

Elementárna teória čísel

11. marca 2019

Obsah

1	Deliteľnosť v obore celých čísel	3
1.1	Základné pojmy a ich vlastnosti	3
1.2	Prvočísla	9
1.3	Číselné sústavy	14
1.4	Kongruencie	15
1.4.1	Pojem kongruentnosti <i>mod</i> n , základné vlastnosti	15
1.4.2	Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel . . .	19
1.5	Eulerova funkcia a Eulerova veta	21
1.5.1	Použitie Eulerovej vety v kryptografii (šifrovaní)	24
1.6	Lineárne kongruencie s jednou neznámou	25
1.7	Aritmetické funkcie φ , τ , σ	26
1.8	Doplňky. Lagrangeova a Wilsonova veta.	29
2	g-adické rozvoje reálnych čísel. Kritéria iracionálnosti.	31
2.1	g -adický rozvoj reálneho čísla	31
2.2	Kritériá racionálnosti	34

Úvod

Verzia: 11. marca 2019

Obsah predmetu

I. Deliteľnosť v obore celých čísel

1. Základné pojmy, najväčší spoločný deliteľ, Euklidov algoritmus, najmenší spoločný násobok.
2. Prvočísla a ich vlastnosti, základná veta aritmetiky, prvočíselná veta.
3. Číselné sústavy, vyjadriteľnosť prirodzeného čísla v g -adickej sústave.
4. Kongruencie, základné vlastnosti relácie kongruentnosti modulo n , použitie kongruencií pri kritériách deliteľnosti prirodzených čísel, Eulerova funkcia, Eulerova veta a jej využitie, lineárne kongruencie s jednou neznámou.
5. Aritmetické funkcie φ , τ , σ a ich vlastnosti.

II. g -adické rozvoje reálnych čísel, kritériá iracionálnosti reálnych čísel

1. Pojem racionálneho a iracionálneho čísla, vyjadriteľnosť reálneho čísla pomocou g -adického rozvoja.
2. Periodické g -adické rozvoje, kritérium racionálnosti reálneho čísla vyjadreného v g -adickom rozvoji. Ďalšie kritériá racionálnosti ($\sqrt[n]{k}$, $n, k \in \mathbb{N}$, $n \geq 2$; $\log r$, $r \in \mathbb{Q}^+$).

Kapitola 1

Deliteľnosť v obore celých čísel

1.1 Základné pojmy a ich vlastnosti

Označenia:

$\mathbb{Z}$ = množina všetkých celých čísel

$\mathbb{N}$ = množina všetkých prirodzených čísel

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

Ak A je konečná množina, tak $|A|$ označuje počet prvkov množiny A .

V celej kapitole číslo znamená celé číslo.

Definícia 1.1.1. Nech $a, b \in \mathbb{Z}$. Hovoríme, že a delí b , ak existuje $c \in \mathbb{Z}$ tak, že $b = c.a$.
Označenie: $a \mid b$ ($a \nmid b$ je negácia $a \mid b$).

Príklad. $-2 \mid 6$, $2 \mid -2$, $0 \mid 0$, $2 \nmid 3$

Veta 1.1.2. Pre ľubovoľné $a, b, c \in \mathbb{Z}$ platí:

- (1) $a \mid a$
- (2) Ak $a \mid b$ a $b \mid c$, tak $a \mid c$.
- (3) $1 \mid a$
- (4) $a \mid 0$
- (5) $b \mid a \Leftrightarrow -b \mid a \Leftrightarrow b \mid -a \Leftrightarrow -b \mid -a$
- (6) $b \mid a \Leftrightarrow |b| \mid |a| \Leftrightarrow b \mid |a| \Leftrightarrow |b| \mid a$
- (7) Ak $a \mid b$, tak $a.c \mid b.c$.
- (8) Ak $a.c \mid b.c$ a $c \neq 0$, tak $a \mid b$.
- (9) Ak $a \mid b$, $a \mid c$, tak pre každé $d, d' \in \mathbb{Z}$ $a \mid d.b \pm d'.c$.
- (10) Ak $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

Dôkaz. (5) Ak $b \mid a$, tak existuje $c \in \mathbb{Z}$, pre ktoré $a = c.b$. Potom $a = (-c).(-b)$, $-c \in \mathbb{Z}$, a preto $-b \mid a$. Ak $-b \mid a$, tak $-(-b) \mid a$, a teda $b \mid a$. Ostatné ekvivalencie sa dokážu podobne.

(9) Ak $a \mid b$ a $a \mid c$, tak existujú $b', c' \in \mathbb{Z}$ pre ktoré $b = b'a$ a $c = c'a$. Potom $db + d'c = db'a + d'c'a = (db' + d'c')a$, a teda $a \mid db + d'c$.

(10) Ak $a \mid b$, tak existuje $c \in \mathbb{Z}$, pre ktoré $b = ca$. Ak $b \neq 0$, tak aj $c \neq 0$ aj $a \neq 0$, a preto $|c| > 0$ aj $|a| > 0$. Pretože $|c| > 0$, máme $1 \leq |c|$. Potom ale $|a| \leq |c||a| = |ca| = |b|$. $\square$

Veta 1.1.3 (o delení so zvyškom). Pre každé $z \in \mathbb{Z}$ a každé $n \in \mathbb{N}$ existuje práve jedna dvojica $(k, q) \in \mathbb{Z} \times \mathbb{Z}$ taká, že $z = kn + q$ a $0 \leq q < n$.

Dôkaz. Existencia. Najprv dokážeme, že veta platí pre každé $z \in \mathbb{N}_0$ a $n \in \mathbb{N}$ indukciou vzhľadom na z .

Pre $z = 0$ $(k, q) = (0, 0)$. $0 = 0n + 0$, $0 \leq 0 < n$.

Nech tvrdenie platí pre $z \geq 0$, dokážeme, že potom platí aj pre $z + 1$.

Teda platí $z = kn + q$, $0 \leq q < n$. Potom $z + 1 = kn + q + 1$. Pretože $0 \leq q < n$, platí $0 < q + 1 \leq n$. Ak $q + 1 = n$, tak máme $z + 1 = (k + 1)n + 0$. Ak $q + 1 < n$, tak máme $z + 1 = kn + (q + 1)$, $0 \leq q + 1 < n$. Teda existencia je dokázaná pre každé $z \geq 0$.

Nech teraz $z < 0$. Potom $-z > 0$ a teda existuje $(k, q) \in \mathbb{Z} \times \mathbb{Z}$ tak, že $-z = kn + q$, $0 \leq q < n$. Ak $q = 0$, tak $z = -kn + 0$, $0 \leq 0 < n$. Ak $q > 0$, tak $q = n - (n - q)$ a $0 < n - q < n$. Potom $z = -kn - q = (-k)n - n + (n - q) = (-k - 1)n + (n - q)$, $0 \leq n - q < n$.

Jednoznačnosť. Nech $z = kn + q = k'n + q'$, $0 \leq q < n$, $0 \leq q' < n$. Nech napríklad $q' \leq q$ (prípád $q \leq q'$ je podobný). Potom $q - q' = (k' - k)n$ a teda $n \mid q - q'$. Ak $q - q' > 0$, tak potom $n \leq q - q' \leq q < n$ - spor. Teda $q - q' = 0$, a preto $q = q'$. Potom $(k - k')n = 0$, a preto aj $k = k'$. $\square$

V problematike deliteľnosti v obore celých čísel hrá dôležitú úlohu pojem najväčší spoločný deliteľ.

Definícia 1.1.4. a) Číslo $c \in \mathbb{Z}$ sa nazýva *spoločný deliteľ* čísel $a, b \in \mathbb{Z}$, ak $c \mid a$ a súčasne $c \mid b$.

b) Najväčší prvok množiny všetkých spoločných deliteľov čísel a, b sa nazýva *najväčší spoločný deliteľ* (n.s.d.) čísel a, b . Označenie: $d = (a, b)$.

c) Čísla $a, b \in \mathbb{Z}$ sa nazývajú *nesúdeliteľné* (súdeliteľné), ak $(a, b) = 1$ ($(a, b) \neq 1$).

Príklad. a) 1 je spoločný deliteľ pre ľubovoľné $a, b \in \mathbb{Z}$ a teda $(a, b) \geq 1$.

b) $(-4, -6) = 2$ a teda $-4, -6$ sú súdeliteľné.

c) $(2, -3) = 1$ a teda 2, -3 sú nesúdeliteľné.

d) Pre každé $a, b \in \mathbb{Z}$ $(a, b) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|)$.

e) Ak $a \neq 0$, tak $(0, a) = |a|$.

f) Ak $a \mid b$ a $a \neq 0$, tak $(a, b) = |a|$.

g) $(a, b) = (b, a)$

h) $(0, 0)$ neexistuje.

Veta 1.1.5. Pre každé $a, b \in \mathbb{Z}$, pre ktoré $a \neq 0$ alebo $b \neq 0$, existuje práve jeden najväčší spoločný deliteľ d .

Dôkaz. Nech $N_{a,b} = \{n \in \mathbb{N}; n \mid a \text{ a súčasne } n \mid b\}$. $1 \in N_{a,b}$ a teda $N_{a,b} \neq \emptyset$. Nech napríklad $a \neq 0$. Pretože každé $n \in N_{a,b}$ delí a , platí $n \leq |a|$. Teda $N_{a,b}$ je zhora ohraňovaná číslom a . Potom ale $N_{a,b}$ má najväčší prvok d , t.j. $d = (a, b)$. Ak $(a, b) = d$ a $(a, b) = d'$, tak $d \leq d'$ a súčasne $d' \leq d$. Teda $d' = d$. $\square$

V nasledujúcom ukážeme, že existuje metóda pre výpočet najväčšieho spoločného deliteľa pre ľubovoľné $a, b \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$. Najprv dokážeme jedno pomocné tvrdenie:

Lema 1.1.6. Nech $a, b, c, c' \in \mathbb{Z}$, $b \neq 0$ a $a = c'b + c$. Potom $(a, b) = (b, c)$.

Dôkaz. Nech $d = (a, b)$, $d' = (b, c)$. Pretože $d \mid a, b$ a $c = a + (-c')b$, platí tiež $d \mid c$. Pretože $d \mid b, c$, dostávame, že $d \leq d'$. Podobne, pretože $d' \mid b, c$ a $a = c'b + c$, platí $d' \mid a$. Pretože $d' \mid a, b$, dostávame $d' \leq d$. Teda $d = d'$. $\square$

Veta 1.1.7 (výpočet najväčšieho spoločného deliteľa). *Nech $a, b \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$. Potom platí:*

- (1) (a) Ak $a \mid b$, tak $(a, b) = |a|$, ak $b \mid a$, tak $(a, b) = |b|$.
 (b) Ak $a \nmid b$ a $b \nmid a$, tak (a, b) vypočítame pomocou Euklidovho algoritmu.
- (2) Ak $d = (a, b)$, tak existujú $r, s \in \mathbb{Z}$ také, že

$$d = ra + sb.$$

Dôkaz. (1a) Ak $a \mid b$ a $a \neq 0$ alebo $b \neq 0$, tak $a \neq 0$. Potom zrejme $(a, b) = |a|$. ($|a| \mid a, b$; ak $d \mid a, b$, tak $d \leq |a|$.)

(2a) Ak $(a, b) = |a|$, tak $|a| = 1a + 0b$, ak $a > 0$, resp. $|a| = (-1)a + 0b$, ak $a < 0$. Podobne pre $b \mid a$.

(1b) Nech $a \nmid b$ a súčasne $b \nmid a$. Potom $a \neq 0$ aj $b \neq 0$ a platí $(a, b) = (|a|, |b|)$. Nech $a_0 = |a|$, $a_1 = |b|$. Potom $a_0, a_1 \in \mathbb{N}$ a podľa vety 1.1.3 existujú $b_1, a_2 \in \mathbb{Z}$ tak, že $a_0 = b_1 a_1 + a_2$, $0 < a_2 < a_1$; platí tiež (lema 1.1.6)

$$(a_0, a_1) = (a_1, a_2).$$

Ďalej existujú $b_2, a_3 \in \mathbb{Z}$ tak, že

$$a_1 = b_2 a_2 + a_3, \quad 0 \leq a_3 < a_2, \quad (a_1, a_2) = (a_2, a_3).$$

Ak $a_3 = 0$, tak $(a_2, a_3) = a_2 = (a_1, a_2) = (a_0, a_1)$. Ak $a_3 > 0$, tak pokračujeme ďalej. Platí $a_1 > a_2 > a_3 > 0$. Ak v k -tom kroku dostaneme

$$a_{k-1} = b_k a_k + a_{k+1}, \quad 0 \leq a_{k+1} < a_k \text{ a } a_{k+1} > 0,$$

tak existujú b_{k+1}, a_{k+2} tak, že

$$a_k = b_{k+1} a_{k+1} + a_{k+2}, \quad 0 \leq a_{k+2} < a_{k+1}.$$

Týmto dostaneme klesajúcu postupnosť $a_1 > a_2 > \dots > a_k > a_{k+1} > \dots$ celých nezáporných čísel, ktorá nemôže byť nekonečná. Preto existuje $l \in \mathbb{N}$ tak, že $a_l > 0$ a $a_{l+1} = 0$.

$$\begin{aligned} a_{l-2} &= b_{l-1} a_{l-1} + a_l \\ a_{l-1} &= b_l a_l + 0. \end{aligned}$$

Potom $a_l = (a_{l-1}, a_l) = (a_{l-2}, a_{l-1}) = \dots = (a_2, a_1) = (a_1, a_0) = (a, b)$.

Uvedený postup sa nazýva *Euklidov algoritmus* a posledný nenulový zvyšok v tomto postupe je n.s.d. a, b .

(2) Využijeme Euklidov algoritmus, kde $a_l = (a_0, a_1)$. $a_l = a_{l-2} + (-b_{l-1})a_{l-1} = a_{l-2} + (-b_{l-1})(a_{l-3} + (-b_{l-2})a_{l-2}) = (-b_{l-1})a_{l-3} + (1 + b_{l-1}b_{l-2})a_{l-2} = \dots = ua_0 + va_1$, $u, v \in \mathbb{Z}$, teda $a_l = u|a| + v|b|$.

Ak $a > 0$, $b > 0$, tak $a_l = ua + vb$.

Ak $a < 0$, $b > 0$, tak $a_l = (-u)a + vb$.

Ak $a > 0$, $b < 0$, tak $a_l = ua + (-v)b$.

Ak $a < 0$, $b < 0$, tak $a_l = (-u)a + (-v)b$. □

Príklad. Určte $d = (-819, 792)$ a nájdite u, v také, že $d = u(-819) + v792$.
 $|-819| = 819, |792| = 792$

$$\begin{array}{ll} 819 : 792 = 1 & 819 = 1 \cdot 792 + 27 \\ 27 & \\ 792 : 27 = 29 & 792 = 29 \cdot 27 + 9 \\ 252 & \\ 9 & \\ 27 : 9 = 3 & (-819, 792) = 9 \\ 0 & \end{array}$$

$$9 = 792 + (-29) \cdot 27 = 792 + (-29)(810 + (-1)792) = (-29)819 + (1 + 29)792 = 29(-819) + 30 \cdot 792$$

Veta 1.1.8. Nech $a, b, c \in \mathbb{Z}$. Potom platí:

- (1) Ak $(a, b) = 1$, $a_1, b_1 \in \mathbb{Z}$, $a_1 \mid a$, $b_1 \mid b$, tak $(a_1, b_1) = 1$.
- (2) Ak $(a, b) = 1$ a $a \mid bc$, tak $a \mid c$.
- (3) Ak $(a, b) = 1$, $a \mid c$, $b \mid c$, tak $ab \mid c$.
- (4) Ak $(a, b) = 1$, $(a, c) = 1$, tak $(a, bc) = 1$.
- (5) Ak $(a, b) = 1$, $m, n \in \mathbb{N}$, tak $(a^m, b^n) = 1$.
- (6) Ak $(a, b) = d$, $a = a'd$, $b = b'd$, tak $(a', b') = 1$.

Dôkaz. (1) Pretože $(a, b) = 1$, existujú $u, v \in \mathbb{Z}$, pre ktoré $1 = ua + vb$. Nech $r \in \mathbb{Z}$ a $r \mid a_1$, $r \mid b_1$. Potom $r \mid a$, $r \mid b$ a preto $r \mid ua + vb = 1$. Preto $|r| \leq 1$ a teda aj $r \leq 1$.

(2) Existujú $u, v \in \mathbb{Z}$, pre ktoré $1 = ua + vb$ a $b' \in \mathbb{Z}$, pre ktoré $bc = b'a$. Potom $c = c(ua + vb) = cua + cvb = cua + vb'a = \underbrace{(cu + vb')}_\in \mathbb{Z} a$. Teda $a \mid c$.

(3) Existujú $u, v, a', b' \in \mathbb{Z}$ tak, že platí $1 = ua + vb$, $c = a'a$, $c = b'b$. Potom $c = c1 = c(ua + vb) = uac + vbc = uab'b + vba'a = (ub' + va')ab$. Teda $ab \mid c$.

(4) Existujú $u, v, u', v' \in \mathbb{Z}$ tak, že $1 = ua + vb$, $1 = u'a + v'c$. Potom $1 = 1 \cdot 1 = (ua + vb)(u'a + v'c) = (uu'a + vbu' + uv'c)a + vv'bc$, $uu'a + vbu' + uv'c, vv'bc \in \mathbb{Z}$. Pre každé $d \in \mathbb{Z}$ platí: ak $d \mid a$ a $d \mid bc$, tak $d \mid 1$ (veta 1.1.2(9)), a preto $d \leq |d| \leq 1$. Teda $1 = (a, bc)$.

(5) Vyplýva z (3), dokáže sa matematickou indukciou. Najprv sa dokáže, že ak $(a, b) = 1$, tak pre všetky $n \in \mathbb{N}$ $(a, b^n) = 1$.

(6) Existujú $u, v \in \mathbb{Z}$ $d = ua + vb$. Potom $d = ua'd + vb'd = (ua' + vb')d$. Pretože $d \neq 0$, máme $1 = ua' + vb'$. Pre každé $d \in \mathbb{Z}$, ak $d \mid a'$, $d \mid b'$, tak $d \mid 1$, a preto $d \leq |d| \leq 1$. Teda $(a', b') = 1$. $\square$

Príklad. a) Vyjadrite číslo $\frac{819}{792}$ v základnom tvare, t.j. v tvare $r = \frac{a}{b}$, kde $(a, b) = 1$ a $b \neq 0$.
 $(819, 792) = 9, 819 : 9 = 91, 792 : 9 = 88, (91, 88) = 1, r = \frac{91}{88}$

b) Nájdite aspoň jedno celočíselné riešenie rovnice $819x + 792y = 27$.
 $819(-29) + 792 \cdot 30 = 9 \quad / : 3$
 $819(-87) + 792 \cdot 90 = 27$

Jedno riešenie je $(-87, 90)$. Popíšeme ako vyzerajú všetky riešenia tejto rovnice. Pre ľubovoľné riešenie platí $819(x+87) + 792(y-90) = 0$. Označme $v = x+87$ a $u = y-90$, máme potom $819u + 792v = 0$. Predelením 9 dostaneme $88u + 91v = 0$, čiže $v = -\frac{88}{91}u$. Keďže 88 a 91 sú nesúdeliteľné, musí platiť $91 \mid u$, $u = 91k$. Z toho dostaneme $v = -88k$. Teda ľubovoľné riešenie má tvar $(-87-88k, 90+91k)$. Množina všetkých riešení je $\{(-87-88k, 90+91k); k \in \mathbb{Z}\}$.

