1 Deliteľnosť v obore celých čísel

1.1 Základné pojmy a ich vlastnosti

1. Zistite, či pre každé $a, b, c \in \mathbb{Z}$ platí:
   a) Ak $a \mid b + c$, tak $a \mid b$ alebo $a \mid c$.
   b) Ak $a \mid b + c$ a $a \mid b$, tak $a \mid c$.
   c) Ak $a \mid b.c$, tak $a \mid b$ alebo $a \mid c$.
   d) Ak $a \mid b$, tak $a \mid b.c$.

2. Nech $a, b \in \mathbb{Z}$ a existujú $u, v \in \mathbb{Z}$ také, že $1 = ua + vb$. Dokážte, že $(a, b) = 1$.

3. Vypočítajte (a, b) aj $[a, b]$, ak
   a) $a = 6320$, $b = 3780$
   b) $a = 10111$, $b = 7365$
   c) $a = 632$, $b = 642$
   d) $a = 819$, $b = 792$
   e) $a = 3366$, $b = 2508$
   [d) 9, 72072; e) 66,127908]

4. Nájdite všetky prirodzené čísla, ktoré sa škrtnutím poslednej cifry zmenšia štvornásobne (12-násobne).

5. Dokážte, že ak pre každé $i = 1, \dots, n$, $j = 1, \dots, m$, $(a_i, b_j) = 1$, tak $(a_1 \dots a_n, b_1 \dots b_m) = 1$.

6. Nájdite, ak existuje, aspoň jedno celočíselné riešenie rovnice:
   a) $193x + 18y = 2$, b) $196x + 105y = 84$, c) $17x + 21y = 1$, d) $196x + 105y = 1$

7. Nech $a, b, c \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$. Dokážte, že rovnica $ax + by = c$ má aspoň jedno celočíselné riešenie $\Leftrightarrow$ $(a, b) \mid c$. Ako vyzerá množina všetkých celočíselných riešení takejto rovnice?

8. K dispozícii je 30-litrová nádoba plná vody a 13l a 17l prázdne nádoby. Je možné odmerať 15l?

9. Je daný uhol $19°$. Je možné len pomocou pravítka a kružidla rozdeliť tento uhol na 19 rovnakých častí?

10. Určte počet všetkých prirodzených čísel menších ako 10^6, ktoré sú nesúdeliteľné s číslom a) 6, b) 30.

11. a) Dokážte, že ak $(a, b) = d$, $c \mid a$ a $c \mid b$, tak $c \mid d$.
    b) Nech $(a, b) = d$, $a = a'c$, $b = b'c$. Potom $d = d'c$ a platí $(a', b') = d'$. Dokážte!

12. Definujte n.s.d. pre tri celé čísla a, b, c (resp. pre $a_1, \dots, a_n$). Dokážte, že ak (a, b, c) označuje n.s.d. a, b, c, tak $(a, b, c) = ((a, b), c) = (a, (b, c))$.

13. Ak $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$ a $\frac{1}{a} + \frac{1}{b} \in \mathbb{Z}$, tak $a = b$ a $a = 1$ alebo $a = 2$. Dokážte!

14. Dokážte, že pre ľubovoľné $c, a, b \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$ platí:
    a) Ak $b \mid c$, tak $(a + c, b) = (a, b)$.
    b) Ak $(a, b) = 1$, tak $(a + b, a - b) = 1$ alebo 2.

15. Dokážte, že pre každé $a \in \mathbb{Z}$ je jedno z čísel a, $a+1$, $a+2$ (a, $a+2$, $a+4$) deliteľné číslom 3.

16. Ak $a, b, c \in \mathbb{Z}$ a $a^2 + b^2 = c^2$, tak a, b nemôžu byť súčasne nepárne.

17. Dokážte: Druhú mocninu každého prirodzeného čísla možno zapísať buď v tvare $4k+1$, alebo v tvare $4k$.

18. Je pravdivé tvrdenie: Ak $ab \mid c^2$, tak aspoň jedno z čísel a a b je deliteľom čísla c?

19. Nájdite najväčšieho spoločného deliteľa čísel: a) $2n+1$ a $2n-1$ b) n^2-1 a n^2+n, c) n^3-1 a n^2-1, d) n^3+2 a $n+1$.

