4 Aritmetică

4.1

P 1. Fie $a, b \in \mathbb{Z}$ două numere întregi, cu $b \neq 0$. Dacă $q, r \in \mathbb{Z}$ verifică $a = bq + r$, arătaţi că $(a, b) = (b, r)$.

P 2. (algoritmul lui Euclid) Fie $a, b \in \mathbb{Z}$ două numere întregi, cu $b \neq 0$, iar $q_1, q_2, \ldots, q_n, q_{n+1} \in \mathbb{Z}$, $r_1, r_2, \ldots, r_n \in \mathbb{N}^*$ astfel încât $|b| > r_1 > r_2 > \cdots > r_n > 0$ şi

$$\begin{aligned}
&a = bq_1 + r_1,\\
&b = r_1 q_2 + r_2,\\
&r_1 = r_2 q_3 + r_3,\\
&\vdots\\
&r_k = r_{k+1} q_{k+2} + r_{k+2},\\
&\vdots\\
&r_{n-2} = r_{n-1} q_n + r_n,\\
&r_{n-1} = r_n q_{n+1} (+0).
\end{aligned}$$

Arătaţi că $(a, b) = r_n$.

P 3. a) Determinaţi $(6188, 4709)$;
b) Determinaţi $(81719, 52003, 33649, 30107)$.

P 4. Fie $a, b \in \mathbb{Z}$ două numere întregi şi $d = (a, b)$. Arătaţi că
a) există două numere întregi u, v astfel încât $au + bv = d$.
b) $d = min\{k \in \mathbb{N}^* | (\exists) u, v \in \mathbb{Z} : k = au + bv\}$.

P 5. Fie $a, b \in \mathbb{Z}$ două numere întregi. Atunci $(a, b) = 1$ dacă şi numai dacă există două numere întregi u, v cu proprietatea că $au + bv = 1$.

P 6. (Lema lui Gauss) Arătaţi că dacă $a, b, c \in \mathbb{Z}$ sunt numere întregi cu proprietatea că $a|bc$ şi $(a, b) = 1$, atunci $a|c$.

P 7. Fie $a, b, c \in \mathbb{Z}$ trei numere întregi şi $(a, b) = d$. Arătaţi că ecuaţia liniară diofantică $ax + by = c$ are soluţii $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ dacă şi numai dacă $d|c$.

P 8. Fie $a, b, c \in \mathbb{Z}$ trei numere întregi, $(a, b) = d$ şi $a_,b_1 \in \mathbb{Z}$ astfel încât $a = da_1$ şi $b = db_1$. Arătaţi că dacă (x_0, y_0) este o soluţie particulară a ecuaţieie liniare diofantice $ax + by = c$, atunci mulţimea tuturor soluţiilor ecuaţiei este

$$\mathcal{S} = \{(x_0 + kb_1, y_0 - ka_1) |\, k \in \mathbb{Z}\}.$$

P 9. Rezolvaţi ecuaţiile liniare diofantice:
a) $47x - 111y = 89$;
b) $51x - 34y = 153$.

P 10. Fie $n \in \mathbb{N}^*$ un număr natural nenul. Relaţia de congruenţă modulo n este relaţia definită pe mulţimea numerelor întregi prin

$$a \equiv b (\text{mod } n) \overset{def}{\Longleftrightarrow} n | a - b.$$

Arătaţi că relaţia de congruenţă modulo n este o relaţie de echivalenţă, compatibilă cu adunarea, scăderea şi înmulţirea numerelor întregi.

P 11. Fie $n \in \mathbb{N}^*$ un număr natural nenul. Un număr întreg $a \in \mathbb{Z}$ se numeşte inversabil modulo n dacă există un număr întreg u astfel încât $au \equiv 1 (\text{mod } n)$. Arătaţi că a este inversabil modulo n dacă şi numai dacă $(a, n) = 1$.

P 12. Fie $n \in \mathbb{N}^*$ un număr natural nenul, iar $a, b \in \mathbb{Z}$ două numere întregi astfel încât $(a, n) = 1$. Arătaţi că congruenţa $ax \equiv b (\text{mod } n)$ are exact o soluţie x_1 în mulţimea $\{0, 1, \ldots, n - 1\}$ şi orice soluţie x a congruenţei satisface relaţia $x \equiv x_1 (\text{mod } n)$.

P 13. Fie $n \in \mathbb{N}^*$ un număr natural nenul, $a, b \in \mathbb{Z}$ două numere întregi şi $d = (a, n)$. Arătaţi că dacă $d|b$, atunci congruenţa $ax \equiv b (\text{mod } n)$ are exact d soluţii $x_1, x_2, \ldots, x_d$ în mulţimea $\{0, 1, \ldots, n - 1\}$.

P 14. Rezolvaţi următoarele congruenţe:
a) $256x \equiv 179 (\text{mod } 337)$;
b) $1215x \equiv 560 (\text{mod } 2755)$;
c) $1296x \equiv 1105 (\text{mod } 2413)$.