V časti b) predchádzajúceho príkladu sme ukázali, ako sa rieši lineárna diofantická rovnica s dvoma neznámymi. Vo všeobecnosti má lineárna diofantická rovnica s dvoma neznámymi tvar $ax + by = c$, kde $a, b, c \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$. Riešením takejto rovnice je usporiadaná dvojica $(u, v) \in \mathbb{Z} \times \mathbb{Z}$, pre ktorú platí $au + bv = c$. Vyriešiť lineárnu diofantickú rovnicu znamená nájsť množinu všetkých jej celočíselných riešení.

Veta 1.1.9. *Nech $ax + by = c$ je lineárna diofantická rovnica s dvoma neznámymi, t. j. $a, b, c \in \mathbb{Z}$, $a \neq 0$ alebo $b \neq 0$, nech $d = (a, b)$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ (zrejme $a_1, b_1 \in \mathbb{Z}$ a podľa predchádzajúcej vety $(a_1, b_1) = 1$). Potom platí:*

a) *Daná rovnica $ax + by = c$ má aspoň jedno celočíselné riešenie vtedy a len vtedy, keď $d \mid c$.*

b) *Ak (u_0, v_0) je jedno (ľubovoľné) riešenie rovnice $ax + by = c$, tak $S = \{(u_0 - kb_1, v_0 + ka_1) : k \in \mathbb{Z}\}$ je množina všetkých celočíselných riešení tejto rovnice.*

Dôkaz. a) Nech rovnica $ax + by = c$ má celočíselné riešenie (u_0, v_0) . Potom $au_0 + bv_0 = c$ a pretože $d \mid a$ a $d \mid b$ platí tiež, že $d \mid au_0 + bv_0 = c$.

Obrátene, nech $d \mid c$, t. j. existuje $c_1 \in \mathbb{Z}$ tak, že $c = c_1 d$. Pretože $d = (a, b)$, existujú $r, s \in \mathbb{Z}$ také, že $d = ar + bs$. Potom $arc_1 + bsc_1 = dc_1 = c$ a teda (rc_1, sc_1) je celočíselné riešenie rovnice $ax + by = c$.

b) Nech $(u_0 - kb_1, v_0 + ka_1) \in S$. Potom $a(u_0 - kb_1) + b(v_0 + ka_1) = au_0 + bv_0 - (da_1 kb_1 - db_1 ka_1) = c$ a teda $(u_0 - kb_1, v_0 + ka_1)$ je riešenie rovnice $ax + by = c$.

Nech teraz (u, v) je celočíselné riešenie rovnice $ax + by = c$. Potom $d(a_1(u - u_0) + b_1(v - v_0)) = au + bv - (au_0 + bv_0) = c - c = 0$ a, pretože $d \neq 0$, dostávame $a_1(u - u_0) + b_1(v - v_0) = 0$. Nech napríklad $a \neq 0$ a teda aj $a_1 \neq 0$. Potom $a_1(u - u_0) = -b_1(v - v_0)$ ($u - u_0, v - v_0 \in \mathbb{Z}$) a preto $a_1 \mid b_1(v - v_0)$. Ale $(a_1, b_1) = 1$ a preto $a_1 \mid v - v_0$. Potom existuje $k \in \mathbb{Z}$, pre ktoré platí $v - v_0 = ka_1$ a teda aj $v = v_0 + ka_1$. Ďalej platí $a_1(u - u_0) = -b_1(v - v_0) = -b_1 ka_1$ a pretože $a_1 \neq 0$, dostávame $u - u_0 = -kb_1$ a preto $u = u_0 - kb_1$. Teda existuje $k \in \mathbb{Z}$ tak, že $(u, v) = (u_0 - kb_1, v_0 + ka_1)$ a preto $(u, v) \in S$. Ak $a = 0$, tak $b \neq 0$ a postupujeme podobne ako v prípade, keď $a \neq 0$.

□

Definícia 1.1.10. Nech $a, b \in \mathbb{Z}$. Číslo $c \in \mathbb{Z}$ sa nazýva *spoločný násobok* čísel a, b , ak $a \mid c$ aj $b \mid c$. Najmenšie prirodzené číslo n , ktoré je spoločným násobkom a, b sa nazýva *najmenší spoločný násobok* (n.s.n.) čísel a, b . Označenie: $[a, b]$.

Príklad. $[4, 6] = [-4, -6] = 12$

Pre ľubovoľné $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ platí $[a, b] = [|a|, |b|]$.

Veta 1.1.11.

(1) *Nech $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Potom existuje práve jedno $k \in \mathbb{N}$ také, že $k = [a, b]$.*

(2) *Ak $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, tak $(a, b)[a, b] = |a||b|$.*

Dôkaz. (1) Nech $K_{a,b} = \{n \in \mathbb{N}; a \mid n \text{ a súčasne } b \mid n\}$. Pretože $|a||b| \in K_{a,b}$, platí $K_{a,b} \neq \emptyset$. Potom ale existuje najmenší prvok k množiny $K_{a,b}$. Zrejme $k = [a, b]$. Ak $[a, b] = k$, $[a, b] = k'$, tak $k \leq k'$ a súčasne $k' \leq k$ a teda $k = k'$.

(2) Označme $d = (a, b)$, $k = [a, b]$. Existujú $a', b' \in \mathbb{Z}$ $a = da'$, $b = db'$. Potom (veta 1.1.8(5)) $(a', b') = 1$. Ďalej $|a| = d|a'|$, $|b| = d|b'|$, $(|a'|, |b'|) = 1$.

$$|a||b| = d|a'|d|b'| = dd|a'||b'|$$

Stačí teraz overiť, že $d|a'||b'| = k$.

$d|a'||b'| = |a||b'| \Rightarrow |a| \mid d|a'||b'| \Rightarrow a \mid d|a'||b'|$. Podobne pre b .

Nech teraz $m \in \mathbb{N}$ a $a \mid m$ aj $b \mid m$. Potom (pretože $d \mid a$) $d \mid m$ a teda existuje $m' \in \mathbb{N}$ také, že $m = dm'$.

Pretože $a \mid m$, máme $|a| = d|a'| \mid m = dm'$. Pretože $d \neq 0$, máme $|a'| \mid m'$.

Podobne sa ukáže, že $|b'| \mid m'$. Pretože $(|a'|, |b'|) = 1$, platí tiež $|a'||b'| \mid m$. Potom ale $d|a'||b'| \mid dm' = m$. Teda $d|a'||b'| = [a, b] = k$. $\square$

Príklad. Určte $c = [-819, 792]$.

Vieme, že $(-819, 792) = 9$. Potom $c = \frac{819 \cdot 792}{9} = 792 \cdot 91 = 72\,072$.

Teda $[-819, 792] = 72\,072$

Cvičenia

- Zistite, či pre každé $a, b, c \in \mathbb{Z}$ platí:
 - Ak $a \mid b + c$, tak $a \mid b$ alebo $a \mid c$.
 - Ak $a \mid b + c$ a $a \mid b$, tak $a \mid c$.
 - Ak $a \mid b \cdot c$, tak $a \mid b$ alebo $a \mid c$.
 - Ak $a \mid b$, tak $a \mid b \cdot c$.
- Nech $a, b \in \mathbb{Z}$ a existujú $u, v \in \mathbb{Z}$ také, že $1 = ua + vb$. Dokážte, že $(a, b) = 1$.
- Vypočítajte (a, b) aj $[a, b]$, ak
 - $a = 6320$, $b = 3780$
 - $a = 10111$, $b = 7365$
 - $a = 632$, $b = 642$
 - $a = 819$, $b = 792$
 - $a = 3366$, $b = 2508$
 [d) 9, 72072; e) 66,127908]
- Nájdite všetky prirodzené čísla, ktoré sa škrtnutím poslednej cifry zmenšia štvornásobne (12-násobne).
- Dokážte, že ak pre každé $i = 1, \dots, n$, $j = 1, \dots, m$, $(a_i, b_j) = 1$, tak $(a_1 \dots a_n, b_1 \dots b_m) = 1$.
- Nájdite, ak existuje, aspoň jedno celočíselné riešenie rovnice:
 - $193x + 18y = 2$, b) $196x + 105y = 84$, c) $17x + 21y = 1$, d) $196x + 105y = 8$
- Dokážte, že ak $a, b, c \in \mathbb{Z}$, $(a, b) = k$, $(a, c) = m$ a $(b, c) = 1$, tak $(a, bc) = km$.
- K dispozícii je 30-litrová nádoba plná vody a 13l a 17l prázdne nádoby. Je možné odmerať 15l?
- 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 $(a, b) = d$, $0 < c$, $a = a'c$, $b = b'c$. Potom $d = d'c$ a platí $(a', b') = d'$. Dokážte!
c) Nech $(a, b) = d$, $k \in \mathbb{N}$. Potom $(ak, bk) = dk$. Dokážte!
12. Definujte n.s.d. pre tri celé čísla a, b, c resp. pre $a_1, \dots, a_n$. Označenia: (a, b, c) , resp. $(a_1, \dots, a_n)$. Dokážte, že platí:
a) $(a, b, c) = ((a, b), c) = (a, (b, c))$,
b) Ak $n \geq 2$, $a_1, \dots, a_n, a_{n+1} \in \mathbb{Z}$, $d_1 = (a_1, \dots, a_n)$, $d = (d_1, a_{n+1})$, tak $d = (a_1, \dots, a_n, a_{n+1})$.
c) Ak $d = (a_1, \dots, a_n)$, tak existujú $u_1, \dots, u_n \in \mathbb{Z}$ tak, že $d = u_1.a_1 + \dots + u_n.a_n$.
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 $4k$, $k \in \mathbb{N}_0$.
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 ($n \in \mathbb{N}$): 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

(Pytagoras 6.stor.p.n.l., Euklides 365-300 p.n.l., Eratostenes 276-194 p.n.l.)

Definícia 1.2.1. Prirodzené číslo $p > 1$ sa nazýva *prvočíslo*, ak má práve dva rôzne kladné delitele a to 1 a p (hovoríme im aj triviálne delitele). Číslo $m > 1$ sa nazýva *zložené číslo*, ak m nie je prvočíslo, t.j. existuje $k \in \mathbb{N}$, $1 < k < m$ tak, že $k \mid m$ (ekvivalentne, existujú $k, l \in \mathbb{N}$, $1 < k, l < m$ také, že $m = kl$).

Príklad. a) 1 nie je ani prvočíslo ani zložené číslo.

b) 2, 3, 5, 7, 11, 13, 17, 19, ..., 1 000 000 009 649, 1 000 000 009 651, ..., $2^{20\,996\,011} - 1$, ... sú prvočísla. $2^{216\,091} - 1$ bolo v r. 1985 najväčšie známe prvočíslo, má 65 050 čífer v desiatkovej sústave.

c) 4, 6, 21, každé párne číslo $n > 2$ sú zložené čísla.

Veta 1.2.2 (Vlastnosti prvočísel). Nech p, q sú prvočísla. Potom platí:

- (1) Pre každé $a \in \mathbb{Z}$, $(a, p) = 1$ alebo $(a, p) = p$.
- (2) Pre ľubovoľné $a, b \in \mathbb{Z}$ ak $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.

(3) Ak $p \neq q$, tak $(p, q) = 1$.

(4) Ak $p \neq q$, tak pre každé $m, n \in \mathbb{N}$ $(p^m, q^n) = 1$.

Dôkaz. (1) $(a, p) = d \in \mathbb{N}$, $d \mid p$, a preto $d = 1$ alebo $d = p$.

(2) Nepriamo. Nech $p \nmid a$ a súčasne $p \nmid b$. Potom $(a, p) = 1$ aj $(b, p) = 1$. Potom ale $(ab, p) = 1$, a preto $p \nmid ab$.

(3) Vyplýva z (1).

(4) Vyplýva z vety 1.1.8(4). □

Veta 1.2.3 (Základná veta aritmetiky). Pre každé $n \geq 2$ existuje $k \in \mathbb{N}$ a prvočísla $p_1, \dots, p_k$ tak, že $n = p_1 \dots p_k$. Toto vyjadrenie je jednoznačné, až na poradie činiteľov.

Dôkaz. Existencia. Matematickou indukciou 2. typu.

$n = 2$. Tu $k = 1$, $p_1 = 2$ t.j. $2 = 2$ je žiadané vyjadrenie.

Nech $n > 2$ a výrok platí pre všetky m , $2 \leq m < n$. Ak n je prvočíslo, potom $k = 1$, $p_1 = n$, t.j. $n = n$ je žiadané vyjadrenie. Ak n je zložené číslo, tak existujú $m, l \in \mathbb{N}$, $1 < m, l < n$ také, že $n = ml$. Pretože $2 \leq m, l < n$, podľa indukčného predpokladu existujú $r, s \in \mathbb{N}$ a prvočísla $p_1, \dots, p_r, p_{r+1}, \dots, p_{r+s}$ tak, že $m = p_1 \dots p_r$, $l = p_{r+1} \dots p_{r+s}$. Potom $n = p_1 \dots p_r \dots p_{r+s}$, $r+s \in \mathbb{N}$, je požadované vyjadrenie (rozklad), $p_1, \dots, p_{r+s}$ sú prvočísla.

Jednoznačnosť. Opäť indukciou 2. typu.

$n = 2$. $2 = p_1 \dots p_k$, $k \in \mathbb{N}$ $p_1, \dots, p_k$ sú prvočísla. $p_1 \mid 2$, $p_1 \neq 1$, a preto $p_1 = 2$. Ak $k > 1$, tak dostaneme $1 = p_2 \dots p_k$. Potom $p_2 \mid 1$, a preto $p_2 \leq 1$, čo je spor. Teda $k = 1$. Dostali sme $2=2$.

Nech $n > 2$ a výrok platí pre všetky $m \in \mathbb{N}$, $2 \leq m < n$. Nech $n = p_1 \dots p_k = q_1 \dots q_l$, $k, l \in \mathbb{N}$, $p_1, \dots, p_k, q_1, \dots, q_l$ sú prvočísla. $p_1 \mid q_1, \dots, q_l$, a preto existuje $i \in \{1, \dots, l\}$ $p_1 \mid q_i$. Potom $p_1 = q_i$. $p_1 \mid n$ a teda existuje $m \in \mathbb{N}$ $n = p_1 m$.

Nech $m = 1$. Potom $n = p_1 = q_1 \dots q_i \dots q_l$, $p_1 = q_i$. Ak $l > 1$ tak dostaneme $1 = q_1 \dots q_{i-1} q_{i+1} \dots q_l > 1$, čo je spor. Teda $l = 1$, $q_i = q_1 = p_1$. Dostali sme $n = p_1 = q_1$.

Nech $m \geq 2$. Potom $m = p_2 \dots p_k = q_1 \dots q_{i-1} \dots q_{i+1} \dots q_l$. Podľa indukčného predpokladu je vyjadrenie m jednoznačné, až na poradie činiteľov, t.j. existuje bijektívne zobrazenie $\sigma': \{2, \dots, k\} \rightarrow \{1, \dots, i-1, i+1, \dots, l\}$ také, že $\forall j \in \{2, \dots, k\}$ $q_{\sigma'(j)} = p_j$ (zrejme $k-1 = l-1$). Potom ale zobrazenie $\sigma: \{1, \dots, k\} \rightarrow \{1, \dots, l\}$; $\sigma(1) = i$ a $\sigma(j) = \sigma'(j)$ pre každé $j \geq 2$ je bijektívne (a teda $k = l$) a pre každé $j \in \{1, \dots, n\}$ $q_{\sigma(j)} = p_j$. Teda vyjadrenie čísla n je jednoznačné, až na poradie činiteľov. □

Dôsledok 1.2.4. Pre každé $n \in \mathbb{N}$, $n > 1$ existuje prvočíslo p také, že $p \mid n$.

Príklad. a) $600 = 2.2.2.3.5.5 = 2^3.3^1.5^2$, $2 \neq 3, 5$, $3 \neq 5$

b) $n \geq 2$ $n = p_1, \dots, p_k = q_1^{l_1} \dots q_m^{l_m}$, $q_1, \dots, q_m$ sú navzájom rôzne prvočísla, $l_1, \dots, l_m \in \mathbb{N}$ je kanonický rozklad čísla n na prvočísla.

Veta 1.2.5. Množina všetkých prvočísel je nekonečná.

Dôkaz (Euklides). Nepriamo. Nech $p_1, \dots, p_k$, $k \in \mathbb{N}$, sú všetky prvočísla. Utvorme číslo $n = p_1 \dots p_k + 1$. Zrejme $n > p_1 \dots p_k > 1$, a preto $n > 2$. Potom existuje prvočíslo p také, že $p \mid n$. Pretože $p_1, \dots, p_k$ sú všetky prvočísla, existuje i , $1 \leq i \leq k$ také, že $p = p_i$. Teda $p_i \mid p_1 \dots p_k$, $p_i \mid n$, a preto $p_i \mid n - p_1 \dots p_k = 1$. Potom $p_i \leq 1$, čo je spor. □

Veta 1.2.6. Nech $n = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad čísla $n > 1$ a $d \in \mathbb{N}$. Potom $d \mid n \Leftrightarrow d = p_1^{t_1} \dots p_k^{t_k}$, kde pre každé $i = 1, \dots, k$ je $0 \leq t_i \leq l_i$.

Dôkaz. $\Rightarrow$ Nech $d \mid n$. Potom existuje $c \in \mathbb{N}$ také, že $n = c.d$. Pretože $c.d = p_1^{l_1} \dots p_k^{l_k}$ a tento rozklad je až na poradie činiteľov jednoznačný, musí platiť $c = p_1^{s_1} \dots p_k^{s_k}$, $d = p_1^{t_1} \dots p_k^{t_k}$, kde pre každé i je $0 \leq s_i$, $0 \leq t_i$ a $s_i + t_i = l_i$. Teda pre každé i je $0 \leq t_i \leq l_i$.

$\Leftarrow$ Nech $d = p_1^{t_1} \dots p_k^{t_k}$ a pre každé $i = \{1, \dots, k\}$ $0 \leq t_i \leq l_i$. Potom pre každé $i = \{1, \dots, k\}$ platí $l_i - t_i \geq 0$. Potom $c = p_1^{l_1 - t_1} \dots p_k^{l_k - t_k} \in \mathbb{N}$ a $c.d = p_1^{l_1 - t_1} \dots p_k^{l_k - t_k} \cdot p_1^{t_1} \dots p_k^{t_k} = p_1^{l_1} \dots p_k^{l_k} = n$. $\square$

Dôsledok 1.2.7. Nech $m, n \in \mathbb{N}$ a $p_1 \dots p_k$ sú všetky (navzájom rôzne) prvočísla, ktoré sa vyskytujú v kanonickom rozklade m a n . Potom $m = p_1^{l_1} \dots p_k^{l_k}$, $l_1 \dots l_k \in \mathbb{N}_0$, $n = p_1^{t_1} \dots p_k^{t_k}$, $t_1 \dots t_k \in \mathbb{N}_0$ a platí

$$\begin{aligned} (m, n) &= p_1^{s_1} \dots p_k^{s_k}, & \text{kde } s_i &= \min\{l_i, t_i\} \text{ pre } i = 1, \dots, k, \\ [m, n] &= p_1^{r_1} \dots p_k^{r_k}, & \text{kde } r_i &= \max\{l_i, t_i\} \text{ pre } i = 1, \dots, k. \end{aligned}$$

Dôkaz. Cvičenie. $\square$

Príklad. Určte (5445, 2625) aj [5445, 2625]

Riešenie:

$$5445 = 3^2 \cdot 5 \cdot 11^2 = 3^2 \cdot 5 \cdot 7^0 \cdot 11^2$$

$$2625 = 3 \cdot 5^3 \cdot 7 = 3 \cdot 5^3 \cdot 7 \cdot 11^0$$

$$(5445, 2625) = 3 \cdot 5 \cdot 7^0 \cdot 11^0 = 15$$

$$[5445, 2625] = 3^2 \cdot 5^3 \cdot 7 \cdot 11^2 = 952875$$

Veta 1.2.5 hovorí, že prvočísel je nekonečne veľa ale nehovorí o tom, ako sú v množine $\mathbb{N}$ rozložené. Pre ľubovoľné $x \in \mathbb{R}$ nech $\pi(x)$ je počet všetkých prvočísel, ktoré sú menšie alebo rovné ako x . Potom zrejme $\pi(-1) = \pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(8) = 4$ atď. Funkcia $\pi(x)$ je jednou z možností vyjadrenia rozloženia prvočísel, neexistuje však žiaden vzorec, ktorý by vyjadroval hodnotu $\pi(n)$ pre každé $n \in \mathbb{N}$. Preto bola snaha aproximovať hodnoty funkcie $\pi(x)$ nejakými elementárnymi funkciami. Jedna z takých funkcií, ktorú navrhol Gauss (18. storočie), je funkcia $f(x) = \frac{x}{\ln x}$. Gauss vyslovil hypotézu, že táto funkcia dobre aproximuje funkciu $\pi(x)$, t.j. že platí $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$. Až koncom 19. storočia (1896) sa tento výsledok podarilo dokázať a nazýva sa prvočíselná veta.