20. Dokážte, že súčin štyroch po sebe idúcich prirodzených čísel je deliteľný 24.

1.2 Prvočísla

1. Dokážte, že ak $n \geq 2$ je zložené číslo a p je najmenšie prvočíslo, ktoré delí n, tak $p \leq \sqrt{n}$.

2. Zistite, či 283 (397) je prvočíslo.

3. Eratostenovo sito.

4. Nech $m > 1$. Dokážte, že najmenšie $k \in \mathbb{N}$, $k > 1$, ktoré delí m je prvočíslo.

5. Dokážte, že ak $2^n - 1$ je prvočíslo ($n \in \mathbb{N}$), tak n je prvočíslo. Ukážte, že obrátené tvrdenie neplatí. ($M_n = 2^n - 1$ - Mersenovo číslo[1]) [$M_{11} = 2^{11} - 1 = 2047$ nie je prvočíslo, $23 \mid M_{11}$.]

6. Dokážte, že ak $2^n + 1$ ($n \in \mathbb{N}$) je prvočíslo, tak existuje $m \in \mathbb{N}_0$ tak, že $n = 2^m$. Ukážte na príklade, že obrátený výrok neplatí. ($F_n = 2^{2^n} + 1$ - Fermatove čísla) [$F_5 = 2^{32} + 1$ nie je prvočíslo, $641 \mid F_5$[2].]

7. Dokážte, že pre každé $k \in \mathbb{N}$ existuje k po sebe nasledujúcich prirodzených čísel, ktoré sú všetky zložené čísla.

8. Dokážte, že pre každé $n \in \mathbb{N}$, $n > 2$ existuje prvočíslo p také, že $n < p < n!$

9. a) Dokážte, že ak $p > 3$ je prvočíslo, tak existuje $k \in \mathbb{N}_0$, pre ktoré $p = 6k+1$ alebo $p = 6k+5$.
   b) Nájdite všetky prvočísla p také, že $p+2$ aj $p+10$ sú tiež prvočísla.

10. Nech $a, b \in \mathbb{N}$, $a > 0$, $b > 0$ a $a.b = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad. Potom $a = p_1^{t_1} \dots p_k^{t_k}$, $b = p_1^{s_1} \dots p_k^{s_k}$, kde pre každé i $0 \leq t_i, s_i \leq l_i$. Dokážte, že $(a, b) = p_1^{u_1} \dots p_k^{u_k}$, kde $u_i = \min\{t_i, s_i\}$ pre všetky $i = 1, \dots, k$ a $[a, b] = p_1^{v_1} \dots p_k^{v_k}$, kde $v_i = \max\{t_i, s_i\}$ pre všetky $i = 1, \dots, k$.

11. Nájdite kanonické rozklady čísel 4725, 3718, 3234 a určte (4725,3718), [4725,3718], (3718,3234), [3718, 3234].

12. Nájdite všetky delitele čísel: a) 72, b) $11^5.17^2$.

[1] mních Mersenne 1644
[2] Euler 1930

13. Nájdite prirodzené číslo, ktoré je deliteľné číslom 2 a číslom 9 a má práve 14 deliteľov v $\mathbb{N}$.

14. Dokážte, že $n^4 + 4$ nie je prvočíslo pre $n \geq 2$, $5 \nmid n$.

15. Zistite, ktoré z uvedených čísel je rovné druhej mocnine nejakého prirodzeného čísla: a) $2^2.3^{12}.7^5$, b) $23^{12}.12^{13}$, c) 1234321, d) 157996443.

16. Zistite, koľkými nulami končí číslo a) 100!, b) 1000!

17. Aspoň dvojciferné číslo, ktorého všetky cifry sú rovnaké nie je druhou mocninou žiadneho prirodzeného čísla. Dokážte!