4.2

P 15. (teorema lui Wilson) Dacă $p \in \mathbb{N}^*$ este un număr prim, atunci $(p-1)! \equiv -1 (\text{mod } p)$.

P 16. (mica teoremă a lui Fermat) Dacă $p \in \mathbb{N}^*$ este un număr prim şi $a \in \mathbb{Z}$ este relativ prim cu p, atunci $a^{p-1} \equiv 1 (\text{mod } p)$.

P 17. (mica teoremă a lui Fermat, var.2**)** Dacă $p \in \mathbb{N}^*$ este un număr prim şi $a \in \mathbb{Z}$ un număr întreg, atunci $a^p \equiv a (\text{mod } p)$.

P 18. (teorema lui Euler) Fie $n \in \mathbb{N}^*$ un număr natural nenul şi $a \in \mathbb{Z}$ un număr întreg, relativ prim cu n. Atunci $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, unde φ este funcţia lui Euler, dată de $\varphi(n) =$ numărul numerelor naturale k cu proprietatea că $k < n$ şi $(k, n) = 1$.

P 19. Fie $n \in \mathbb{N}^*$ un număr natural nenul şi $a \in \mathbb{Z}$ un număr întreg, relativ prim cu n. Arătaţi că congruenţa $ax \equiv b (\text{mod } n)$ este echivalentă cu $x \equiv a^{\varphi(n)-1} b (\text{mod } n)$.

P 20. (Lema chinezească a resturilor.) Fie $m_1, m_2, \dots, m_k \in \mathbb{N}^*$ numere naturale nenule cu proprietatea că $(m_i, m_j) = 1$ pentru $i \neq j$ şi $r_1, r_2, \dots, r_k \in \mathbb{Z}$ numere întregi oarecare. Arătaţi că există un unic număr natural $r \in \{0, 1, \dots, m-1\}$, unde $m = m_1 m_2 \dots m_k$, astfel încât sistemul de congruenţe

$$\begin{cases} x \equiv r_1 (\text{mod } m_1) \\ x \equiv r_2 (\text{mod } m_2) \\ \vdots \\ x \equiv r_k (\text{mod } m_k) \end{cases}$$

să fie echivalent cu congruenţa $x \equiv r (\text{mod } m)$.

P 21. Rezolvaţi sistemele de congruenţe:
a) $x \equiv r_1 (\text{mod } 13)$, $x \equiv r_2 (\text{mod } 17)$;
b) $x \equiv r_1 (\text{mod } 25)$, $x \equiv r_2 (\text{mod } 27)$, $x \equiv r_3 (\text{mod } 59)$;
c) $x \equiv 3 (\text{mod } 8)$, $x \equiv 11 (\text{mod } 20)$, $x \equiv 1 (\text{mod } 15)$;
d) $x \equiv 1 (\text{mod } 3)$, $x \equiv 4 (\text{mod } 5)$, $x \equiv 2 (\text{mod } 7)$, $x \equiv 9 (\text{mod } 11)$, $x \equiv 3 (\text{mod } 13)$;
e) $3x + 4y - 29 \equiv 0 (\text{mod } 143)$, $2x - 9y + 84 \equiv 0 (\text{mod } 143)$.

4.3

P 22. (criterii de divizibilitate) Fie $n = \overline{a_k a_{k-1} \dots a_2 a_1 a_0}_{(10)}$ un număr natural nenul, cu $a_0, a_1, \dots, a_k \in \{0, 1, \dots, 9\}$. Atunci au loc următoarele congruenţe:
a) $n \equiv a_0 (\text{mod } 2, 5, 10)$;
b) $n \equiv \overline{a_1 a_0} (\text{mod } 4, 15, 100)$;
c) $n \equiv \overline{a_{l-1} \dots a_1 a_0} (\text{mod } 2^l, 5^l, 10^l)$;
d) $n \equiv a_0 + 2a_1 (\text{mod } 4)$;
e) $n \equiv a_0 + 2a_1 + 4a_2 (\text{mod } 8)$;
f) $n \equiv a_0 + a_1 + \dots + a_k (\text{mod } 3, 9)$;
g) $n \equiv a_0 - a_1 + \dots + (-1)^k a_k (\text{mod } 11)$;
h) Dacă $d \in \mathbb{N}^*$ este coprim cu 10, iar $m, m' \in \mathbb{N}^*$ au proprietatea că $10m \equiv 1 (\text{mod } d)$ şi $10m' \equiv -1 (\text{mod } d)$, atunci $d | n \iff d | \overline{a_k \dots a_2 a_1} + m a_0 \iff d | \overline{a_k \dots a_2 a_1} - m' a_0$;
i) $7 | n \iff 7 | \overline{a_k \dots a_2 a_1} + 5a_0 \iff 7 | \overline{a_k \dots a_2 a_1} - 2a_0$;
j) $13 | n \iff 13 | \overline{a_k \dots a_2 a_1} + 4a_0$;
k) $17 | n \iff 17 | \overline{a_k \dots a_2 a_1} - 5a_0$;
l) $19 | n \iff 19 | \overline{a_k \dots a_2 a_1} + 2a_0$;
m) $23 | n \iff 23 | \overline{a_k \dots a_2 a_1} + 7a_0$;
n) $29 | n \iff 29 | \overline{a_k \dots a_2 a_1} + 3a_0$;
p) $31 | n \iff 31 | \overline{a_k \dots a_2 a_1} - 3a_0$;
q) $7 (\text{sau } 11, \text{sau } 13) | n \iff 7 (\text{sau } 11, \text{sau } 13) | \overline{a_k \dots a_4 a_3} - \overline{a_2 a_1 a_0}$;
r) $27 (\text{sau } 37) | n \iff 27 (\text{sau } 37) | \overline{a_k \dots a_4 a_3} + \overline{a_2 a_1 a_0}$;
s) $11 | n \iff 11 | \overline{a_k \dots a_3 a_2} + \overline{a_1 a_0}$;
t) $101 | n \iff 101 | \overline{a_k \dots a_3 a_2} - \overline{a_1 a_0}$.