Veta 1.2.8 (prvočíselná veta). Nech pre každé $x \in \mathbb{R}$ $\pi(x)$ označuje počet všetkých prvočísel menších alebo rovných ako x . Potom

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Porovnanie hodnôt funkcií $\pi(x)$ a $\frac{x}{\ln x}$ pre niektoré hodnoty x :

x	$\pi(x)$	$\frac{x}{\ln x}$
1 000	168	145
10 000	1 229	1 086
100 000	9 592	8 686
1 000 000	78 498	72 382
10 000 000	664 579	620 419

Poznámka. V teórii čísel existuje rad dodnes nevyriešených problémov, známych už viacerým storočím. Napríklad je to problém, či prvočíselných dvojčiat je nekonečne veľa alebo len konečný počet (ak p aj $p + 2$ sú prvočísla, tak dvojica $p, p + 2$ sa nazýva prvočíselné dvojčatá; napr. 3,5; 5,7; 11,13; ..., $p = 1\,000\,000\,009\,649, p + 2$.)

Je známe, že pre každé $n > 1$ existuje prvočíslo p tak, že $n < p < 2n$. Ďalej je známe, že existuje $n_0 \in \mathbb{N}$ tak, že pre každé $n \geq n_0$ existuje prvočíslo p tak, že $n^3 < p < (n+1)^3$. Nie je však známe, či podobné tvrdenie platí pre n^2 a $(n+1)^2$. Takisto nie je známe, či v postupnosti $\{n^2 + 1\}_{n=1}^{\infty}$ je konečne alebo nekonečne veľa prvočísel.

Nové konkrétne prvočísla sa často hľadajú medzi špeciálnymi typmi prirodzených čísel, najznámejšie sú prípady čísel typu $2^n + 1$ a $2^n - 1$ ($n \in \mathbb{N}$). S tým súvisí aj nasledujúca veta.

Veta 1.2.9. a) Ak $n \in \mathbb{N}$ a $2^n + 1$ je prvočíslo, tak existuje $k \in \mathbb{N}_0$ tak, že $n = 2^k$.
b) Ak $n \in \mathbb{N}$ a $2^n - 1$ je prvočíslo, tak aj n je prvočíslo.

Dôkaz. a) Nepriamo. Nech pre každé $k \in \mathbb{N}_0$ platí $n \neq 2^k$. Potom $n > 1$ ($1 = 2^0$) a existujú prvočísla $p_1, \dots, p_m$ tak, že $n = p_1 \dots p_m$. Pretože $n \neq 2^m$, existuje i tak, že $p_i \neq 2$ a teda p_i je nepárne a $3 \leq p_i$. Pretože $p_i \mid n$, existuje $d \in \mathbb{N}$, pre ktoré $n = dp_i$. Potom $2^n + 1 = 2^{dp_i} + 1 = (2^d)^{p_i} + 1 = (2^d + 1) \cdot ((2^d)^{p_i-1} - (2^d)^{p_i-2} + \dots + 1)$. Zrejme $2^d + 1 \geq 2$ a pretože pre každé $l \in \mathbb{N}$ platí $(2^d)^l > (2^d)^{l-1}$ platí tiež, že $(2^d)^{p_i-1} - (2^d)^{p_i-2} + \dots + 1 \geq 2$. Teda $2^n + 1$ nie je prvočíslo.

b) Cvičenie. □

Prirodzené číslo $M_p = 2^p - 1$, kde p je prvočíslo, sa nazýva Mersennovo číslo, ak je M_p prvočíslo, tak sa nazýva Mersennovo prvočíslo. Marin Mersenne bol francúzsky mních, ktorý sa zaoberal takýmito prvočíslami a už v roku 1644 zistil, že pre $p = 2, 3, 5, 17, 19$ je $M_p = 2^p - 1$ prvočíslo.

Prirodzené číslo $F_n = 2^{2^n} + 1$, kde $n \in \mathbb{N}_0$ sa nazýva Fermatovo číslo. Čísla $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ a $F_4 = 2^{16} + 1$ sú prvočísla a Fermat sa domnieval, že všetky Fermatove čísla sú prvočísla. V roku 1732 však Euler ukázal, že $F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$ je zložené číslo. Doteraz sa nepodarilo dokázať, že existuje Fermatovo číslo $F_n, n > 5$, ktoré by bolo prvočíslom. Fermatove prvočísla majú význam aj pre geometriu. V roku 1801 Gauss dokázal, že pravidelný n -uholník sa dá zostrojiť pomocou pravítka a kružidla (euklidovskou konštrukciou) práve vtedy, keď $n = 2^k p_1 \dots p_m$, kde $p_1, \dots, p_m$ sú Fermatove prvočísla.

Cvičenia

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. ($M_n = 2^n - 1$ - Mersennovo číslo¹) [$M_{11} = 2^{11} - 1 = 2047$ nie je prvočíslo, $23 \mid M_{11}$.]
6. Zistite, pre ktoré prvočísla p je $p^2 + 1$ prvočíslo.
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 $n < p < n!$

¹mních Mersenne 1644

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) $11^5 \cdot 17^2$.
13. Nájdite všetky $n \in \mathbb{N}_0$, pre ktoré $3n + 1 \mid 1260$.
14. Nájdite prirodzené číslo, ktoré je deliteľné číslom 2 a číslom 9 a má práve 14 deliteľov v $\mathbb{N}$.
15. Dokážte, že $n^4 + 4$ nie je prvočíslo pre $n \geq 2$.
16. Zistite, ktoré z uvedených čísel je rovné druhej mocnine nejakého prirodzeného čísla:
a) $2^2 \cdot 3^{12} \cdot 7^5$, b) $23^{12} \cdot 12^{13}$, c) 1234321, d) 157996443.
17. Zistite, koľkými nulami končí číslo a) 100!, b) 1000!
18. Aspoň dvojciferné číslo, ktorého všetky cifry sú rovnaké nie je druhou mocninou žiadneho prirodzeného čísla. Dokážte!
- 19*. Nájdite všetky prvočísla tvaru $\frac{n(n+1)}{2} - 1$, kde $n \in \mathbb{N}$.
20. Dokážte, že existuje nekonečne veľa prvočísel tvaru $6k - 1$ ($k \in \mathbb{N}$).
21. Ak p a $p + 2$ sú prvočíselné dvojčatá a $p > 3$, tak $6 \mid p + 1$. Dokážte!
22. Vypočítajte počet deliteľov čísla 324000.
23. Určte, ktoré z čísel 156200, 40960 a 46656 je s druhou mocninou nejakého prirodzeného čísla n a súčasne tretou mocninou nejakého prirodzeného čísla k .
- 24*. Koľko čísel menších ako $3^n 5^m$ je s číslom $3^n 5^m$ nesúdeliteľných?
- 25*. V rovnosti $\text{LIK} \times \text{LIK} = \text{BUBLIK}$ nahraďte každé písmeno cifrou tak, aby vznikla identita. (Rôznym písmenám zodpovedajú rôzne cifry.) Riešte tú istú úlohu pre rovnosť $\text{SUK} \times \text{SUK} = \text{BARSUK}$. (Návod: všimnite si, že $1000 \mid \text{LIK} \times (\text{LIK} - 1)$ a čísla LIK a $\text{LIK} - 1$ sú nesúdeliteľné.)
- 26*. Nájdite prirodzené čísla k, n tak, aby platilo $28k^4 = 75n^3$ a aby k bolo najmenšie možné také číslo.
- 27*. Nájdite prirodzené čísla k, m, n tak, aby platilo $45km^2 = 8n^3$ a súčasne $kmn < 1000$.
- 28*. Dokážte, že ak p je prvočíslo a $0 < n < p$, tak $p \mid \binom{p}{n} = \frac{p(p-1)\dots(p-n+1)}{n!}$.

1.3 Číselné sústavy

$$\begin{aligned} 203 &= 2 \cdot 10^2 + 0 \cdot 10 + 3 \cdot 10^0 & 0 \leq 2, 0, 3 < 10 \\ 203 &= 4 \cdot 7^2 + 1 \cdot 7 + 0 \cdot 7^0 = (410)_7 & 0 \leq 4, 1, 0 < 7 \\ 13 &= 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0 = (1101)_2 \end{aligned}$$

Veta 1.3.1. *Nech $g \in \mathbb{N}$, $g \geq 2$. Potom pre každé $n \in \mathbb{N}$ existuje $k \in \mathbb{N}_0$ a $c_0, \dots, c_k \in \mathbb{N}_0$ tak, že pre všetky $i \in \{0, \dots, k\}$ $c_i \leq g-1$, $c_k \neq 0$ a $n = c_k g^k + \dots + c_1 g + c_0$. Toto vyjadrenie je jednoznačné.*

Dôkaz. Existencia. Matematickou indukciou. Pre $n = 1$, $k = 0$, $c_0 = 1$ - platí.

Nech $n > 1$ a pre všetky $m \in \mathbb{N}$, $m < n$ výrok platí. Dokážeme, že potom platí aj pre n . Podľa vety 1.1.3 existujú $l, c_0 \in \mathbb{Z}$ tak, že

$$n = l \cdot g + c_0, \quad 0 \leq c_0 < g.$$

Zrejme $l \geq 0$, pretože ak $l < 0$, tak $l \leq -1$, a preto $l \cdot g \leq -g$ a potom $n = l \cdot g + c_0 \leq -g + c_0 < 0$... spor.

Ak $l = 0$, máme $n = c_0$, t.j. $k = 0$, $c_0 \leq g-1$, $c_0 \in \mathbb{N}_0$, $c_0 \neq 0$, t.j. výrok platí.

Nech $l \geq 1$. Pretože $1 < g$, platí $l < l \cdot g \leq l \cdot g + c_0 = n$. Teda $1 \leq l < n$ a podľa indukčného predpokladu existuje $k \in \mathbb{N}_0$, $b_0, \dots, b_k \in \mathbb{N}_0$ tak, že pre všetky i $b_i \leq g-1$, $b_k \neq 0$ a $l = b_k g^k + \dots + b_1 g + b_0$. Potom

$$n = l \cdot g + c_0 = b_k g^{k+1} + \dots + b_0 g + c_0.$$

Ak položíme $b_0 = c_1, \dots, b_k = c_{k+1}$, tak dostaneme $n = c_{k+1} g^{k+1} + \dots + c_1 g + c_0$, $(\forall i) c_i \leq g-1$, $c_{k+1} \neq 0$, $k+1 \in \mathbb{N}_0$. Teda výrok platí pre n .

Jednoznačnosť. Nech $n = c_k g^k + \dots + c_1 g + c_0 = d_m g^m + \dots + d_1 g + d_0$, $k, m \in \mathbb{N}_0$, a pre všetky i $0 \leq c_i \leq g-1$, $c_k \neq 0$, pre všetky j $0 \leq d_j \leq g-1$, $d_m \neq 0$. Najprv dokážeme, že $k = m$. Nepriamo. Nech $k \neq m$. Potom $k < m$ alebo $k > m$. Nech $k < m$. Potom $k+1 \leq m$ a

$$\begin{aligned} n &= c_k g^k + \dots + c_0 \leq (g-1)g^k + \dots + (g-1) = \\ &= (g-1)(g^k + \dots + 1) = g^{k+1} - 1 < g^{k+1} \leq g^m \leq d_m g^m + \dots + d_0 = n \end{aligned}$$

Teda $n < n$... spor. Podobne pre $m < k$.

Preto $k = m$.

Nech existuje i také, že $c_i \neq d_i$ a j je najväčšie číslo, pre ktoré $c_j \neq d_j$. Nech napríklad $c_j < d_j$. Potom

$$\begin{aligned} 0 &= n - n = (d_j - c_j)g^j + \dots + (d_1 - c_1)g + (d_0 - c_0) \geq \\ &\geq (d_j - c_j)g^j - (g-1)g^{j-1} - \dots - (g-1) \geq g^j - (g^j - 1) = 1 > 0. \end{aligned}$$

Teda $0 > 0$... spor. Podobne pre $d_j < c_j$.

Preto pre $i = 0, \dots, k$ $c_i = d_i$. □

Vyjadrenie $n = c_k g^k + \dots + c_1 g + c_0$, $k \in \mathbb{N}_0$, $c_0, \dots, c_k \in \mathbb{N}_0$, $\forall i$ $c_i \leq g-1$, $c_k \neq 0$, ktoré zapisujeme tiež $n = (c_k \dots c_0)_g$, sa nazýva vyjadrenie čísla n v g -adickej sústave.

Príklad. Vyjadrite číslo 356 v sedmičkovej sústave.

$$\begin{array}{rcl}
 356 : 7 = 50 & & 356 = 50 \cdot 7 + 6 \\
 6 & & \\
 50 : 7 = 7 & & 50 = 7 \cdot 7 + 1 \\
 1 & & 356 = (7 \cdot 7 + 1) \cdot 7 + 6 = 7^3 + 1 \cdot 7 + 6 \\
 7 : 7 = 1 < 7 & & = 1 \cdot 7^3 + 0 \cdot 7^2 + 1 \cdot 7 + 6 = (1016)_7 \\
 0 & &
 \end{array}$$

Vyjadrite 356 v päťkovej sústave.

$$\begin{array}{rcl}
 356 : 5 = 71 & 71 : 5 = 14 & 14 : 5 = 2 < 5 \\
 1 & 1 & 4
 \end{array}$$

$$356 = (2411)_5$$

Cvičenia

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 $n = (a_1 a_0)_{10} = (a_1 a_0 2)_3$.
7. Nájdite také dvojice m, n prirodzených čísel, $m \neq n$, pre ktoré aritmetický priemer m, n je dvojciferné číslo ab a geometrický priemer m, n je dvojciferné číslo ba (v dekadické sústave).

1.4 Kongruencie

1.4.1 Pojem kongruentnosti mod n , základné vlastnosti

Vo vzťahu k deliteľnosti číslom 5 možno množinu $\mathbb{Z}$ rozdeliť na čísla deliteľné 5 a nedeliteľné 5. Čísla nedeliteľné 5 možno ešte rozdeliť podľa toho, aký zvyšok dávajú po delení číslom 5. Čísla, ktoré dávajú rovnaký zvyšok po delení 5 majú, čo sa týka deliteľnosti číslom 5 rovnaké vlastnosti, budeme hovoriť, že sú kongruentné mod 5.

Definícia 1.4.1. Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Hovoríme, že a je kongruentné s b modulo n , ak $n \mid a - b$. Zápis: $a \equiv b \pmod{n}$.

Príklad. $4 \equiv 1 \pmod{3}$, $-2 \equiv 3 \pmod{5}$, $\forall a, b \in \mathbb{Z} \ a \equiv b \pmod{1}$

Veta 1.4.2. Nech $a, b, c, d \in \mathbb{Z}$ a $n \in \mathbb{N}$. Potom platí:

- (1) $a \equiv a \pmod{n}$
- (2) Ak $a \equiv b \pmod{n}$, tak $b \equiv a \pmod{n}$.
- (3) Ak $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, tak $a \equiv c \pmod{n}$.
- (4) Ak $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, tak $a \pm c \equiv b \pm d \pmod{n}$ a $a.c \equiv b.d \pmod{n}$.
- (5) Ak $a.c \equiv b.c \pmod{n}$, $(c, n) = 1$, tak $a \equiv b \pmod{n}$.
- (6) Ak $f(x) = a_k x^k + \dots + a_1 x + a_0$, $a_i \in \mathbb{Z}$ a $c \equiv d \pmod{n}$, tak $f(c) \equiv f(d) \pmod{n}$.
- (7) Pre každé $a \in \mathbb{Z}$ existuje práve jedno $l \in \{0, 1, \dots, n-1\}$ také, že $a \equiv l \pmod{n}$.
- (8) Ak $a = a'n + k$, $b = b'n + l$ a $0 \leq k, l < n$, tak $a \equiv b \pmod{n} \Leftrightarrow k = l$.
- (9) Ak $a \equiv b \pmod{n}$, tak $(a, n) = (b, n)$.

Dôkaz. (1) $n \mid a - a = 0$

(2) Ak $n \mid a - b$, tak $n \mid -(a - b) = b - a$.

(3) Ak $n \mid a - b$, $n \mid b - c$, tak $n \mid (a - b) + (b - c) = a - c$

(4) Ak $n \mid a - b$, $n \mid c - d$, tak $n \mid (a - b) \pm (c - d) = (a \pm c) - (b \pm d)$.

$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b)$. Ak $n \mid a - b$, $n \mid c - d$, tak $n \mid d(a - b) + a(c - d) = ac - bd$.

(5) Ak $n \mid ac - bc = (a - b).c$, $(n, c) = 1$, tak $n \mid a - b$.

(6) Ak $c \equiv d \pmod{n}$, tak pre každé $i \in \{1, \dots, k\}$ $c^i \equiv d^i \pmod{n}$. Potom $\forall i$ $a_i c^i \equiv a_i d^i \pmod{n}$, $a_0 \equiv a_0 \pmod{n}$, a preto $a_k c^k + \dots + a_1 c + a_0 \equiv a_k d^k + \dots + a_1 d + a_0 \pmod{n}$.

(7) Existujú $k, l \in \mathbb{Z}$ tak, že $a = k.n + l$ a $0 \leq l < n$, t.j. $l \in \{0, 1, \dots, n-1\}$. Potom $a - l = k.n$, t.j. $n \mid a - l$. Preto $a \equiv l \pmod{n}$. Nech $l' \in \{0, 1, \dots, n-1\}$ a $a \equiv l' \pmod{n}$. Potom $l \equiv l' \pmod{n}$ a teda $n \mid l' - l$. Preto $n \mid |l' - l|$. Súčasne $0 \leq |l' - l| < n$. Preto $|l - l'| = 0$, t.j. $l = l'$.

(8) $\Rightarrow$ Ak $a \equiv b \pmod{n}$, tak $k \equiv l \pmod{n}$, lebo platí $a \equiv k \pmod{n}$ a $b \equiv l \pmod{n}$. Pretože $k, l \in \{0, 1, \dots, n-1\}$, máme $k = l$.

$\Leftarrow$ $a \equiv k \pmod{n}$, $b \equiv l \pmod{n}$. Ak $k = l$, tak $a \equiv b \pmod{n}$.

(9) $n \mid a - b$, $(a, n) = d$, $(b, n) = d'$

$d \mid a, n$, preto $d \mid a, a - b$ a potom $d \mid a - (a - b) = b$.