18*. Nájdite všetky prvočísla tvaru $\frac{n(n+1)}{2} - 1$, kde $n \in \mathbb{N}$.

19. Dokážte, že existuje nekonečne veľa prvočísel tvaru $6k - 1$ ($k \in \mathbb{N}$).

20. Ak p a $p + 2$ sú prvočíselné dvojčatá a $p > 3$, tak $6 \mid p + 1$. Dokážte!

21. Vypočítajte počet deliteľov čísla 324000.

22*. Koľko čísel menších ako $3^n 5^m$ je s číslom $3^n 5^m$ nesúdeliteľných?

23*. V rovnosti LIK $\times$ LIK = BUBLIK nahraďte každé písmeno cifrou tak, aby vznikla identita. (Rôznym písmenám zodpovedajú rôzne cifry.) Riešte tú istú úlohu pre rovnosť SUK $\times$ SUK = BARSUK. (Návod: všimnite si, že $1\,000 \mid$ LIK $\times$ (LIK $- 1$) a čísla LIK a LIK $- 1$ sú nesúdeliteľné.)

1.3 Číselné sústavy

1. Vyjadrite čísla 217, 1513, 2120 v a) 3-kovej, b) 5-kovej, c) 9-kovej sústave.

2. Vyjadrite číslo 12892 v 5-kovej a 6-kovej sústave a číslo $(10321)_4$ v desiatkovej sústave. [$12892 = (403032)_5 = (135404)_6$]

3. Vyjadrite čísla $(257)_8$, $(301)_4$ v dvojkovej sústave a čísla $(111100101)_2$, $(1100101)_2$ v štvorkovej a osmičkovej sústave.

4. Vyjadrite v dvojkovej sústave prvých 6 prvočísel.

5. Určte číslo n, pre ktoré platí $n = (a_1 a_0)_9 = (a_0 a_1)_{10}$.

6. Určte číslo n, pre ktoré platí $n = (a_1 a_0)_{10} = (a_1 a_0 2)_3$.

1.4 Kongruencie

Pojem kongruentnosti *mod n*, základné vlastnosti

1. Nájdite poslednú cifru čísla a) $213^{174} + 25^{17}$, b) $99^{99} + (7^{17})^{17}$, c) $127^{37} + 45^{131} + 109^{18}$.

2. Nájdite všetky prirodzené čísla n, pre ktoré a) $7 \mid 2^n - 1$, b) $7 \mid 2^n + 1$.

3. Nech $a, b \in \mathbb{Z}$. Dokážte, že $19 \mid 10a + b \Leftrightarrow 19 \mid a + 2b$.

4. Overte, či $19 \mid 539828$ s využitím predchádzajúcej úlohy.

5. Nech $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$. Dokážte, že ak $f(4)$ aj $f(5)$ je nepárne číslo, tak rovnica $ax^2 + bx + c = 0$ nemá celočíselné korene.

6. Dokážte, že pre každé $n \in \mathbb{N}$ platí: Ak $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, $k \in \mathbb{N}$ a pre každé $i = 1, \ldots, n$ $a_i \equiv b_i \,(mod\ k)$, tak $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \,(mod\ k)$ a $a_1 \ldots a_n \equiv b_1 \ldots b_n \,(mod\ k)$.

7. Určte poslednú cifru čísla $n = 22.51 + 698^5$ pri jeho vyjadrení v sedmičkovej sústave.

8. Ak $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$, $m \mid n$ a $a \equiv b \,(mod\ n)$, tak $a \equiv b \,(mod\ m)$. Dokážte!

