdot 7^5 \cdot 11^6}$.

38. Sigui p un nombre natural primer senar. A partir d'uns quants casos particulars, esbrineu una llei general per a decidir en quines circumstàncies -1 és un quadrat en $\mathbb{Z}/p\mathbb{Z}$ i ens quines no ho és. Intenteu demostrar aquesta llei.

39. Repetiu l'exercici anterior però per a 2 en lloc de -1; és a dir, esbrineu una llei general per a decidir en quines circumstàncies 2 és un quadrat en $\mathbb{Z}/p\mathbb{Z}$ i ens quines no ho és, i intenteu demostrar aquesta llei.

40. (a) Demostreu que -2 és un quadrat mòdul un nombre primer $p > 2$ i, i només si, $p \equiv 1$ o bé $p \equiv 3 \pmod{8}$.

(b) Sigui n un nombre enter, i posem $N := (2n+1)^2+2$. Demostreu que N és divisible per un nombre natural primer p tal que $p \equiv 3 \pmod{8}$.

(c) Demostreu que hi ha una infinitat de nombres primers de la forma $8k+3$, $k \in \mathbb{N}$.

41. Siguin a i n nombres naturals relativament primers. Estudieu quan l'equació congruencial

$$X^2 \equiv a \pmod{n}$$

té solució.

42. Demostreu que hi ha una infinitat de nombres naturals primers de la forma $4k+1$

43. Per a quins nombres naturals primers p el nombre 3 és residu quadràtic mòdul p? I -3?

44. Sigui $N > 6$ un nombre enter per al qual existeix alguna arrel primitiva mòdul N. Demostreu que el producte de totes les arrels primitives mòdul N és $1 \in (\mathbb{Z}/N\mathbb{Z})^*$.

45. Siguin p un nombre natural primer i $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Demostreu que per a tot nombre enter n tal que $\mathrm{mcd}(n, p-1) = 1$, la congruència $X^n \equiv a \pmod{p}$ té una solució i només una.

46. Siguin p un nombre natural primer, $a \in (\mathbb{Z}/p\mathbb{Z})^*$, i m l'ordre de a en $(\mathbb{Z}/p\mathbb{Z})^*$. Demostreu que la congruència $X^n \equiv a \pmod{p}$ té solució si, i només si, $\mathrm{mcd}(p-1, n)$ divideix $\dfrac{p-1}{m}$ i que, en aquest cas, el nombre de solucions de la congruència és $\mathrm{mcd}(p-1, n)$.

47. Siguin p un nombre natural primer senar i g un nombre enter no múltiple de p. Demostreu que g és una arrel primitiva mòdul p si, i només si, per a tot divisor primer ℓ de $p-1$ és $g^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p}$.

48. Sigui p un nombre natural primer senar tal que $q := 2p-1$ també sigui un nombre primer, i posem $N := pq$. Demostreu que N és un nombre pseudoprimer respecte de tota base $b \in (\mathbb{Z}/N\mathbb{Z})^*$ que sigui un quadrat en $(\mathbb{Z}/q\mathbb{Z})^*$. En particular, N és pseudoprimer, com a mínim, per a la meitat de les bases possibles.

49. (a) Sigui $N := pq$ el producte de dos nombres naturals primers senars p i q. Demostreu que si N és pseudoprimer respecte d'una base $b > 1$, llavors $p|(b^{q-1}-1)$ i $q|(b^{p-1}-1)$.

(b) Deduïu de l'apartat anterior que, fixats un nombre primer p i una base $b > 1$, el conjunt dels nombres primers q per als quals $N := pq$ és pseudoprimer respecte de la base b és finit.