Teda $d \mid n, b$, a preto $d \leq d'$. Podobne sa ukáže, že $d' \leq d$. □

Uvažujme o kongruentnosti $\pmod{5}$. Je to relácia ekvivalencie na $\mathbb{Z}$. Podľa predchádzajúcej vety, časť (8) platí, že $a \equiv b \pmod{5}$ práve vtedy, keď zvyšok po delení čísla a a zvyšok po delení čísla b číslom 5 sú rovnaké. Množina $[1]_5 = \{5z + 1; z \in \mathbb{Z}\}$ obsahuje všetky celé čísla, ktorých zvyšok po delení číslom 5 je 1 a teda pre ľubovoľné $a, b \in [1]_5$ platí $a \equiv b \pmod{5}$. Ak $c \notin [1]_5$ a $a \in [1]_5$, tak $c \not\equiv a \pmod{5}$.

Analogicky, množiny $[0]_5 = \{5z; z \in \mathbb{Z}\}$, $[2]_5 = \{5z + 2; z \in \mathbb{Z}\}$, $[3]_5 = \{5z + 3; z \in \mathbb{Z}\}$, $[4]_5 = \{5z + 4; z \in \mathbb{Z}\}$ sú množiny navzájom kongruentných prvkov $\pmod{5}$, ktoré sa nazývajú zvyškové triedy $\pmod{5}$. Ak prvky c , resp. d patria do rôznych zvyškových tried, tak $c \not\equiv d \pmod{5}$. Je zrejmé, že $\mathbb{Z} = [0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$ a tieto zvyškové triedy sú navzájom disjunktné. Analogická situácia nastáva pre ľubovoľné $n \in \mathbb{N}$.

Definícia 1.4.3. Nech $n \in \mathbb{N}$ a $a \in \mathbb{Z}$. Množina $[a]_n = \{c \in \mathbb{Z}; c \equiv a \pmod{n}\}$ sa nazýva *zvyšková trieda modulo n* .

Príklad. a) $[1]_5 = \{1 + 5z; z \in \mathbb{Z}\}$, lebo $a \equiv 1 \pmod{5} \Leftrightarrow a - 1 = 5z \Leftrightarrow a = 1 + 5z$

b) $[6]_5 = \{6 + 5z; z \in \mathbb{Z}\} = \{1 + 5(z + 1); z \in \mathbb{Z}\} = [1]_5$

c) $a \in [a]_n$, lebo $a \equiv a \pmod{n}$.

d) $[0]_n = \{n \cdot z; z \in \mathbb{Z}\}$ - všetky čísla deliteľné n

$[1]_n = \{1 + n \cdot z; z \in \mathbb{Z}\}$ - všetky čísla, ktorých zvyšok po delení n je 1

$[2]_n = \{2 + n \cdot z; z \in \mathbb{Z}\}$

$\vdots$

$[n - 1]_n = \{(n - 1) + n \cdot z; z \in \mathbb{Z}\}$

$[n]_n = [0]_n, [n + 1]_n = [1]_n, \dots, [-1]_n = [n - 1]_n, \dots$

Zrejme platí $[0]_n \cup [1]_n \cup \dots \cup [n - 1]_n = \mathbb{Z}$.

Veta 1.4.4. *Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Potom platí:*

$$(1) \quad a \equiv b \pmod{n} \Leftrightarrow [a]_n = [b]_n$$

$$(2) \quad a \not\equiv b \pmod{n} \Leftrightarrow [a]_n \cap [b]_n = \emptyset$$

$$(3) \quad \text{Pre každé } a \in \mathbb{Z} \text{ existuje } k \in \{0, \dots, n - 1\} \text{ tak, že } [a]_n = [k]_n.$$

Dôkaz. (1) $\Rightarrow$ Nech $c \in [a]_n$. Potom $c \equiv a \pmod{n}$. Pretože $a \equiv b \pmod{n}$ dostávame $c \equiv b \pmod{n}$ a teda $c \in [b]_n$. Dokázali sme, že $[a]_n \subseteq [b]_n$. Podobne sa ukáže, že $[b]_n \subseteq [a]_n$.

$$\Leftarrow [a]_n = [b]_n \Rightarrow b \in [a]_n \Rightarrow a \equiv b \pmod{n}.$$

(2) $\Rightarrow$ Nech $[a]_n \cap [b]_n \neq \emptyset$. Potom existuje $c \in [a]_n \cap [b]_n$ a teda $c \equiv a \pmod{n}$, $c \equiv b \pmod{n}$. Potom $a \equiv b \pmod{n}$, čo je spor. Teda $[a]_n \cap [b]_n = \emptyset$.

$$\Leftarrow \text{Ak } a \equiv b \pmod{n}, \text{ tak } [a]_n = [b]_n \text{ a teda } [a]_n \cap [b]_n \neq \emptyset \text{ (lebo } a \in [a]_n \cap [b]_n).$$

(3) Pre každé $a \in \mathbb{Z}$ existuje $k \in \{0, \dots, n - 1\}$ tak, že $a \equiv k \pmod{n}$ (pozri vetu 1.4.2(7)). Teda $[a]_n = [k]_n$. $\square$

Označme $\mathbb{Z}/(n) = \{[a]_n : a \in \mathbb{Z}\}$. Potom $\mathbb{Z}/(n) = \{[0]_n, [1]_n, \dots, [n - 1]_n\}$. Na tejto množine možno definovať operácie $\oplus, \odot$ nasledovne:

$$[a]_m \oplus [b]_n = [a + b]_n, \quad [a]_m \odot [b]_n = [a \cdot b]_n.$$

Z vlastnosti 1.4.2(4) vyplýva, že operácie sú definované korektne, t.j. výsledok nezávisí na výbere reprezentantov zvyškových tried. Ľahko sa overí, že platí:

Veta 1.4.5. *Pre každé prvočíslo p je $(\mathbb{Z}/(p), \oplus, \odot)$ pole.*

Dôkaz. Nech $[a]_p, [b]_p, [c]_p \in \mathbb{Z}/(p)$. Potom $[a]_p \oplus [b]_p = [a + b]_p = [b + a]_p = [b]_p \oplus [a]_p$, $([a]_p \oplus [b]_p) \oplus [c]_p = [a + b]_p \oplus [c]_p = [(a + b) + c]_p = [a + (b + c)]_p = [a]_p \oplus [b + c]_p = [a]_p \oplus ([b]_p \oplus [c]_p)$. Teda operácia $\oplus$ je komutatívna aj asociatívna. Zrejme $[0]_p$ je nulový prvok. Platí tiež $[a]_p \oplus [p - a]_p = [p]_p = [0]_p$ a preto $[p - a]_p$ je opačný prvok k prvku $[a]_p$. Komutatívnosť a asociatívnosť operácie $\odot$ sa dokáže podobne ako v prípade operácie $\oplus$. Zrejme $[1]_p$ je jednotkový prvok ($[1]_p \neq [0]_p$). Nech teraz $[a]_p \neq [0]_p$. Potom $a \not\equiv 0 \pmod{p}$ a preto $p \nmid a$. Pretože p je prvočíslo, platí potom $(a, p) = 1$ a existujú $u, v \in \mathbb{Z}$ tak, že $u \cdot a + v \cdot p = 1$. Potom zrejme $p \mid u \cdot a - 1$ a teda $u \cdot a \equiv 1 \pmod{p}$. Z toho vyplýva, že $[u]_p \odot [a]_p = [u \cdot a]_p = [1]_p$ a teda $[u]_p$ je inverzný prvok k prvku $[a]_p$.

Ešte zostáva overiť distributívnosť násobenia vzhľadom na sčítanie v $(\mathbb{Z}/(p), \oplus, \odot)$:
 $[a]_p \odot ([b]_p \oplus [c]_p) = [a]_p \odot [b + c]_p = [a \cdot (b + c)]_p = [a \cdot b + a \cdot c]_p = [a \cdot b]_p \oplus [a \cdot c]_p = [a]_p \odot [b]_p \oplus [a]_p \odot [c]_p$. $\square$

Príklad. $(\mathbb{Z}/(3), \oplus, \odot)$ je pole.

Porovnajme operácie v tomto poli a v poli $(\mathbb{Z}_3, +, \cdot)$, ktoré poznáme z lineárnej algebry:

$$[1]_3 \oplus [2]_3 = [3]_3 = [0]_3$$

$$[2]_3 \odot [2]_3 = [4]_3 = [1]_3$$

Vidíme, že toto pole je „v podstate“ totožné s polom $(\mathbb{Z}_3, +, \cdot)$.

Podobná situácia ako v predchádzajúcom príklade platí aj všeobecne pre každé prvočíslo p . Nech $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ je množina zvyškov po delení číslom p . Podľa vety 1.4.2.(7) pre každé $a \in \mathbb{Z}$ existuje práve jedno $l \in \mathbb{Z}_p$ tak, že $a \equiv l \pmod{p}$. Ďalej, z tejto vety vyplýva, že ak $l, q \in \mathbb{Z}_p$ a $[l]_p = [q]_p$ (t. j. $l \equiv q \pmod{p}$), tak $l = q$. Na množine $\mathbb{Z}_p$ definujeme operácie $\boxplus, \boxdot$ takto: pre každé $m, k \in \mathbb{Z}_p$ je $m \boxplus k$ zvyšok po delení čísla $m + k$ číslom p a $m \boxdot k$ je zvyšok po delení čísla $m \cdot k$ číslom p . Teda $m \boxplus k, m \boxdot k \in \mathbb{Z}_p$ a existujú $u, v \in \mathbb{Z}$ tak, že $m + k = u \cdot p + (m \boxplus k)$ a $m \cdot k = v \cdot p + (m \boxdot k)$. Z toho je zrejmé, že $m \boxplus k \equiv m + k \pmod{p}$, $m \boxdot k \equiv m \cdot k \pmod{p}$ a preto pre každé $m, k \in \mathbb{Z}_p$ platí $[m \boxplus k]_p = [m + k]_p = [m]_p \oplus [k]_p$ a $[m \boxdot k]_p = [m \cdot k]_p = [m]_p \odot [k]_p$ ($\oplus$ a $\odot$ sú operácie v $(\mathbb{Z}/(p), \oplus, \odot)$). Pomocou týchto vzťahov a toho, že $(\mathbb{Z}/(p), \oplus, \odot)$ je pole ľahko overíme, že aj $(\mathbb{Z}_p, \boxplus, \boxdot)$ je pole. Pre ilustráciu overíme distributívnosť $\boxdot$ vzhľadom na $\boxplus$ a existenciu inverzných prvkov k nenulovým prvkom v $(\mathbb{Z}_p, \boxplus, \boxdot)$.

Nech $k, l, m \in \mathbb{Z}_p$. Potom $[k \boxdot (l \boxplus m)]_p = [k \cdot (l + m)]_p = [k]_p \odot [l + m]_p = [k]_p \odot [l]_p \oplus [m]_p = [k \cdot (l + m)]_p = [k \cdot l + k \cdot m]_p = [k \cdot l]_p \oplus [k \cdot m]_p = [k \boxdot l]_p \oplus [k \boxdot m]_p = [(k \boxdot l) \boxplus (k \boxdot m)]_p = [(k \boxdot l) \boxplus (k \boxdot m)]_p$. Pretože $k \boxdot (l \boxplus m)$ aj $(k \boxdot l) \boxplus (k \boxdot m)$ sú prvky $\mathbb{Z}_p$, dostávame, že $k \boxdot (l \boxplus m) = (k \boxdot l) \boxplus (k \boxdot m)$.

Nech teraz $k \in \mathbb{Z}_p$, $k \neq 0$. Potom $k \not\equiv 0 \pmod{p}$ a teda $[k]_p \neq [0]_p$ v $\mathbb{Z}/(p)$. Pretože $(\mathbb{Z}/(p), \oplus, \odot)$ je pole, existuje $[a]_p \in \mathbb{Z}/(p)$ také, že $[k]_p \odot [a]_p = [1]_p$. Ďalej existuje $m \in \mathbb{Z}_p$ také, že $a \equiv m \pmod{p}$ a teda $[a]_p = [m]_p$. Potom $[k \boxdot m]_p = [k \cdot m]_p = [k]_p \odot [m]_p = [k]_p \odot [a]_p = [1]_p$ a pretože $k \boxdot m, 1 \in \mathbb{Z}_p$ dostávame, že platí $k \boxdot m = 1$. Teda m je inverzný prvok k prvku k v $(\mathbb{Z}_p, \boxplus, \boxdot)$.

Cvičenia

- Nájdite poslednú cifru čísla a) $213^{174} + 25^{17}$, b) $99^{99} + (7^{17})^{17}$, c) $127^{37} + 45^{131} + 109^{18}$.
- Nájdite všetky prirodzené čísla n , pre ktoré a) $7 \mid 2^n - 1$, b) $7 \mid 2^n + 1$.
- Nech $a, b \in \mathbb{Z}$. Dokážte, že $19 \mid 10a + b \Leftrightarrow 19 \mid a + 2b$.
- Overte, či $19 \mid 539828$ s využitím predchádzajúcej úlohy.
- 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.
- Dokážte, že pre každé $n \in \mathbb{N}$ platí: Ak $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$, $k \in \mathbb{N}$ a pre každé $i = 1, \dots, n$ $a_i \equiv b_i \pmod{k}$, tak $a_1 + \dots + a_n \equiv b_1 + \dots + b_n \pmod{k}$ a $a_1 \dots a_n \equiv b_1 \dots b_n \pmod{k}$.
- a) Určte poslednú cifru čísla $n = 22 \cdot 51 + 698^5$ pri jeho vyjadrení v päťkovej a v sedmičkovej sústave.
b) Určte posledné dve cifry čísla $n = 2135^{176} + 244^{32} + 12^{241}$ v trojkovej sústave.
- Ak $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$, $m \mid n$ a $a \equiv b \pmod{n}$, tak $a \equiv b \pmod{m}$. Dokážte!
- Aký je zvyšok 167^{452} po delení 11?

10. a) V poli $\mathbb{Z}_{23}$ nájdite inverzné prvky k prvkom 6 a 11.
 b) V poli $\mathbb{Z}_{29}$ nájdite opačné a inverzné prvky k prvkom 5, 14 a 25.
11. Nech p je prvočíslo a $f : \mathbb{Z}_p \rightarrow \mathbb{Z}/(p)$ je zobrazenie definované predpisom $f(k) = [k]_p$. Dokážte, že f je bijektívne zobrazenie a pre každé $k, m \in \mathbb{Z}_p$ platí $f(k \boxplus m) = f(k) \oplus f(m)$ a $f(k \boxminus m) = f(k) \odot f(m)$.

1.4.2 Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel

Veta 1.4.6. *Prirodzené číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 9, resp. 3 $\Leftrightarrow$ číslo $c_k + \dots + c_1 + c_0$ je deliteľné číslom 9, resp. 3.*

Dôkaz.

$$c_k + \dots + c_1 + c_0 = c_k 1^k + \dots + c_1 1 + c_0$$

Zoberme polynóm $f(x) = c_k x^k + \dots + c_1 x + c_0$. Zrejme $c_i \in \mathbb{N}_0 \subseteq \mathbb{Z}$. Potom $n = f(10)$, $c_k + \dots + c_1 + c_0 = f(1)$. Platí $10 \equiv 1 \pmod{9}$. Potom podľa 1.4.2(6)

$$n = f(10) \equiv f(1) = c_k + \dots + c_1 + c_0 \pmod{9}.$$

Potom $9 \mid n \Leftrightarrow 9 \mid c_k + \dots + c_1 + c_0$, lebo čísla kongruentné modulo 9 dávajú pri delení číslom 9 rovnaké zvyšky.

Platí tiež $10 \equiv 1 \pmod{3}$, a preto $n = f(10) \equiv f(1) = c_k + \dots + c_1 + c_0 \pmod{3}$. Teda

$$3 \mid n \Leftrightarrow 3 \mid c_k + \dots + c_1 + c_0.$$

□

Príklad. $3 \mid 149688 \Leftrightarrow 3 \mid 36 \Leftrightarrow 3 \mid 9$

Veta 1.4.7. *Číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 11 práve vtedy, keď $11 \mid c_0 - c_1 + c_2 - \dots + (-1)^k c_k$*

Dôkaz. Využijeme polynóm $f(x) = c_k x^k + \dots + c_1 x + c_0$ ($c_i \in \mathbb{Z}$). Zrejme $f(10) = n$ a $f(-1) = c_0 - c_1 + c_2 - \dots + (-1)^k c_k$. Platí $10 \equiv -1 \pmod{11}$, a preto

$$n = f(10) \equiv f(-1) = c_0 - c_1 + c_2 - \dots + (-1)^k c_k \pmod{11}$$

Preto

$$11 \mid n \Leftrightarrow 11 \mid c_0 - c_1 + c_2 - \dots + (-1)^k c_k.$$

□

Príklad. $11 \mid 25916 \Leftrightarrow 11 \mid 6 - 1 + 9 - 5 + 2 = 11$. Teda $11 \mid 25916$.

Veta 1.4.8. *Číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 7, resp. 11 resp. 13 $\Leftrightarrow$ číslo 7, resp. 11, resp. 13 delí číslo $q = c_0 + c_1 10 + c_2 10^2 - (c_3 + c_4 10 + c_5 10^2) + (c_6 + c_7 10 + c_8 10^2) - \dots$*

Príklad. Pre $n = 38\,431\,252\,145$ je $q = 145 - 252 + 421 - 38 = 286$. $286 : 13 = 22$, t.j. $13 \mid 286 \Rightarrow 13 \mid n$.

Dôkaz. Utvorme polynóm $f(x) = (c_0 + c_1 10 + c_2 10^2) + (c_3 + c_4 10 + c_5 10^2)x + (c_6 + c_7 10 + c_8 10^2)x^2 + \dots$

$$f(10^3) = n, f(-1) = q.$$

$$10^3 \equiv -1 \pmod{7},$$

lebo $10^3 - (-1) = 1001 = 143 \cdot 7 = 7 \cdot 11 \cdot 13$. $n = f(10^3) \equiv f(-1) = q \pmod{7}$. Preto

$$7 \mid n \Leftrightarrow 7 \mid q.$$

$$10^3 \equiv -1 \pmod{11}$$

$$n = f(10^3) \equiv f(-1) = q \pmod{11}$$

$$\text{Teda } 11 \mid m \Leftrightarrow 11 \mid q.$$

Podobne pre 13, pretože $10^3 \equiv -1 \pmod{13}$. □

Príklad. $7 \mid 10\,192\,896 \Leftrightarrow 7 \mid 896 - 192 + 10 = 714$

$$7 \mid 10\,192\,896$$

Veta 1.4.9. *Nech $g \geq 2$ a $n = c_k g^k + \dots + c_1 g + c_0$ je prirodzené číslo. Potom platí:*

$$g - 1 \mid n \Leftrightarrow g - 1 \mid c_k + \dots + c_0$$

$$g + 1 \mid n \Leftrightarrow g + 1 \mid c_0 - c_1 + \dots + (-1)^k c_k$$

Dôkaz. Využijeme polynóm $f(x) = c_k x^k + \dots + c_1 x + c_0$, $n = f(g)$, $c_k + \dots + c_0 = f(1)$, $c_0 - c_1 + \dots + (-1)^k c_k = f(-1)$ a to, že $g \equiv 1 \pmod{g-1}$ a $g \equiv -1 \pmod{g+1}$. □

Cvičenia

- Dokážte, že číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 27, resp. $37 \Leftrightarrow 27$ resp. 37 delí číslo $(c_0 + c_1 10 + c_2 10^2) + (c_3 + c_4 10 + c_5 10^2) + \dots = c_2 c_1 c_0 + c_5 c_4 c_3 + \dots$
- Zistite, či čísla 149 688, 301 587, 10 291 698 sú deliteľné
 - číslom 3, resp. 9,
 - číslom 7, 11, resp. 13,
 - číslom 27, resp. 37.
- Dokážte, že číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 101 $\Leftrightarrow$ číslo 101 delí číslo $(c_0 + c_1 10) - (c_2 + c_3 10) + (c_4 + c_5 10) - \dots = c_1 c_0 - c_3 c_2 + c_5 c_4 - \dots$
- Nech $p = 10^{m-1} + 10^{m-2} + \dots + 10 + 1 = \overbrace{11 \dots 1}^{m \text{ cifier}}$ je prvočíslo. Potom aj m je prvočíslo. Ukážte, že obrátené tvrdenie neplatí.
- Dokážte, že číslo $n = c_k 10^k + \dots + c_1 10 + c_0$ je deliteľné číslom 5 $\Leftrightarrow c_0 = 5$ alebo $c_0 = 0$.
- Nech $n = c_k 10^k + \dots + c_1 10 + c_0$. Dokážte, že platí:
 - $4 \mid n \Leftrightarrow 4 \mid 10c_1 + c_0 (=c_1 c_0)$
 - $8 \mid n \Leftrightarrow 8 \mid 10^2 c_2 + 10c_1 + c_0 (=c_2 c_1 c_0)$
- Zistite, či je číslo $(7812)_9$ deliteľné ôsmimi a desiatimi.
- Zistite, či je číslo $(1202)_6$ deliteľné dvomi a tromi.