9. Aký je zvyšok 167^{452} po delení 11?

Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel

1. Dokážte, že číslo $n = c_k 10^k + \ldots + c_1 10 + c_0$ je deliteľné číslom 27, resp. 37 $\Leftrightarrow$ 27 resp. 37 delí číslo $(c_0 + c_1 10 + c_2 10^2) + (c_3 + c_4 10 + c_5 10^2) + \ldots = c_2c_1c_0 + c_5c_4c_3 + \ldots$

2. Zistite, či čísla 149 688, 301 587, 10 291 698 sú deliteľné
a) číslom 3, resp. 9,
b) číslom 7, 11, resp. 13,
c) číslom 27, resp. 37.

3. Dokážte, že číslo $n = c_k 10^k + \ldots + c_1 10 + c_0$ je deliteľné číslom 101 $\Leftrightarrow$ číslo 101 delí číslo $(c_0 + c_1 10) - (c_2 + c_3 10) + (c_4 + c_5 10) - \ldots = c_1c_0 - c_3c_2 + c_5c_4 - \ldots$

4. Nech $p = 10^{m-1} + 10^{m-2} + \ldots + 10 + 1 = \overbrace{11\ldots1}^{m \text{ cifier}}$ je prvočíslo. Potom aj m je prvočíslo. Ukážte, že obrátené tvrdenie neplatí.

5. Dokážte, že číslo $n = c_k 10^k + \ldots + c_1 10 + c_0$ je deliteľné číslom 5 $\Leftrightarrow$ $c_0 = 5$ alebo $c_0 = 0$.

6. Nech $n = c_k 10^k + \ldots + c_1 10 + c_0$. Dokážte, že platí:
a) $4 \mid n \Leftrightarrow 4 \mid 10c_1 + c_0$ $(=c_1c_0)$
b) $8 \mid n \Leftrightarrow 8 \mid 10^2 c_2 + 10c_1 + c_0$ $(=c_2c_1c_0)$

7. Zistite, či je číslo $(7812)_9$ deliteľné ôsmimi a desiatimi.

8. Zistite, či je číslo $(1202)_6$ deliteľné dvomi a tromi.

1.5 Eulerova funkcia a Eulerova veta

1. Dokážte, že platí:
a) $42 \mid n^7 - n$ pre každé $n \in \mathbb{Z}$,
b) $7 \mid n^{6k} - 1$ pre každé $k \in \mathbb{N}$ a $n \in \mathbb{Z}$ také, že $(n, 7) = 1$,
c) $n^{13} - n$, $n \in \mathbb{Z}$ je deliteľné každým z čísel 2,3,5,7,13.

2. Ak p, q sú prvočísla, $p \neq q$, tak pre každé celé číslo a platí: $p.q \mid a^{p \cdot q} - a^p - a^q + a$.

3. Nájdite všetky riešenia rovnice $2^m - 3^n = 1$ v obore prirodzených čísel.

4. Dokážte, že ak $n \in \mathbb{N}$ a $(10, n) = 1$, tak existuje $k \in \mathbb{N}$ tak, že $k.n = 99\ldots9$ - má všetky cifry rovné 9.

5. Dokážte, že pre každé $n \in \mathbb{N}$ platí:
a) $n^{10} = 11k$ alebo $n^{10} = 11k + 1$
b) $n^{12} = 13k$ alebo $n^{12} = 13k + 1$
c) $n^{20} = 25k$ alebo $25k + 1$

6. Nech $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a, n) = 1$. Nech k je najmenšie prirodzené číslo, pre ktoré $a^k \equiv 1\,(mod\ n)$. Potom pre každé $l \in \mathbb{N}$ také, že $a^l \equiv 1\,(mod\ n)$ platí, že $k \mid l$. Špeciálne, $k \mid \varphi(n)$. Dokážte!

7. Nájdite najmenšie prirodzené číslo n tak, aby
a) $253^n \equiv 1\,(mod\ 257)$
b) $2^n \equiv 1\,(mod\ 257)$.

8. Dokážte, že ak p, q sú prvočísla a $p \neq q$, tak $p^{q-1} + q^{p-1} \equiv 1\,(mod\ pq)$ a $p^q + q^p \equiv p + q\,(mod\ pq)$.