P 23. Determinaţi descompunerile în factori primi ale următoarelor numere naturale: 82798848, 81057226635000, 125!, 244943325, 282321246671737.

P 24. Determinaţi restul împărţirii numărului $\left(12371^{56}+34\right)^{28}$ prin 111.

4.4

P 25. Fie $a \in \mathbb{Z}$. Atunci:
a) $a^2 \equiv 0$ sau $1 \pmod 4$;
b) $a^2 \equiv 0$ sau $1 \pmod 3$;
c) $a^2 \equiv 0, 1$ sau $4 \pmod 5$;
d) $a^2 \equiv 0, 1, 2$ sau $4 \pmod 7$;
e) $a^3 \equiv 0, 1$ sau $6 \pmod 7$;
f) $a^3 \equiv 0, 1$ sau $8 \pmod 9$.

P 26. Fie $n \in \mathbb{N}$, $n \equiv 3 \pmod 4$. Arătaţi că nu există numere întregi a, b, astfel încât $n = a^2 + b^2$.

P 27. Fie $n \in \mathbb{N}$, $n \equiv 7 \pmod 8$. Arătaţi că nu există numere întregi a, b, c, astfel încât $n = a^2 + b^2 + c^2$.

P 28. Fie $n \in \mathbb{N}$, cu $(n, 6) = 1$. Arătaţi că $24 | n^2 - 1$.

P 29. Fie $m, n \in \mathbb{N}^*$, cu $\frac{m}{n} < \sqrt{7}$. Arătaţi că $\frac{m}{n} + \frac{1}{mn} < \sqrt{7}$.

P 30. Fie $x, y, z \in \mathbb{N}^*$. Arătaţi că $x^2 + y^2 = z^2$ dacă şi numai dacă există $k, m, n \in \mathbb{N}^*$, cu $m > n$, $(m, n) = 1$ şi $m \not\equiv n \pmod 2$, astfel că

$$\{x, y\} = \{2kmn, k(m^2 - n^2)\}, \quad z = k(m^2 + n^2).$$

P 31. Arătaţi că nu există $x, y, z \in \mathbb{N}^*$, astfel încât $x^4 + y^4 = z^2$.

4.5

P 32. Arătaţi că exponentul unui număr prim p în descompunerea în factori a numărului $n!$ este

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

P 33. Fie $p \in \mathbb{P}$ un număr prim, iar $n \in \mathbb{N}^*$ un număr natural a cărui scriere în baza p este $n = \overline{a_k a_{k-1} \dots a_2 a_1 a_0}_{(p)}$. Arătaţi că

$$v_p(n!) = \frac{n - (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0)}{p - 1}.$$

P 34. Cu câte zerouri se termină numărul 2021! ?

P 35. Arătaţi că dacă numărul $F_n = 2^n + 1$ este prim, atunci n este o putere a lui 2.

P 36. Arătaţi că $641 | 2^{32} + 1$.

P 37. Arătaţi că dacă numărul $M_n = 2^n - 1$ este prim, atunci n este prim.

P 38. Verificaţi că $2^{11} - 1 = 23 \cdot 89$.

4.6

P 39. Fie $p \in \mathbb{P}$ un număr prim, iar $a \in \{1, 2, \dots, p-1\}$. Arătaţi că simbolul lui Legendre verifică congruenţa

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

P 40. Fie $p \in \mathbb{P}$ un număr prim, iar $a, b, c \in \mathbb{Z}$, cu $a \notin p\mathbb{Z}$. Arătaţi că congruenţa

$$ax^2 + bx + c \equiv 0 \pmod p$$

are soluţii dacă şi numai dacă $\left(\frac{\Delta}{p}\right) = 1$, unde $\Delta = b^2 - 4ac$.