1.5 Eulerova funkcia a Eulerova veta

Definícia 1.5.1 (Eulerova² funkcia). Zobrazenie $\varphi: \mathbb{N} \rightarrow \mathbb{R}$, ktoré každému n priradí počet prvkov množiny $\{k \in \mathbb{N}; k \leq n \text{ a } (k, n) = 1\}$ sa nazýva *Eulerova funkcia* (teda $\varphi(n)$ je počet všetkých prirodzených čísel menších alebo rovných ako n , ktoré sú nesúdeliteľné s n .)

Príklad. a) $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(8) = 4$

b) Ak $n > 1$, tak $\varphi(n)$ je počet všetkých prirodzených čísel menších ako n a nesúdeliteľných s n (lebo $(n, n) = n > 1$).

c) Pre každé prvočíslo p platí $\varphi(p) = p - 1$.

Veta 1.5.2 (Eulerova). *Nech $n \in \mathbb{N}$. Potom pre každé $a \in \mathbb{Z}$, pre ktoré $(a, n) = 1$, platí*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dôkaz. Ak $n = 1$, tak $\varphi(1) = 1$ a pre každé $a \in \mathbb{Z}$ platí $a^1 \equiv 1 \pmod{1}$. Nech $n \geq 2$ a $r_1, \dots, r_k$ sú všetky navzájom rôzne prirodzené čísla také, že pre každé $i = 1, \dots, k$ $1 \leq r_i \leq n$ a $(r_i, n) = 1$. Potom zrejme $k = \varphi(n)$.

Nech $a \in \mathbb{Z}$, $(a, n) = 1$. Potom pre $i = 1, \dots, k$ $(a.r_i, n) = 1$. Pretože $a.r_i \in \mathbb{Z}$ existuje práve jedno $l_i \in \{r_1, \dots, r_k\}$ také, že $a.r_i \equiv l_i \pmod{n}$. Podľa vety 1.4.2(9) $(l_i, n) = (a.r_i, n) = 1$. Preto $l_i \in \{r_1, \dots, r_k\}$ a $\{l_1, \dots, l_k\} \subseteq \{r_1, \dots, r_k\}$.

Nech $i, i' \in \{1, \dots, k\}$ a $l_i = l_{i'}$. Potom $a.r_i \equiv a.r_{i'} \pmod{n}$ a pretože $(a, n) = 1$, dostávame $r_i \equiv r_{i'} \pmod{n}$. Pretože $1 \leq r_i, r_{i'} \leq n$, $|r_i - r_{i'}| \leq n - 1$, a preto $r_i = r_{i'}$ a teda $i = i'$. Teda ak $i \neq i'$, tak $l_i \neq l_{i'}$ t.j. $\{l_1, \dots, l_k\}$ má k prvkov, a preto $\{l_1, \dots, l_k\} = \{r_1, \dots, r_k\}$. Potom $l_1.l_2 \dots l_k = r_1.r_2 \dots r_k$.

Pretože pre každé $i = 1, \dots, k$ $a.r_i \equiv l_i \pmod{n}$, podľa vety 1.4.2(4)

$$a.r_1.a.r_2 \dots a.r_k \equiv l_1.l_2 \dots l_k \pmod{n},$$

a teda

$$a^k r_1.r_2 \dots r_k \equiv r_1.r_2 \dots r_k \pmod{n}.$$

Ak pre všetky i $(r_i, n) = 1$, tak $(r_1.r_2 \dots r_k, n) = 1$, a preto podľa vety 1.4.2(5) $a^k \equiv 1 \pmod{n}$. Teda $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Dôsledok 1.5.3. *Ak p je prvočíslo, tak pre každé $a \in \mathbb{Z}$ také, že $p \nmid a$ $a^{p-1} \equiv 1 \pmod{p}$.*

Dôkaz. Ak p je prvočíslo, tak $\varphi(p) = p - 1$ a $(a, p) = 1 \Leftrightarrow p \nmid a$. $\square$

Dôsledok 1.5.4 (Malá veta Fermatova). *Ak p je prvočíslo, tak pre každé $a \in \mathbb{Z}$ platí*

$$a^p \equiv a \pmod{p}.$$

Dôkaz. Pre každé $a \in \mathbb{Z}$ platí $p \mid a$ alebo $p \nmid a$. Ak $p \mid a$, tak $a \equiv 0 \pmod{p}$ a potom $a^p \equiv 0^p = 0 \pmod{p}$. Teda $a^p \equiv a \pmod{p}$.

Ak $p \nmid a$, tak $a^{p-1} \equiv 1 \pmod{p}$, $a \equiv a \pmod{p}$ a teda $a^p \equiv a \pmod{p}$. $\square$

Je prirodzené sa pýtať, či neplatí aj obrátené tvrdenie: Ak $n \in \mathbb{N}$, $n \geq 2$ a pre každé $a \in \mathbb{Z}$ platí $a^n \equiv a \pmod{n}$, tak n je prvočíslo. Odpoveď je záporná. Napríklad, číslo $n = 561 = 3.11.17$ je zložené číslo a pre každé $a \in \mathbb{Z}$ platí $a^{561} \equiv a \pmod{561}$.

Príklad.

²Euler 1707-1783

1. Dokážte, že pre každé $n \in \mathbb{N}$ platí, že $15 \mid n^5 - n$.
 Riešenie: $n^5 \equiv n \pmod{5}$, a preto $5 \mid n^5 - n$.
 $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n^3 - n)(n^2 + 1)$. $n^3 \equiv n \pmod{3}$, a preto $3 \mid n^3 - n$ a potom $3 \mid (n^3 - n)(n^2 + 1) = n^5 - n$. Teda $5 \mid n^5 - n$, $3 \mid n^5 - n$ a $(3, 5) = 1$, a preto $15 = 3 \cdot 5 \mid n^5 - n$.
2. Dokážte, že ak p je prvočíslo a $a \in \mathbb{Z}$ také, že $p \nmid a$ (t.j. $a \not\equiv 0 \pmod{p}$), tak existuje $b \in \mathbb{Z}$ také, že $a \cdot b \equiv 1 \pmod{p}$.
 Riešenie: $a^{p-1} \equiv 1 \pmod{p}$, $p - 1 \geq 1$. Stačí zobrať $b = a^{p-2}$. Potom $a \cdot b = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$.
3. Dokážte, že ak $n \in \mathbb{N}$, tak n^{12} je buď deliteľné číslom 13 alebo zvyšok po delení n^{12} číslom 13 je 1.
 Riešenie: Pretože 13 je prvočíslo, tak $13 \mid n$ alebo $(n, 13) = 1$. Ak $13 \mid n$, tak $13 \mid n^{12}$. Ak $(n, 13) = 1$, tak podľa Eulerovej vety $n^{\varphi(13)} \equiv 1 \pmod{13}$, t.j. $n^{12} \equiv 1 \pmod{13}$. Teda existuje $k \in \mathbb{Z}$ tak, že $n^{12} = 13k + 1$.

Veta 1.5.5. Ak $n > 1$ a $n = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad čísla n na prvočísla, tak

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Dôkaz. Nech $n > 2$, $n = p_1^{l_1} \dots p_k^{l_k}$. Je zrejmé, že ak $m \in \mathbb{N}$, tak $(m, n) = 1 \Leftrightarrow$ pre všetky $i = 1, \dots, k$ $p_i \nmid m$. Teda $\varphi(n)$ je počet všetkých $m \in \mathbb{N}$, ktoré nie sú deliteľné prvočíslami $p_1, \dots, p_k$ a pre ktoré $m \leq n$. Pre každé $j \in \{1, \dots, k\}$ označme $\varphi_{p_1, \dots, p_j}(n)$ počet všetkých tých čísel $m \in \mathbb{N}$, pre ktoré $m \leq n$ a m nie je deliteľné číslami $p_1, \dots, p_j$. Zrejme $\varphi_{p_1, \dots, p_k}(n) = \varphi(n)$.

Teraz dokážeme tento výrok: Pre každé $n \in \mathbb{N}$, $n \geq 2$, platí: Ak $n = p_1^{l_1} \dots p_k^{l_k}$, $p_1, \dots, p_k$ sú navzájom rôzne prvočísla, tak pre každé $j \in \{1, \dots, k\}$ $\varphi_{p_1, \dots, p_j}(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_j}\right)$.

Nepriamo. Nech existuje $n \in \mathbb{N}$, $n \geq 2$, pre ktoré uvedený výrok neplatí. Potom existuje najmenšie prirodzené číslo s touto vlastnosťou. Označme ho n_0 .

Nech $n_0 = p_1^{l_1} \dots p_k^{l_k}$, $p_1, \dots, p_k$ sú navzájom rôzne prvočísla, $k \geq 1$. Keďže pre n_0 uvedený výrok neplatí, existuje $j \in \{1, \dots, k\}$ také, že $\varphi_{p_1, \dots, p_j}(n_0) \neq n_0 \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_j}\right)$. Nech j_0 je najmenšie také číslo.

Uvažujme teraz o $\varphi_{p_1}(n_0)$. $\varphi_{p_1}(n_0)$ je počet prirodzených čísel $m \in \mathbb{N}$, $m \leq n$, pre ktoré $p_1 \nmid m$. Čísla $p_1, 2p_1, \dots, \frac{n_0}{p_1}p_1$ sú všetky kladné násobky p_1 menšie alebo rovné ako n_0 , t.j. všetky prirodzené čísla menšie alebo rovné ako n_0 , ktoré sú deliteľné číslom p_1 . Ich počet je $\frac{n_0}{p_1}$. Preto

$$\varphi_{p_1}(n_0) = n_0 - \frac{n_0}{p_1} = n_0 \left(1 - \frac{1}{p_1}\right).$$

Pre n_0 a $j = 1$ výrok platí, a preto $j_0 \geq 2$ a $j_0 - 1 \geq 1$. Z našej voľby j_0 vyplýva, že

$$\varphi_{p_1 \dots p_{j_0-1}}(n_0) = n_0 \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0-1}}\right)$$

a

$$\varphi_{p_1 \dots p_{j_0}}(n_0) \neq n_0 \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0}}\right)$$

$\varphi_{p_1 \dots p_{j_0-1}}(n_0)$ je počet všetkých tých $m \in \mathbb{N}$, $m \leq n_0$, ktoré nie sú deliteľné $p_1, \dots, p_{j_0-1}$. $\varphi_{p_1 \dots p_{j_0}}(n_0)$ dostaneme tak, že do $\varphi_{p_1 \dots p_{j_0-1}}(n_0)$ odrátame počet všetkých kladných násobkov čísla p_{j_0} , ktoré sú menšie alebo rovné ako n_0 a ktoré nie sú násobkami čísel $p_1, \dots, p_{j_0-1}$.

Všetky kladné násobky čísla p_{j_0} , menšie alebo rovné ako n_0 , sú $1 \cdot p_{j_0}, 2 \cdot p_{j_0}, \dots, l \cdot p_{j_0}, \dots, \frac{n_0}{p_{j_0}} \cdot p_{j_0}$, ich počet je $\frac{n_0}{p_{j_0}}$. Ak $i \in \{1, \dots, j_0 - 1\}$, tak $p_i \mid l \cdot p_{j_0} \Leftrightarrow p_i \mid l$, ekvivalentne $p_i \nmid l \cdot p_{j_0} \Leftrightarrow p_i \nmid l$. Pritom $1 \leq l \leq \frac{n_0}{p_{j_0}}$.

Teda $\varphi_{p_1, \dots, p_{j_0-1}}\left(\frac{n_0}{p_{j_0}}\right)$ je počet tých l , $1 \leq l \leq \frac{n_0}{p_{j_0}}$, ktoré nie sú deliteľné žiadnym z čísel $p_1, \dots, p_{j_0-1}$, ktorý je totožný s počtom všetkých kladných násobkov čísla p_{j_0} , ktoré sú $\leq n_0$ a nie sú deliteľné žiadnym z čísel $p_1, \dots, p_{j_0-1}$.

Číslo $\frac{n_0}{p_{j_0}} < n_0$ a pretože $j_0 \geq 2$, $\frac{n_0}{p_{j_0}} \geq p_1 \geq 2$. Preto platí

$$\varphi_{p_1, \dots, p_{j_0-1}}\left(\frac{n_0}{p_{j_0}}\right) = \frac{n_0}{p_{j_0}} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0-1}}\right).$$

Potom

$$\begin{aligned} \varphi_{p_1, \dots, p_{j_0}}(n_0) &= \varphi_{p_1, \dots, p_{j_0-1}}(n_0) - \varphi_{p_1, \dots, p_{j_0-1}}\left(\frac{n_0}{p_{j_0}}\right) = \\ &= n_0 \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0-1}}\right) - \frac{n_0}{p_{j_0}} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0-1}}\right) = \\ &= n_0 \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{j_0-1}}\right) \left(1 - \frac{1}{p_{j_0}}\right). \end{aligned}$$

Tým sme dokázali, že pre každé $n \geq 2$ ak $n = p_1^{l_1} \dots p_k^{l_k}$, tak pre každé $j \in \{1, \dots, k\}$ $\varphi_{p_1, \dots, p_j}(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_j}\right)$. Špeciálne,

$$\varphi(n) = \varphi_{p_1, \dots, p_k}(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_j}\right).$$

□

Cvičenia

- Dokážte, že platí:
 - $42 \mid n^7 - n$ pre každé $n \in \mathbb{Z}$,
 - $7 \mid n^{6k} - 1$ pre každé $k \in \mathbb{N}$ a $n \in \mathbb{Z}$ také, že $(n, 7) = 1$,
 - $n^{13} - n$, $n \in \mathbb{Z}$ je deliteľné každým z čísel 2,3,5,7,13.
- Ak p, q sú prvočísla, $p \neq q$, tak pre každé celé číslo a platí: $p \cdot q \mid a^{p \cdot q} - a^p - a^q + a$.
- Nájdite všetky riešenia rovnice $2^m - 3^n = 1$ v obore prirodzených čísel.
- Dokážte, že ak $n \in \mathbb{N}$ a $(10, n) = 1$, tak existuje $k \in \mathbb{N}$ tak, že $k \cdot n = 99 \dots 9$ - má všetky cifry rovné 9.
- Dokážte, že pre každé $n \in \mathbb{N}$ platí:
 - $n^{10} = 11k$ alebo $n^{10} = 11k + 1$
 - $n^{12} = 13k$ alebo $n^{12} = 13k + 1$
 - $n^{20} = 25k$ alebo $25k + 1$
- Nech $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a, n) = 1$. Nech k je najmenšie prirodzené číslo, pre ktoré $a^k \equiv 1 \pmod{n}$. Potom pre každé $l \in \mathbb{N}$ také, že $a^l \equiv 1 \pmod{n}$ platí, že $k \mid l$. Špeciálne, $k \mid \varphi(n)$. Dokážte!

7. Nájdite najmenšie prirodzené číslo n tak, aby
 - a) $253^n \equiv 1 \pmod{257}$
 - b) $2^n \equiv 1 \pmod{257}$.
8. Dokážte, že ak p, q sú prvočísla a $p \neq q$, tak $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ a $p^q + q^p \equiv p + q \pmod{pq}$.
9. Na príklade ukážte, že ak $(a, n) > 1$, tak nemusí platiť $a^{\varphi(n)} \equiv 1 \pmod{n}$.
10. Nájdite najmenšie prirodzené číslo, pre ktoré platí $6x \equiv 1 \pmod{35}$.
- 11*. Nájdite najväčší spoločný deliteľ množiny čísel $\{n^{13} - n, n \in \mathbb{Z}\}$.

1.5.1 Použitie Eulerovej vety v kryptografii (šifrovaní)

Jedna z metód šifrovania, ktorá sa v súčasnosti používa a je odolná voči odhaleniu je exponenciálna šifra, ktorej podstata je založená na poznatkoch z teórie čísel, vrátane Eulerovej vety.

Nech p je prvočíslo, $p > 2$ a $k > 1$ je prirodzené číslo, pre ktoré $(k, p-1) = 1$. Potom existuje q tak, že $k \cdot q \equiv 1 \pmod{p-1}$, $q \in \{1, \dots, p-2\}$, ktoré možno vypočítať pomocou Euklidovho algoritmu a vety o delení so zvyškom. Existujú $q', z \in \mathbb{Z}$ tak, že $1 = q'k + z(p-1)$ a existuje $q \in \{0, \dots, p-2\}$, že $q' \equiv q \pmod{p-1}$ (q je zvyšok po delení čísla q' číslom $p-1$). Zrejme $k \cdot q' \equiv 1 \pmod{p-1}$ a potom aj $k \cdot q \equiv 1 \pmod{p-1}$. Preto existuje $l \in \mathbb{Z}$ tak, že $k \cdot q - 1 = l(p-1)$ a teda $k \cdot q = 1 + l(p-1)$. Pretože $k > 1$, platí $k \cdot q > 1$. Preto $l \cdot (p-1) > 0$ a teda $l > 0$.

Ak $a \in \mathbb{Z}$, $0 < a < p$ a $a^k \equiv b \pmod{p}$, tak $b^q \equiv (a^k)^q = a^{k \cdot q} = a^{1+l(p-1)} = a \cdot (a^{p-1})^l \equiv a \pmod{p}$, lebo $a^{p-1} \equiv 1 \pmod{p}$, pretože $p \nmid a$.

Ak teda je dané prvočíslo $p > 2$ a prirodzené číslo $k > 1$, $(k, p-1) = 1$, (k sa nazýva kľúč šifry), $a \in \{1, \dots, p-1\}$ a poznáme (jednoznačne určené) číslo $b \in \{1, \dots, p-1\}$, pre ktoré $b \equiv a^k \pmod{p}$, tak pomocou k a p vieme určiť q a aj $a \equiv b^q \pmod{p}$, pričom ak $0 < a < p$, tak je toto číslo určené jednoznačne.

Príklad. Zašifrujeme (a odšifrujeme) slovo FIRE pomocou prvočísla $p = 5801$, kľúča $k = 61$ tak, že text rozdelíme na bloky po 2 písmená, t.j. po 4 cifry (aby sme dostali čísla menšie ako 5801). Najprv nahradíme písmená číslami: $A \rightarrow 00, B \rightarrow 01, C \rightarrow 02, D \rightarrow 03, E \rightarrow 04, F \rightarrow 05, G \rightarrow 06, H \rightarrow 07, I \rightarrow 08, J \rightarrow 09, K \rightarrow 10, L \rightarrow 11, M \rightarrow 12, N \rightarrow 13, O \rightarrow 14, P \rightarrow 15, Q \rightarrow 16, R \rightarrow 17, \dots, Z \rightarrow 25$. Teda FIRE prepíšeme na 05081704 a rozdelíme na 2 bloky po 4 cifry (=2 písmená).