9. Na príklade ukážte, že ak $(a, n) > 1$, tak nemusí platiť $a^{\varphi(n)} \equiv 1\,(mod\ n)$.

10. Nájdite najmenšie prirodzené číslo, pre ktoré platí $6x \equiv 1\,(mod\ 35)$.

11*. Nájdite najväčší spoločný deliteľ množiny čísel $\{n^{13} - n, n \in \mathbb{Z}\}$.

Použitie Eulerovej vety v kryptografii (šifrovaní)

1.6 Lineárne kongruencie s jednou neznámou

1. Vyriešte lineárne kongruencie s jednou neznámou:
a) $10x \equiv 14\,(mod\ 12)$
b) $7x \equiv 46\,(mod\ 21)$
c) $15x \equiv -72\,(mod\ 18)$
d) $14x \equiv -63\,(mod\ 35)$

2. Zistite, ktoré z nasledujúcich kongruencií sú riešiteľné: a) $6x \equiv 1\,(mod\ 9)$, b) $9x \equiv 3\,(mod\ 6)$, c) $14x \equiv 21\,(mod\ 70)$.

3. Riešte kongruencie: a) $20x \equiv 4\,(mod\ 30)$, b) $20x \equiv 30\,(mod\ 4)$, c) $353x \equiv 254\,(mod\ 400)$.

4. Do kongruencie $10x \equiv 15\,(mod\ n)$ doplňte za n také číslo, aby:
a) kongruencia nemala riešenie,
b) kongruencia mala práve 2 riešenia.

1.7 Aritmetické funkcie φ, τ, σ

1. Vypočítajte $\varphi(144)$, $\varphi(1000)$.

2. Vypočítajte $\sigma(144)$, $\sigma(1000)$.

3. Určte $\tau(2p^3)$ a $\sigma(2p^3)$, ak p je nepárne prvočíslo.

1.8 Doplnky. Lagrangeova a Wilsonova veta.

2 g-adické rozvoje reálnych čísel. Kritéria iracionálnosti.

2.1 g-adický rozvoj

2.2 Kritériá racionálnosti

1. Dokážte, že nasledujúce číslo sú iracionálne: a) $\sqrt{3}+\sqrt{5}$, b) $\sqrt{3}(\sqrt{6}-3)$, c)$\frac{4\sqrt{3}-3}{6}$, d)$\sqrt{3}-\sqrt{2}$, e) $\sqrt[3]{3}+\sqrt{2}$, f) $\log 2+\log 3$.

2. Nech $r=\frac{c}{d}$, $(c,d)=1$, $d,c\in\mathbb{Z}$, je racionálny koreň rovnice $a_kx^k+a_{k-1}x^{k-1}+\dots a_0=0$, pričom $a_0,\dots,a_k\in\mathbb{Z}$, $a_k\neq 0$. Dokážte, že potom $c\mid a_0$ a $d\mid a_k$. Z toho dostaneme, že pre rovnicu $x^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0=0$, $a_i\in\mathbb{Z}$ platí: Každý racionálny koreň tejto rovnice je celé číslo.

3. Nájdite 5-adický rozvoj nasledujúcich čísel: $\frac{35}{11}$, $\frac{13}{9}$, $\frac{1}{24}$.

4. Nájdite celé čísla a, b tak, aby a) $\frac{a}{b}=0,123$, b) $\frac{a}{b}=2,1\overline{25}$, a) $\frac{a}{b}=3,\overline{9157}$.

5. Nájdite $a,b\in\mathbb{Z}$ tak, aby
   a) $\frac{a}{b}=2+\frac{1}{5}+\frac{3}{5^2}+\frac{1}{5^3}+\frac{3}{5^4}+\frac{1}{5^5}+\frac{3}{5^6}+\ldots=(2,131313\ldots)_5$
   b) $\frac{p}{q}=3+\frac{2}{7}+\frac{3}{7^2}+\frac{3}{7^3}+\frac{3}{7^4}+\ldots=(3,23333\ldots)_7$.