0508 1704

Teraz máme

$$\begin{aligned} 508^{61} &\equiv 2713 \pmod{5801}, & 508 < 5801, \\ 1704^{61} &\equiv 3726 \pmod{5801}, & 1704 < 5801. \end{aligned}$$

Zašifrovaný text je teda 2713 3726.

Pre odšifrovanie určíme q také, že $61q \equiv 1 \pmod{5800}$, je to číslo $q = 1141$ (pomocou Euklidovho algoritmu vypočítame, že $1 = (-12) \cdot 5800 + 1141 \cdot 61$). Potom určíme, že

$$\begin{aligned} 2713^{1141} &\equiv 508 \pmod{5801} \\ 3726^{1141} &\equiv 1704 \pmod{5801} \end{aligned}$$

a dostaneme pôvodný text 0508 1704, po prepísaní do písmen FIRE.

Táto metóda je značne odolná voči rozlúšteniu šifry pomocou kryptoanalýzy. Aj v prípade, že kryptoanalytik pozná používané prvočíslo p , určenie k pomocou najrýchlejších známych algoritmov vyžaduje pre veľké p veľa času. Napríklad pre 100-ciferné číslo to pre najvýkonnejší počítač (v 80-tych rokoch) vyžadovalo 75 rokov, pre 200-ciferné prvočíslo dokonca $4 \cdot 10^9$ rokov.

1.6 Lineárne kongruencie s jednou neznámou

Lineárna kongruencia modulo n s jednou neznámou má tvar

$$a \cdot x \equiv b \pmod{n},$$

kde $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N}$ a x je neznáma.

Definícia 1.6.1. Zvyšková trieda $[c]_n$ modulo n sa nazýva *riešením* lineárnej kongruencie $a \cdot x \equiv b \pmod{n}$ ak $a \cdot c \equiv b \pmod{n}$.

Uvedená definícia je korektná, ak nezávisí od výberu reprezentanta zvyškovej triedy $[c]_n$. Nech $[c]_n = [d]_n$. Potom $c \equiv d \pmod{n}$, a preto aj $a \cdot c \equiv a \cdot d \pmod{n}$. Teda $a \cdot c \equiv b \pmod{n} \Leftrightarrow a \cdot d \equiv b \pmod{n}$. Ináč povedané, $[c]_n$ je riešenie kongruencie $a \cdot x \equiv b \pmod{n} \Leftrightarrow$ pre každé $d \in [c]_n$ platí $a \cdot d \equiv b \pmod{n}$.

Veta 1.6.2. Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $a \neq 0$ a $(a, n) = d$. Potom platí:

(1) Kongruencia $a \cdot x \equiv b \pmod{n}$ má riešenie $\Leftrightarrow d \mid b$

(2) Ak $d \mid b$, tak lineárna kongruencia $a \cdot x \equiv b \pmod{n}$ má práve d riešení.

Dôkaz. (1) $\Rightarrow$ Nech $[c]_n$ je riešenie danej kongruencie. Potom $a \cdot c \equiv b \pmod{n}$, a preto $n \mid a \cdot c - b$. Pretože $d \mid n$, platí aj $d \mid a \cdot c - b$ a pretože $d \mid a$, platí aj $d \mid a \cdot c$. Potom $d \mid a \cdot c - (a \cdot c - b) = b$.

$\Leftarrow$ Existujú $u, v \in \mathbb{Z}$ tak, že $d = u \cdot a + v \cdot n$. $d \mid b$, preto existuje $b' \in \mathbb{Z}$ tak, že $b = b' \cdot d$. Potom $b = b' \cdot d = b' \cdot u \cdot a + b' \cdot v \cdot n$. Teda $a(b' \cdot u) - b = (-b' \cdot v) \cdot n$, t.j. $n \mid a(b' \cdot u) - b$. Potom $a \cdot (b' \cdot u) \equiv b \pmod{n}$ a $[b' \cdot u]_n$ je riešenie danej kongruencie.

(2) Pretože $d \mid b$, existuje riešenie $[c_0]_n$ danej kongruencie. $d \mid n$ a preto existuje $l \in \mathbb{N}$ také, že $n = l \cdot d$. Položme $c_1 = c_0 + l, c_2 = c_0 + 2l, \dots, c_{d-1} = c_0 + (d-1) \cdot l$. Dokážeme, že $[c_0]_n, [c_1]_n, \dots, [c_{d-1}]_n$ sú navzájom rôzne riešenia danej kongruencie a že sú to všetky riešenia. $d \mid a$ a teda existuje $a' \in \mathbb{Z}$ tak, že $a = a' \cdot d$. Pre každé $i = 0, \dots, d-1$ $a \cdot c_i = a \cdot c_0 + a \cdot i \cdot l = a \cdot c_0 + a' \cdot i \cdot d \equiv a \cdot c_0 \pmod{n}$, a preto $a \cdot c_i \equiv b \pmod{n}$.

Teda pre každé $i = 0, \dots, d-1$ $[c_i]_n$ je riešenie $a \cdot x \equiv b \pmod{n}$. Nech $0 \leq i < j \leq d-1$. Potom $0 < c_j - c_i = (j-i) \cdot l \leq j \cdot l < d \cdot l = n$, a preto $n \nmid c_j - c_i$. Teda $c_i \not\equiv c_j \pmod{n}$, t.j. $[c_i]_n \neq [c_j]_n$.

Nech $[c]_n$ je riešenie danej kongruencie. Potom $a \cdot c \equiv b \pmod{n}$ a preto $a \cdot c \equiv a \cdot c_0 \pmod{n}$. Potom $n = l \cdot d \mid a \cdot c - a \cdot c_0 = a' \cdot d(c - c_0)$. Potom $l \mid a'(c - c_0)$. Ale $(a', l) = 1$, a preto $l \mid c - c_0$. Potom existuje $z \in \mathbb{Z}$ $c = c_0 + z \cdot l$. Podľa vety o delení so zvyškom existujú $s, j \in \mathbb{Z}$ tak, že $z = d \cdot s + j$ a $0 \leq j \leq d-1$. Potom $c = c_0 + j \cdot l + s \cdot d \equiv c_0 + j \cdot l \equiv c_0 + j \cdot l = c_j \pmod{n}$. Teda existuje $j \in \{0, \dots, d-1\}$ tak, že $[c_i]_n = [c_j]_n$. $\square$

Príklad. 1. Vyriešte lineárnu kongruenciu $20x \equiv 28 \pmod{12}$.

Riešenie. $(20, 12) = 4$, $4 \mid 28$ a teda existujú práve 4 riešenia.

$$\begin{aligned} 4 &= (-1) \cdot 20 + 2 \cdot 12 \quad / : 4 \\ 20(-7) + 14 \cdot 12 &= 28 \\ 20(-7) &\equiv 28 \pmod{12} \end{aligned}$$

$$c_0 = -7, c_1 = -7 + 3 = -4, c_2 = -7 + 2 \cdot 3 = -1, c_3 = -7 + 3 \cdot 3 = 2$$

Riešenia sú $[-7] = [5]$, $[-4] = [8]$, $[-1] = [11]$, $[2]$.

Pretože $20x \equiv 8x \pmod{12}$ a $28 \equiv 4 \pmod{12}$, je daná kongruencia ekvivalentná s kongruenciou $8x \equiv 4 \pmod{12}$.

2. Vyriešte kongruenciu $15x \equiv -66 \pmod{18}$.

$(15, 18) = 3$, $3 \mid -66$ kongruencia má 3 riešenia.

$$-66 \equiv 6 \pmod{18}$$

$$15x \equiv 6 \pmod{18}$$

$$3 = (-1) \cdot 15 + 1 \cdot 18$$

$$15 \cdot (-2) + 2 \cdot 18 = 6$$

$$15 \cdot (-2) \equiv 6 \pmod{18}$$

$[-2] = [16]$ je riešenie. $18 : 3 = 6$, ďalšie riešenia sú $[4]$ a $[10]$.

Cvičenia

1. Vyriešte lineárne kongruencie s jednou neznámou:

- a) $10x \equiv 14 \pmod{12}$
- b) $7x \equiv 46 \pmod{21}$
- c) $15x \equiv -72 \pmod{18}$
- d) $14x \equiv -63 \pmod{35}$

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

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

4. Do kongruencie $10x \equiv 15 \pmod{n}$ doplňte za n také číslo, aby:

- a) kongruencia nemala riešenie,
- b) kongruencia mala práve 2 riešenia.

1.7 Aritmetické funkcie φ , τ , σ

Definícia 1.7.1. (1) Ľubovoľné zobrazenie $f: \mathbb{N} \rightarrow \mathbb{R}$ sa nazýva *aritmetická funkcia*.

(2) Aritmetická funkcia $f: \mathbb{N} \rightarrow \mathbb{R}$ sa nazýva *multiplikatívna*, ak platí:

- (a) Existuje $n \in \mathbb{N}$ tak, že $f(n) \neq 0$.
- (b) Ak $m, n \in \mathbb{N}$ a $(m, n) = 1$, tak $f(m \cdot n) = f(m) \cdot f(n)$,

Príklad. Eulerova funkcia φ je aritmetická funkcia a ukážeme, že je multiplikatívna.

Funkcia $\pi: \mathbb{N} \rightarrow \mathbb{R}$, $\pi(n)$ je počet všetkých prvočísel menších alebo rovných ako n je aritmetická funkcia, nie je multiplikatívna. $\pi(2) = 1$, $\pi(3) = 2$, $\pi(6) = 3$, $(2, 3) = 1$, $6 = 2 \cdot 3$, $3 = \pi(6) \neq \pi(2) \cdot \pi(3) = 2$

Lema 1.7.2. Ak f je multiplikatívna aritmetická funkcia, tak $f(1) = 1$.

Dôkaz. Existuje $n \in \mathbb{N}$, $f(n) \neq 0$. $(1, n) = 1$. $1 \cdot f(n) = f(1 \cdot n) = f(1) \cdot f(n)$. Preto $f(1) = 1$. $\square$

Definícia 1.7.3. Pre každé $n \in \mathbb{N}$ $\tau(n)$ označuje počet všetkých kladných deliteľov čísla n a $\sigma(n)$ súčet všetkých kladných deliteľov čísla n .

Príklad. $\tau(1) = 1$, $\tau(2) = 2$, $\tau(8) = 4$, pre každé prvočíslo p $\tau(p) = 2$.
 $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(8) = 15$, pre každé prvočíslo p $\sigma(p) = p + 1$.

$\tau, \sigma: \mathbb{N} \rightarrow \mathbb{R}$ sú aritmetické funkcie.

Veta 1.7.4. Nech $n \in \mathbb{N}$, $n > 1$ a $n = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad čísla n na prvočísla. Potom platí:

$$(1) \tau(n) = (l_1 + 1) \dots (l_k + 1)$$

$$(2) \sigma(n) = \frac{p_1^{l_1+1}-1}{p_1-1} \dots \frac{p_k^{l_k+1}-1}{p_k-1} = (p_1^{l_1} + p_1^{l_1-1} + \dots + p_1 + 1) \dots (p_k^{l_k} + p_k^{l_k-1} + \dots + p_k + 1)$$

Dôkaz. (1) $d \mid n \Leftrightarrow d = p_1^{t_1} \dots p_k^{t_k}$, kde $0 \leq t_i \leq l_i$ pre $i = 1, \dots, k$. Teda $\tau(n) = (l_1 + 1) \dots (l_k + 1)$.

$$(2) (p_1^{l_1} + p_1^{l_1-1} + \dots + p_1 + 1)(p_2^{l_2} + p_2^{l_2-1} + \dots + p_2 + 1) \dots (p_k^{l_k} + p_k^{l_k-1} + \dots + p_k + 1) = \sum_{0 \leq t_i \leq l_i} p_1^{t_1} \dots p_k^{t_k} = \sum_{d \mid n} d = \sigma(n) \quad \square$$

Veta 1.7.5. Funkcie φ, τ, σ sú multiplikatívne.

Dôkaz. $\varphi(1) = \tau(1) = \sigma(1) = 1$, t.j. pre $1 \in \mathbb{N}$ je $\varphi(1) \neq 0$, $\tau(1) \neq 0$, $\sigma(1) \neq 0$.

Nech $m, n \in \mathbb{N}$, $(m, n) = 1$. Ak $m = 1$, tak pre každé $f \in \{\varphi, \tau, \sigma\}$ platí:

$$f(1.n) = f(n) = 1.f(n) = f(1).f(n).$$

Podobne pre $n = 1$.

Nech $m > 1$ aj $n > 1$. Potom $m = p_1^{l_1} \dots p_k^{l_k}$, $n = q_1^{r_1} \dots q_s^{r_s}$, $p_1, \dots, p_k$ aj $q_1, \dots, q_s$ sú navzájom rôzne prvočísla. Pretože $(m, n) = 1$, $\{p_1, \dots, p_k\} \cap \{q_1, \dots, q_s\} = \emptyset$ a teda $p_1, \dots, p_k, q_1, \dots, q_s$ sú navzájom rôzne prvočísla a $m.n = p_1^{l_1} \dots p_k^{l_k} q_1^{r_1} \dots q_s^{r_s}$ je kanonický rozklad čísla $m.n$ na prvočísla.

Podľa vety 1.5.5

$$\begin{aligned} \varphi(m.n) &= m.n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_s}\right) = \\ &= m \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) . n \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_s}\right) = \varphi(m). \varphi(n) \end{aligned}$$

Podľa vety 1.7.4

$$\begin{aligned} \tau(m.n) &= (l_1 + 1) \dots (l_k + 1)(r_1 + 1) \dots (r_s + 1) = \tau(m). \tau(n) \\ \sigma(m.n) &= (p_1^{l_1} + p_1^{l_1-1} + \dots + p_1 + 1) \dots (p_k^{l_k} + p_k^{l_k-1} + \dots + p_k + 1)(q_1^{r_1} + q_1^{r_1-1} + \dots + q_1 + 1) \dots (q_s^{r_s} + q_s^{r_s-1} + \dots + q_s + 1) = \sigma(m). \sigma(n) \quad \square \end{aligned}$$

Veta 1.7.6. Pre Eulerovu funkciu φ platí:

$$\sum_{d \mid n} \varphi(d) = n.$$

Dôkaz. $n = 1. \sum_{d \mid 1} \varphi(d) = \varphi(1) = 1$.

Nech $n > 1$, $n = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad n . $d \mid n \Leftrightarrow d = p_1^{t_1} \dots p_k^{t_k}$, $0 \leq t_i \leq l_i$. Pretože ak $i \neq j$, tak $(p_i^{t_i}, p_j^{t_j}) = 1$,

$$\varphi(d) = \varphi(p_1^{t_1}) \dots \varphi(p_k^{t_k}).$$

Potom

$$\begin{aligned} \sum_{d \mid n} \varphi(d) &= \sum_{0 \leq t_i \leq l_i} \varphi(p_1^{t_1} \dots p_k^{t_k}) = \sum_{0 \leq t_i \leq l_i} \varphi(p_1^{t_1}) \dots \varphi(p_k^{t_k}) = \\ &= (1 + \varphi(p_1) + \dots + \varphi(p_1^{l_1}))(1 + \varphi(p_2) + \dots + \varphi(p_2^{l_2})) \dots (1 + \varphi(p_k) + \dots + \varphi(p_k^{l_k})). \end{aligned}$$

Pre každé prvočíslo p a $l \in \mathbb{N}$ $\varphi(p^l) = p^l - p^{l-1}$, lebo $p, 2p, \dots, p^{l-1}p$ sú všetky čísla deliteľné p , ktoré sú menšie alebo rovné p^l a ich počet je p^{l-1} . Potom

$$\begin{aligned} \sum_{d \mid n} \varphi(d) &= (1 + (p_1 - 1) + (p_1^2 - p_1) + \dots + (p_1^{l_1} - p_1^{l_1-1})) \cdot \\ &\quad (1 + (p_2 - 1) + (p_2^2 - p_2) + \dots + (p_2^{l_2} - p_2^{l_2-1})) \dots \\ &\quad \dots (1 + (p_k - 1) + (p_k^2 - p_k) + \dots + (p_k^{l_k} - p_k^{l_k-1})) = p_1^{l_1} \dots p_k^{l_k} = n. \end{aligned}$$

□

Číslo $n \in \mathbb{N}$ sa nazýva *dokonalé*, ak $\sigma(n) = 2n$, t.j. súčet vlastných deliteľov čísla n je rovný n . Dokonalé čísla sú napríklad $6=1+2+3$ ($\sigma(6) = 12$), 28 ($\sigma(28) = 56$), 496 , 8128 . Prvá časť nasledujúcej vety bola známa už Euklidovi.

Veta 1.7.7. Ak $2^n - 1$ je prvočíslo, tak $a = 2^{n-1}(2^n - 1)$ je dokonalé a každé párne dokonalé číslo má tento tvar.

Dôkaz. Ak $2^n - 1$ je prvočíslo a $a = 2^{n-1}(2^n - 1)$. Potom

$$\sigma(a) = \sigma(2^{n-1}(2^n - 1)) = \frac{2^n - 1}{2 - 1} (2^n - 1 + 1) = 2^n (2^n - 1) = 2a.$$

Nech teraz a je párne dokonalé číslo. Potom $a = m \cdot 2^{n-1}$, $n \geq 2$, $m > 0$, m je nepárne. Pretože a je dokonalé, platí

$$m \cdot 2^n = 2a = \sigma(a) = \sigma(m \cdot 2^{n-1}) = \sigma(m) \sigma(2^{n-1}) = \sigma(m) (2^n - 1).$$

Preto $\sigma(m) = \frac{m \cdot 2^n}{2^n - 1}$ - je to prirodzené číslo, $(2^n, 2^n - 1) = 1$, a preto $2^n - 1 \mid m$. Potom $\frac{m}{2^n - 1}$ je prirodzené číslo a $\frac{m}{2^n - 1} \mid m$. Naviac,

$$\sigma(m) = \frac{m \cdot 2^n}{2^n - 1} = \frac{m(2^n - 1) + m}{2^n - 1} = m + \frac{m}{2^n - 1}.$$

Pretože m a $\frac{m}{2^n - 1}$ sú kladné delitele čísla m , $m \neq \frac{m}{2^n - 1}$ (lebo $n > 2$ a preto $2^n - 1 > 1$) a $\sigma(m)$ je súčtom všetkých kladných deliteľov čísla m , m a $\frac{m}{2^n - 1}$ sú všetky delitele čísla m . Teda m má práve dva kladné delitele a preto m je prvočíslo. Potom, zrejme, $\frac{m}{2^n - 1} = 1$, teda $m = 2^n - 1$ je prvočíslo a $a = 2^{n-1}(2^n - 1)$. □

Pretože nie je známe, či Mersennových prvočísel je nekonečne veľa, nie je známe ani to, či párnych dokonalých čísel je nekonečne veľa. V súčasnosti nie je známe ani jedno nepárne dokonalé číslo. Je dokázané, že ak existuje, tak má aspoň 8 prvočíselných deliteľov a musí byť väčšie ako 10^{80} (Cohen). V r. 1977 bol avizovaný výsledok, že také číslo musí byť väčšie ako 10^{200} ale dôkaz nebol publikovaný. Naznačuje to však skutočnosť, že asi neexistuje nepárne dokonalé číslo.

Cvičenia

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.

Nech p je prvočíslo a $a.x \equiv b \pmod{p}$ je lineárna kongruencia. Ak $(a, p) = 1$, tak daná kongruencia má práve jedno riešenie. Ak teda $a.x \equiv b \pmod{p}$ má viac ako jedno riešenie, tak $(a, p) \neq 1$ a teda $(a, p) = p$. Potom, keďže má riešenie, platí $p \mid b$ a pretože $(a, p) = p$, platí tiež $p \mid a$. Okrem lineárnych kongruencií s jednou neznámou možno uvažovať o kongruenciách vyššieho stupňa,

$$f(x) \equiv 0 \pmod{n}, \text{ kde } f(x) = a_n x^n + \dots + a_1 x + a_0$$

a $a_0, a_1, \dots, a_n \in \mathbb{Z}$ s neznámou x . Pre takéto kongruencie podľa prvočíselného modulu platí analógia horeuvedeného výsledku pre lineárne kongruencie.

Veta 1.8.1 (Lagrangeova). *Nech $f(x) = a_n x^n + \dots + a_1 x + a_0$ je polynóm s celočíselnými koeficientami, $a_n \neq 0$ a p je prvočíslo. Potom ak kongruencia*

$$f(x) \equiv 0 \pmod{p}$$

má viac ako n riešení, tak pre každé $i = 1, \dots, n$

$$p \mid a_i.$$

Dôkaz. Pripomeňme, že riešením kongruencie $f(x) \equiv 0 \pmod{p}$ je zvyšková trieda $[c]_p$, pre ktorú platí, že $f(c) \equiv 0 \pmod{p}$. Vetu dokážeme indukciou vzhľadom na stupeň n polynómu $f(x)$.

Pre $n = 1$ máme kongruenciu

$$a_1 x + a_0 \equiv 0 \pmod{p}.$$

Nech $[c_0]_p, [c_1]_p$ sú dve rôzne riešenia tejto kongruencie. Potom $c_0 \not\equiv c_1 \pmod{p}$ a $a_1 c_0 + a_0 \equiv 0 \pmod{p}$, $a_1 c_1 + a_0 \equiv 0 \pmod{p}$. Potom $a_1 c_0 + a_0 \equiv a_1 c_1 + a_0 \pmod{p}$, a preto

$$a_1 c_0 \equiv a_1 c_1 \pmod{p}.$$

Ak by platilo $(a_1, p) = 1$, tak dostaneme $c_0 \equiv c_1 \pmod{p}$, čo je v spore s predpokladom. Preto platí $(a_1, p) \neq 1$ a teda $p \mid a_1$. Potom ale $a_1 \equiv 0 \pmod{p}$, a preto $a_1 c_0 \equiv 0 \pmod{p}$. Potom $a_1 c_0 + a_0 \equiv a_0 \pmod{p}$ a súčasne $a_1 c_0 + a_0 \equiv 0 \pmod{p}$. Teda $a_0 \equiv 0 \pmod{p}$, t.j. $p \mid a_0$.

Nech teraz tvrdenie platí pre $n \geq 1$. Dokážeme, že potom platí aj pre $n + 1$. Nech

$$f(x) = a_{n+1} x^{n+1} + \dots + a_1 x + a_0$$

a kongruencia

$$a_{n+1} x^{n+1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

má $n + 2$ rôznych riešení $[c_0]_p, [c_1]_p, \dots, [c_{n+1}]_p$. Teda pre každé $i = 0, \dots, n + 1$

$$f(c_i) \equiv 0 \pmod{p}.$$

Vydělíme polynóm $f(x)$ polynómom $x - c_0$ (so zvyškom) a dostaneme $f(x) = (x - c_0) \cdot g(x) + r$, kde $g(x) = b_n x^n + \dots + b_0$, $r \in \mathbb{Z}$. Zrejme platí $b_n = a_{n+1} \neq 0$ a $r = f(c_0)$. ($f(c_0) = (c_0 - c_0)g(c_0) + r = 0g(c_0) + r = r$) Teda $g(x)$ je polynóm n -tého stupňa.

Nech i je ľubovoľné číslo $1 \leq i \leq n + 1$. Potom $f(c_i) = (c_i - c_0)g(c_i) + f(c_0) \equiv 0 \pmod{p}$. Pretože $f(c_0) \equiv 0 \pmod{p}$, dostávame $(c_i - c_0)g(c_i) \equiv 0 \pmod{p}$ a teda $p \mid (c_i - c_0)g(c_i)$. Pretože $[c_i]_p \neq [c_0]_p$ platí $c_i \not\equiv c_0 \pmod{p}$ a teda $p \nmid c_i - c_0$. Pretože p je prvočíslo, dostávame $p \mid g(c_i)$ a teda

$$g(c_i) \equiv 0 \pmod{p}.$$

Teda kongruencia $b_n x^n + \dots + b_0 \equiv 0 \pmod{p}$ má $n + 1$ rôznych riešení $[c_1]_p, \dots, [c_{n+1}]_p$ a podľa indukčného predpokladu potom $p \mid b_i$ pre $i = 0, 1, \dots, n$.

Z platnosti

$$a_{n+1}x^{n+1} + a_n x^n + \dots + a_1 x + a_0 = (x - c_0)(b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) + f(c_0),$$

porovnaním koeficientov polynómov, dostávame: $a_{n+1} = b_n$, $a_n = b_{n-1} - b_n c_0$, $a_{n-1} = b_{n-2} - b_{n-1} c_0, \dots, a_2 = b_1 - b_2 c_0$, $a_1 = b_0 - b_1 c_0$, $a_0 = f(c_0) - b_0 c_0$. Pretože $p \mid b_n, b_{n-1}, \dots, b_0, f(c_0)$, je zrejme, že potom $p \mid a_{n+1}, a_n, \dots, a_1, a_0$. $\square$

Nasledujúca Wilsonova veta, ktorú však ako prvý dokázal Lagrange, charakterizuje prvočísla.³

Veta 1.8.2 (Wilsonova). Číslo $p > 1$ je prvočíslo vtedy a len vtedy, keď

$$(p - 1)! \equiv -1 \pmod{p}.$$

Dôkaz. Pre $p = 2$ a $p = 3$ výrok zrejme platí. Nech $p > 3$. Pre každé $k \in \{1, 2, \dots, p - 1\}$ je $(k, p - 1) = 1$ a preto existujú $u, v \in \mathbb{Z}$, pre ktoré $k \cdot u + p \cdot v = 1$ a teda $k \cdot u \equiv 1 \pmod{p}$. Ďalej, existuje k' také, že $k' \in \{1, 2, \dots, p - 1\}$ a $u \equiv k' \pmod{p}$. Potom aj $k \cdot k' \equiv 1 \pmod{p}$. Ak $m \in \{1, 2, \dots, p - 1\}$ a $k \cdot m \equiv 1 \pmod{p}$, tak $k \cdot k' \equiv k \cdot m \pmod{p}$ a pretože $(k, p) = 1$, dostávame, že $k' \equiv m \pmod{p}$. Potom $p \mid |k' - m|$, $|k' - m| < p$ a teda $|k' - m| = 0$, t. j. $k' = m$. Teda pre každé $k \in \{1, 2, \dots, p - 1\}$ existuje práve jedno $k' \in \{1, 2, \dots, p - 1\}$ pre ktoré $k \cdot k' \equiv 1 \pmod{p}$. Ak $k = k'$, tak $k \cdot k \equiv 1 \pmod{p}$. Potom $p \mid k^2 - 1 = (k - 1) \cdot (k + 1)$ a pretože p je prvočíslo, platí $p \mid k - 1$ alebo $p \mid k + 1$. Ale $k - 1 < p$, $0 < k + 1 \leq p$, preto $k - 1 = 0$ alebo $k + 1 = p$. Teda ak $k \in \{2, \dots, p - 2\}$, tak $k \neq k'$. Preto $\{1, 2, \dots, p - 1\} = \{1, k_1, k'_1, \dots, k_{\frac{p-3}{2}}, k'_{\frac{p-3}{2}}, p - 1\}$, kde pre každé $i \in \{1, \dots, \frac{p-3}{2}\}$ platí $k_i \cdot k'_i \equiv 1 \pmod{p}$. Potom $(p - 1)! = 1 \cdot 2 \cdot \dots \cdot (p - 1) = 1 \cdot k_1 \cdot k'_1 \cdot \dots \cdot k_{\frac{p-3}{2}} \cdot k'_{\frac{p-3}{2}} \cdot (p - 1)$ a $1 \cdot k_1 \cdot k'_1 \cdot \dots \cdot k_{\frac{p-3}{2}} \cdot k'_{\frac{p-3}{2}} \cdot (p - 1) \equiv p - 1 \pmod{p}$. Teda $(p - 1)! \equiv p - 1 \pmod{p}$. Súčasne platí $p - 1 \equiv -1 \pmod{p}$ a teda máme $(p - 1)! \equiv -1 \pmod{p}$.

$\Leftarrow$ Nech by p bolo zložené. Potom existuje $m \in \mathbb{N}$, $1 < m < p$, pre ktoré $m \mid p$. Pretože $m \leq p - 1$, m sa vyskytuje medzi činiteľmi vystupujúcimi v $(p - 1)!$ a preto $m \mid (p - 1)!$. Podľa predpokladu, $(p - 1)! \equiv -1 \pmod{p}$, preto $p \mid (p - 1)! + 1$ a pretože $m \mid p$, platí tiež $m \mid (p - 1)! + 1$. Ale potom $m \mid (p - 1)! + 1 - (p - 1)! = 1$ a z toho dostávame, že $m \leq 1$, čo je spor. Teda p je prvočíslo. $\square$

³V [1] možno nájsť dôkaz Wilsonovej vety použitím Vandermondovho determinantu.

Kapitola 2

g -adické rozvoje reálnych čísel. Kritéria iracionálnosti.

V tejto kapitole sa budeme zaoberať reálnymi číslami. Ak a, b sú reálne čísla tak $[a, b) = \{r \in \mathbb{R} : a \leq r < b\}$.

Najprv pripomeňme pojem racionálneho čísla a pojem celá časť reálneho čísla.

Reálne číslo a sa nazýva *racionálne*, ak existuje $z \in \mathbb{Z}$ a $n \in \mathbb{N}$ tak, že $a = \frac{z}{n}$ (ekvivalentne: existuje $n \in \mathbb{N}$ tak, že $a \cdot n \in \mathbb{Z}$). Je známe, že napríklad číslo $\sqrt{2}$ nie je racionálne číslo.

Celé číslo z sa nazýva *celá časť* reálneho čísla a , ak platí: $z \leq a < z + 1$. Označenie: $[a]$. Teda $[a] \in \mathbb{Z}$ a $[a] \leq a < [a] + 1$. Pretože pre každé reálne číslo existuje práve jedno celé číslo $z \in \mathbb{Z}$, pre ktoré $z \leq a < z + 1$, každé reálne číslo má práve jednu celú časť (vyplýva to napríklad z toho, že $\mathbb{R} = \bigcup_{z \in \mathbb{Z}} [z, z + 1)$ a ak $z_1 < z_2$, tak $z_1 + 1 \leq z_2$ a preto $[z_1, z_1 + 1) \cap [z_2, z_2 + 1) = \emptyset$). Napríklad, $[\frac{10}{3}] = 3$, $[-\frac{10}{3}] = -4$, $[\sqrt{2}] = 1$, $[3] = 3$.

Je zrejmé, že $0 \leq a - [a] < 1$ a ak $a \geq 0$, tak $[a] \in \mathbb{N}_0$.

Je známe, že ak $g \in \mathbb{N}$ a $g \geq 2$, tak pre každé $n \in \mathbb{N}$ platí $n < g^n$ (dokáže sa to matematickou indukciou). Potom, ak $r \in \mathbb{R}$ a $r > 0$, tak existuje $n \in \mathbb{N}$, pre ktoré $n \geq \frac{1}{r}$ a potom $\frac{1}{g^n} < \frac{1}{n} \leq r$ (toto v nasledujúcej časti použijeme).

Pripomeňme, že $\mathbb{R}$ označuje množinu všetkých reálnych čísel, $\mathbb{R}^+ = \{a \in \mathbb{R} : a > 0\}$ a $\mathbb{R}_0^+ = \mathbb{R}^+ \cup \{0\}$. $\mathbb{Q}$ označuje množinu všetkých racionálnych čísel, $\mathbb{Q}^+ = \{r \in \mathbb{Q} ; r > 0\}$, $\mathbb{Q}_0^+ = \mathbb{Q}^+ \cup \{0\}$.

2.1 g -adický rozvoj reálneho čísla

Užitočným nástrojom pri štúdiu g -adických rozvojev reálnych čísel je pojem nekonečného číselného radu, jeho súčtu a s tým súvisiaci pojem konvergenzie postupnosti. Pretože tieto pojmy nemáme k dispozícii, urobíme to bez nich (menej výhodným a elegantným spôsobom).

Reálne číslo $\frac{9}{8}$ môžeme vyjadriť aj v tvare $1,125 = 1 + \frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3} = [\frac{9}{8}] + \frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3}$, pričom platí $1, 2, 5 \in \{0, 1, \dots, 9\}$, $0 \leq \frac{9}{8} - [\frac{9}{8}] = \frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3} < 1$, $0 \leq \frac{9}{8} - ([\frac{9}{8}] + \frac{1}{10}) = \frac{2}{10^2} + \frac{5}{10^3} < \frac{1}{10}$, $0 \leq \frac{9}{8} - ([\frac{9}{8}] + \frac{1}{10} + \frac{2}{10^2}) = \frac{5}{10^3} < \frac{1}{10^2}$.

Stretli sme sa už aj s tým, že $\frac{5}{3} = 1,666\dots = [\frac{5}{3}], 666\dots = [\frac{5}{3}] + \frac{6}{10} + \frac{6}{10^2} + \frac{6}{10^3} + \dots + \frac{6}{10^k} + \dots$. Aj v tomto prípade platí že všetky číslice za desatinnou čiarkou sú z množiny $\{0, 1, \dots, 9\}$ a platí $0 \leq \frac{5}{3} - [\frac{5}{3}] < 1$, $0 \leq \frac{5}{3} - ([\frac{5}{3}] + \frac{6}{10}) < \frac{1}{10}$, $0 \leq \frac{5}{3} - ([\frac{5}{3}] + \frac{6}{10} + \frac{6}{10^2}) < \frac{1}{10^2}$, $\dots$, $0 \leq \frac{5}{3} - ([\frac{5}{3}] + \frac{6}{10} + \frac{6}{10^2} + \dots + \frac{6}{10^k}) < \frac{1}{10^k}$, $\dots$. Teda číslo $\frac{5}{3}$ je tu vyjadrené pomocou čísla $[\frac{5}{3}]$ a nekonečnej postupnosti $6, 6, 6, \dots, 6, \dots$ a číslo $\frac{9}{8}$ pomocou čísla $[\frac{9}{8}]$ a konečnej postupnosti

1, 2, 5, ktorú však môžeme doplniť na nekonečnú postupnosť $1, 2, 5, 0, 0, \dots, 0, \dots$. Pritom platí, že všetky členy týchto postupností patria do množiny $\{0, 1, \dots, 9 = 10 - 1\}$ a sú splnené vyššie uvedené nerovnosti. Takéto vyjadrenia reálnych čísel sa nazývajú dekadické rozvoje a ak číslo 10 nahradíme prirodzeným číslom $g \geq 2$ tak dostaneme analogicky g -adické rozvoje s podobnými vlastnosťami.

Definícia 2.1.1. Nech $g \in \mathbb{N}$, $g \geq 2$, $r \in \mathbb{R}_0^+$ a $\{c_k\}_{k=1}^\infty$ je (nekonečná) postupnosť celých nezáporných čísel, ktorá má nasledujúce vlastnosti:

- (1) Pre každé $k \in \mathbb{N}$ platí $c_k \in \{0, 1, \dots, g-1\}$ (t. j. $0 \leq c_k \leq g-1$).
- (2) Pre každé $k \in \mathbb{N}$ platí $0 \leq r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) < \frac{1}{g^k}$.

Potom číslo r zapisujeme v tvare $r = ([r], c_1 c_2 \dots c_k \dots)_g$ (alebo tiež $r = [r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k} + \dots = [r] + \sum_{k=1}^\infty \frac{c_k}{g^k}$) a vyjadrenie $r = ([r], c_1 c_2 \dots c_k \dots)_g$ sa nazýva g -adický rozvoj čísla r .

Z definície je zrejmé, že ak $r \in \mathbb{R}_0^+$ a $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj r , tak pre každé $k \in \mathbb{N}$ platí, že $[r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k} \leq r$.

Veta 2.1.2. Nech $g \in \mathbb{N}$, $g \geq 2$. Potom platí:

- (1) Pre každé reálne číslo $r \in \mathbb{R}_0^+$ existuje práve jedna postupnosť $\{c_k\}_{k=1}^\infty$ celých nezáporných čísel, tak, že $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla r .
- (2) Ak $r, s \in \mathbb{R}_0^+$, $r \neq s$, $r = ([r], c_1 c_2 \dots c_k \dots)_g$ a $s = ([s], d_1 d_2 \dots d_k \dots)_g$ sú g -adické rozvoje čísel r , resp. s , tak $[r] \neq [s]$ alebo existuje $m \in \mathbb{N}$ tak, že $c_m \neq d_m$ (t. j. dve rôzne čísla majú rôzne g -adické rozvoje).

Dôkaz. (1) *Existencia.* Položme $r_1 = r - [r]$. Zrejme $0 \leq r_1 < 1$ a $r = [r] + r_1$.

Ďalej, $c_1 = [g \cdot r_1]$, $r_2 = g \cdot r_1 - c_1$. Platí $0 \leq r_2 < 1$, $gr_1 = c_1 + r_2$. Z $0 \leq gr_1 < g$ vyplýva $0 \leq [gr_1] < g$, t.j. $0 \leq c_1 < g$.

$c_2 = [g \cdot r_2]$, $r_3 = gr_2 - c_2$. Platí $0 \leq r_3 < 1$, $gr_2 = c_2 + r_3$, $0 \leq [gr_2] \leq gr_2 < g$, t.j. $0 \leq c_2 < g$. Takto možno pokračovať matematickou indukciou, t.j. predpokladajme, že máme definované c_n , $0 \leq c_n < g$, r_{n+1} , $0 \leq r_{n+1} < 1$. Potom definujeme

$$c_{n+1} = [g \cdot r_{n+1}], \quad r_{n+2} = gr_{n+1} - c_{n+1},$$

pričom platí $0 \leq r_{n+2} < 1$, $g \cdot r_{n+1} = c_{n+1} + r_{n+2}$ a $0 \leq [gr_{n+1}] \leq gr_{n+1} < g$, t.j. $0 \leq c_{n+1} < g$.

Tým je pre každé $k \in \mathbb{N}$ definované $c_k \in \{0, 1, \dots, g-1\}$ a $r_k \in [0, 1)$, pričom platí $gr_k = c_k + r_{k+1}$ a $r = [r] + r_1$. Potom

$$\begin{aligned} r &= [r] + r_1 = [r] + \frac{gr_1}{g} = [r] + \frac{c_1 + r_2}{g} = [r] + \frac{c_1}{g} + \frac{r_2}{g} = \\ &= [r] + \frac{c_1}{g} + \frac{gr_2}{g^2} = [r] + \frac{c_1}{g} + \frac{c_2}{g^2} + \frac{r_3}{g^2} = \dots = [r] + \frac{c_1}{g} + \frac{c_2}{g^2} + \dots + \frac{c_k}{g^k} + \frac{r_{k+1}}{g^k} \end{aligned}$$

Teda pre každé $k \in \mathbb{N}$ platí $r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) = \frac{r_{k+1}}{g^k}$. Pretože $0 \leq r_{k+1} < 1$, máme $0 \leq \frac{r_{k+1}}{g^k} < \frac{1}{g^k}$ a teda $0 \leq r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) < \frac{1}{g^k}$.

Jednoznačnosť. Nech existujú dve rôzne postupnosti $\{c_k\}_{k=1}^\infty$ a $\{d_k\}_{k=1}^\infty$, pre ktoré platí $r = ([r], c_1 c_2 \dots c_n \dots)_g$ a súčasne $r = ([r], d_1 d_2 \dots d_n \dots)_g$. Pretože postupnosti sa nerovnajú, existuje $m \in \mathbb{N}$ tak, že $c_m \neq d_m$. Nech $k \in \mathbb{N}$ je najmenšie také číslo, pre ktoré $c_k \neq d_k$. Predpokladajme, že $c_k > d_k$. Potom pre všetky $i \in \{1, 2, \dots, k-1\}$ platí $c_i = d_i$ a teda tiež $c_i - d_i = 0$ a $c_k - d_k \geq 1$. Podľa vlastnosti (2) z definície 2.1.1 platí $r \geq [r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}$. Potom $r - ([r] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k}) \geq ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) - ([r] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k}) = (c_k - d_k) \frac{1}{g^k} \geq \frac{1}{g^k}$ a to je spor s vlastnosťou (2) z definície 2.1.1. V prípade, že $c_k < d_k$, postupujeme analogicky.

(2) Nech $r \neq s$, $[r] = [s]$ a pre všetky $n \in \mathbb{N}$ platí $c_n = d_n$. Nech, napríklad, $s < r$. Potom $r - s > 0$ a existuje $k \in \mathbb{N}$ tak, že $\frac{1}{g^k} \leq r - s$. Platí $[s] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k} \leq s$, preto $-s \leq -([s] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k})$ a tiež platí $[s] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k} = [r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}$. Potom $r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) = r - ([s] + \frac{d_1}{g} + \dots + \frac{d_k}{g^k}) \geq r - s \geq \frac{1}{g^k}$. Dostali sme spor s definíciou g -adického rozvoja. Podobne pre prípad $r < s$. □

Poznámka. 1) Ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$, tak $[r]$ je celé nezáporné číslo a vyjadrujeme ho v g -adickej číselnej sústave.

2) Ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$ a pre všetky $l \in \mathbb{N}$, $l \geq k + 1$ je $c_l = 0$, tak g -adický rozvoj r zapisujeme skrátene $r = ([r], c_1 c_2 \dots c_k)_g$.

3) Ak $s \in \mathbb{R}_0^+$ a $s = [s] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}$, kde pre všetky $i \in \{1, \dots, k\}$ platí $c_i \in \{0, 1, \dots, g-1\}$, tak g -adický rozvoj čísla s je $s = ([s], c_1 \dots c_k)_g$.

4) Ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$, tak pre každé $k \in \mathbb{N}$ platí $0 \leq r - ([r], c_1 c_2 \dots c_k)_g < \frac{1}{g^k}$, teda (raciálne) číslo $([r], c_1 c_2 \dots c_k)_g$ aproximuje číslo r s presnosťou lepšou ako $\frac{1}{g^k}$.

5) Ak $r < 0$, tak $-r > 0$ a existuje g -adický rozvoj $-r = ([-r], c_1 c_2 \dots c_k \dots)_g$. Potom g -adický rozvoj čísla r je $r = -([-r], c_1 c_2 \dots c_k \dots)_g$.

6) Vyjadrenie každého reálneho čísla pomocou g -adického rozvoja je jednoznačné.

7) Dá sa dokázať, že ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$, tak množina $\{k \in \mathbb{N} : c_k < g-1\}$ je nekonečná (t. j. neohraničená).

8) Dá sa dokázať, že ak $c_0 \in \mathbb{N}_0$ a $\{c_k\}_{k=1}^\infty$ je postupnosť taká, že pre všetky $k \in \mathbb{N}$ je $c_k \in \{0, 1, \dots, g-1\}$ a súčasne množina $\{k \in \mathbb{N} : c_k < g-1\}$ je nekonečná, tak existuje (práve jedno) $r \in \mathbb{R}_0^+$, pre ktoré je $r = (c_0, c_1 c_2 \dots c_k \dots)_g$ g -adický rozvoj čísla r .

Príklad. Nájdite g -adický rozvoj čísla $r = \frac{19}{3}$ pre $g = 5$.

$$\begin{array}{lll} \frac{19}{3} = 6 + \frac{1}{3}, & [r] = 6 = (11)_5, & r_1 = \frac{1}{3} \\ 5r_1 = \frac{5}{3}, & c_1 = \left[\frac{5}{3} \right] = 1, & r_2 = 5r_1 - c_1 = \frac{2}{3} \\ 5r_2 = \frac{10}{3}, & c_2 = \left[\frac{10}{3} \right] = 3, & r_3 = 5r_2 - c_2 = \frac{1}{3} \\ 5r_3 = \frac{5}{3}, & c_3 = \left[\frac{5}{3} \right] = 1, & r_4 = 5r_3 - c_3 = \frac{2}{3} \\ 5r_4 = \frac{10}{3}, & c_4 = \left[\frac{10}{3} \right] = 3, & \dots \end{array}$$

$$\frac{19}{3} = (11)_5 + \frac{1}{5} + \frac{3}{5^2} + \frac{1}{5^3} + \frac{3}{5^4} + \dots = (11, 1313\overline{13} \dots)_5.$$

Lema 2.1.3. 1) Ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$, tak $r - [r] = (0, c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r - [r]$.

2) Ak $r = ([r], c_1 c_2 \dots c_k \dots)_g$ je g -adický rozvoj čísla $r \in \mathbb{R}_0^+$, tak pre každé $k \in \mathbb{N}$ platí $[g^k \cdot r] = g^k \cdot [r] + g^{k-1} \cdot c_1 + \dots + c_k$ a $g^k \cdot r = ([g^k \cdot r], c_{k+1} c_{k+2} \dots c_{k+n} \dots)_g$ je g -adický rozvoj čísla $g^k \cdot r$.

Dôkaz. 1) Pretože $0 \leq r - [r] < 1$, platí $[r - [r]] = 0$. Naviac, pre každé $k \in \mathbb{N}$ platí $0 \leq (r - [r]) - ([r - [r]] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) = (r - [r]) - (0 + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) = r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) < \frac{1}{g^k}$. Teda $r - [r] = (0, c_1 c_2 \dots c_k \dots)_g$.

2) Nech $k \in \mathbb{N}$. Potom platí $0 \leq r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k}) < \frac{1}{g^k}$ a po vynásobení tejto nerovnosti číslom g^k dostaneme nerovnosť $0 \leq g^k.r - (g^k.[r] + g^{k-1}.c_1 + \dots + c_k) < 1$. Po úprave dostaneme $g^k.[r] + g^{k-1}.c_1 + \dots + c_k \leq g^k.r < (g^k.[r] + g^{k-1}.c_1 + \dots + c_k) + 1$ a preto $[g^k.r] = (g^k.[r] + g^{k-1}.c_1 + \dots + c_k)$.

Dalej, pre každé $m \in \mathbb{N}$ je aj $k + m \in \mathbb{N}$ a preto $0 \leq r - ([r] + \frac{c_1}{g} + \dots + \frac{c_k}{g^k} + \frac{c_{k+1}}{g^{k+1}} + \dots + \frac{c_{k+m}}{g^{k+m}}) < \frac{1}{g^{k+m}}$. Ak túto nerovnosť vynásobíme číslom g^k , dostaneme nerovnosť $0 \leq g^k.r - (g^k.[r] + g^{k-1}.c_1 + \dots + c_k + \frac{c_{k+1}}{g^1} + \dots + \frac{c_{k+m}}{g^m}) = g^k.r - ([g^k.r] + \frac{c_{k+1}}{g^1} + \dots + \frac{c_{k+m}}{g^m}) < \frac{1}{g^m}$. Teda postupnosť $\{c_{k+m}\}_{m=1}^{\infty}$ spĺňa podmienky z definície g -adického rozvoja a preto $g^k.r = ([g^k.r], c_{k+1}c_{k+2} \dots c_{k+n} \dots)_g$. $\square$

2.2 Kritériá racionálnosti

Definícia 2.2.1. Nech $r \in \mathbb{R}_0^+$, $g \in \mathbb{N}$, $g \geq 2$. Potom g -adický rozvoj $r = ([r], c_1 \dots c_n \dots)_g$ čísla r nazývame *periodický*, ak existuje $m \in \mathbb{N}_0$ a $k \in \mathbb{N}$ tak, že pre každé $l \in \mathbb{N}$, $l > m$ platí $c_{l+k} = c_l$. Nech m, k sú najmenšie také čísla. Potom $r = ([r], c_1 \dots c_m d_1 \dots d_k d_1 \dots d_k \dots)_g$, pričom konečná postupnosť $c_1, \dots, c_m$ sa nazýva *predperióda*, konečná postupnosť $d_1, \dots, d_k$ (*základná*) *perióda* g -adického rozvoja čísla r , číslo m sa nazýva *dĺžka predperiódy* a číslo k *dĺžka (základnej) periódy*.

$$r = 2, \underbrace{123}_{\text{predperióda}} \underbrace{4545}_{\text{základná perióda}} \dots$$

Veta 2.2.2. Nech $g \in \mathbb{N}$, $g \geq 2$. Číslo $r \in \mathbb{R}_0^+$ je racionálne vtedy a len vtedy, ak g -adický rozvoj $r = ([r], c_1 \dots c_n \dots)_g$ čísla r je periodický.

Dôkaz. Ak $r = ([r], c_1 \dots c_n c_{n+1} \dots)_g$ je g -adický rozvoj r , tak, podľa lemy 2.1.3, pre každé $k \in \mathbb{N}$ je $g^k.r = ([g^k.r], c_{k+1}c_{k+2} \dots c_{k+n} \dots)_g$ g -adický rozvoj čísla $g^k.r$ a $g^k.r - [g^k.r] = (0, c_{k+1}c_{k+2} \dots)_g$ je g -adický rozvoj čísla $g^k.r - [g^k.r]$.

$\Leftarrow$ Nech teraz $r = ([r], c_1, \dots, c_m d_1, \dots, d_k d_1, \dots, d_k \dots)_g$ má periodický g -adický rozvoj s predperiódou $c_1, \dots, c_m$ a periódou $d_1, \dots, d_k$.

$$\text{Potom } g^m.r - [g^m.r] = 0, d_1 \dots d_k d_1 \dots d_k \dots$$

$$\text{a } g^{m+k}.r - [g^{m+k}.r] = 0, d_1 \dots d_k d_1 \dots d_k \dots$$

$$\text{Teda } g^m.r - [g^m.r] = g^{m+k}.r - [g^{m+k}.r]. \text{ Potom}$$

$$(g^{m+k} - g^m)r = [g^{m+k}.r] - [g^m.r] \text{ a teda}$$

$$r = \frac{[g^{m+k}.r] - [g^m.r]}{g^{m+k} - g^m} \in \mathbb{Q}.$$

$\Rightarrow$ Nech $r \in \mathbb{Q}_0^+$, $r = ([r], c_1 c_2 \dots c_n \dots)_g$. Potom $r - [r] = \frac{a}{b} \in \mathbb{Q} \cap [0, 1)$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}$) a podľa lemy 2.1.3 platí $r - [r] = (0, c_1 c_2 \dots c_n \dots)_g$. Ak $a = 0$, tak $r = ([r], 00 \dots 0 \dots)_g$ má periodický rozvoj. Ak $a \neq 0$, tak $\frac{a}{b} > 0$ a teda $a > 0$. Stačí dokázať, že g -adický rozvoj $\frac{a}{b}$ je periodický.

Ak $\frac{a}{b} = (0, c_1 c_2 \dots c_n \dots)_g$, tak $\forall n \in \mathbb{N} \ v_n = g^n \frac{a}{b} - [g^n \frac{a}{b}] = (0, c_{n+1} c_{n+2} \dots)_g$ a $0 \leq v_n < 1$. Preto $0 \leq v_n.b < b$, pričom $v_n.b = g^n.a - [g^n \frac{a}{b}].b \in \mathbb{N}_0$.

Teda $v_n.b \in \{0, 1, \dots, b-1\}$ a potom $v_n \in \{0, \frac{1}{b}, \dots, \frac{b-1}{b}\}$ - konečná množina. Teda postupnosť $\{v_n\}_{n=1}^{\infty}$ má len konečný počet hodnôt a preto existujú $m, n \in \mathbb{N}$, $m < n$ také, že

$v_m = v_n$. Označme $k = n - m$. Potom $k \in \mathbb{N}$ a $v_n = v_{m+k}$. Pritom

$$v_m = (0, c_{m+1}c_{m+2} \dots c_{m+k}c_{m+k+1} \dots c_{m+2k}c_{m+2k+1} \dots c_{m+3k} \dots)_g$$

$$v_{m+k} = (0, c_{m+k+1} \dots c_{m+2k}c_{m+2k+1} \dots c_{m+3k} \dots)_g$$

Pretože $v_m = v_{m+k}$ a g -adický rozvoj je daný jednoznačne, dostávame: $c_{m+1} = c_{m+k+1}$, $c_{m+2} = c_{m+k+2}$, $\dots$ $c_{m+k} = c_{m+2k}$, $c_{m+k+1} = c_{m+2k+1}$, $\dots$ Teda pre každé $l > m$ platí $c_l = c_{l+k}$ a preto g -adický rozvoj čísla $\frac{a}{b}$ je periodický. $\square$

Príklad. Vyjadrite číslo $r = 2,21123123123 \dots$ v tvare $\frac{z}{n}$, $z \in \mathbb{Z}$, $n \in \mathbb{N}$.

$m = 2$ (dĺžka predperiódy) $k = 3$ (dĺžka periódy)

$$r = \frac{[10^{m+k}r] - [10^m r]}{10^m(10^k - 1)}$$

$$r = \frac{[10^5 r] - [10^2 r]}{10^2(10^3 - 1)} = \frac{221123 - 221}{100 \cdot 999} = \frac{220902}{99900} = \frac{36817}{16650}$$

Ďalšie kritériá pre racionálnosť (alebo aj iracionálnosť) niektorých reálnych čísel sú

Veta 2.2.3. *Nech $n, m \in \mathbb{N}$ a $n \geq 2$. Potom $\sqrt[n]{m}$ je racionálne číslo vtedy a len vtedy, ak existuje $k \in \mathbb{N}$, pre ktoré $k^n = m$.*

Dôkaz. $\Rightarrow$ Nech $\sqrt[n]{m}$ je racionálne číslo. Pretože $\sqrt[n]{m} > 0$, existujú $a, b \in \mathbb{N}$ tak, že $\sqrt[n]{m} = \frac{a}{b}$ a $(a, b) = 1$. Potom platí $b^n \cdot m = a^n$. Pretože $(a, b) = 1$, platí aj $(a^n, b^n) = 1$. Číslo a^n delí $b^n \cdot m$, $(a^n, b^n) = 1$ a preto $a^n \mid m$. Potom $m = l \cdot a^n$. Teda platí $b^n \cdot l \cdot a^n = a^n$, z čoho dostaneme $b^n \cdot l = 1$. Potom ale $b \mid 1$ a preto $b = 1$. Teda máme $m = a^n$, $a \in \mathbb{N}$.

$$\Leftarrow \text{Zrejme. } \sqrt[n]{m} = \sqrt[n]{k^n} = k \in \mathbb{N} \subseteq \mathbb{Q}$$

Nech $\log$ označuje logaritmus pri základe 10. Potom platí

Veta 2.2.4. *Pre každé $r \in \mathbb{Q}^+$, $\log r \in \mathbb{Q}$ vtedy a len vtedy, keď existuje $z \in \mathbb{Z}$ také, že $r = 10^z$.*

Dôkaz. $\Rightarrow$ Nech $r > 1$, $r = \frac{a}{b}$, $a, b \in \mathbb{N}$, $a > b$, $(a, b) = 1$ a nech $\log \frac{a}{b} \in \mathbb{Q}$. Pretože $r = \frac{a}{b} > 1$, $\log \frac{a}{b} > 0$ a existujú $c, d \in \mathbb{N}$, $(c, d) = 1$ tak, že $\log \frac{a}{b} = \frac{c}{d}$. Potom $10^{\frac{c}{d}} = \frac{a}{b}$ a teda $10^c = (\frac{a}{b})^d$. Po úprave, $10^c \cdot b^d = a^d$. Pretože $(a, b) = 1$, platí aj $(b, a^d) = 1$. Pretože $b \mid a^d$, máme $(b, a^d) = b = 1$. Teda máme $10^c = a^d$. $10^c = 2^c 5^c = a^d$, t.j. $a^d = 2^c 5^c$ je kanonický rozklad a^d . Z jednoznačnosti kanonického rozkladu vyplýva, že v kanonickom rozklade čísla a sú práve čísla 2 a 5, t.j. $a = 2^u \cdot 5^v$ je kanonický rozklad a , $u, v \in \mathbb{N}$. Potom $a^d = 2^{ud} \cdot 5^{vd} = 2^c \cdot 5^c$, z čoho dostávame, že $ud = c = vd$. Pretože $(c, d) = 1$ a $d \mid c$, platí $(c, d) = d = 1$. Teda $10^c = a = \frac{a}{b} = r$.

Nech teraz $r < 1$. Potom $\frac{1}{r} > 1$ a platí $\log r = -\log \frac{1}{r}$. Ak $\log r \in \mathbb{Q}$, tak aj $\log \frac{1}{r} \in \mathbb{Q}$ a preto existuje $n \in \mathbb{N}$ tak, že $\frac{1}{r} = 10^n$. Potom $r = 10^{-n}$ a $-n \in \mathbb{Z}$.

Pre $r = 1$ platí $r = 10^0$.

$$\Leftarrow \text{Zrejme. } \log 10^z = z \in \mathbb{Q}$$

Cvičenia

- 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) $\log 2 + \log 3$, g) $10^{\frac{9}{7}}$, h) $\sqrt{2} + \sqrt{3} + \sqrt{5}$.
- Nech $r = \frac{c}{d}$, $(c, d) = 1$, $d, c \in \mathbb{Z}$, je racionálny koreň rovnice $a_k x^k + a_{k-1} x^{k-1} + \dots + a_0 = 0$, 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 $x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0 = 0$, $a_i \in \mathbb{Z}$ platí: Každý racionálny koreň tejto rovnice je celé číslo.

3. Nájďte 5-adický rozvoj nasledujúcich čísel: $\frac{35}{11}$, $\frac{13}{9}$, $\frac{1}{24}$.
4. Nájďte 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. Nájďte $a, b \in \mathbb{Z}$ tak, aby
- a) $\frac{a}{b} = 2 + \frac{1}{5} + \frac{3}{5^2} + \frac{1}{5^3} + \frac{3}{5^4} + \frac{1}{5^5} + \frac{3}{5^6} + \dots = (2,131313\dots)_5$
- b) $\frac{p}{q} = 3 + \frac{2}{7} + \frac{3}{7^2} + \frac{3}{7^3} + \frac{3}{7^4} + \dots = (3,23333\dots)_7$.

Literatúra

- [1] Š. Znám: *Teória čísel*, Alfa, Bratislava, 1986.
- [2] M. Kolibiar a kol.: *Algebra a príbuzné disciplíny*, Alfa, Bratislava, 1992.
- [3] T. Šalát a kol.: *Algebra a teoretická aritmetika 2*, Alfa, Bratislava, 1986.
- [4] C. T. Long: *Elementary introduction to number theory*, 3rd ed., Englewood Cliffs, NJ: Prentice-Hall, 1987.
- [5] M. Kolibiar a kol.: *Vybrané partie z matematiky (skriptum)*, UK, Bratislava, 1979.
- [6] T. Šalát: *Vybrané kapitoly z elementárnej teórie čísel (skriptum)*, UK, Bratislava, 1979.
- [7] T. Hecht, Z. Sklenáriková: *Metódy rieše*, SPN, Bratislava, 1992.
- [8] J. B. Dynkin a kol.: *Matematické hlavolamy*, Alfa, Bratislava.
- [9] G. A. Jones, J. M. Jones: *Elementary Number Theory*, Springer, London, 1998.