Cvičenia

1. 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 $(c_0 + c_1 10 + c_2 10^2) + (c_3 + c_4 10 + c_5 10^2) + \dots = c_2c_1c_0 + c_5c_4c_3 + \dots$

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

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

4. Nech $p = 10^{m-1} + 10^{m-2} + \dots + 10 + 1 = \overbrace{11\dots1}^{m \text{ cifier}}$ je prvočíslo. Potom aj m je prvočíslo. Ukážte, že obrátené tvrdenie neplatí.

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

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

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

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

1.5 Eulerova funkcia a Eulerova veta

Definícia 1.5.1 (Eulerova[3] funkcia). Zobrazenie $\varphi\colon \mathbb{N} \to \mathbb{R}$, ktoré každému n priradí počet prvkov množiny $\{k \in \mathbb{N}; k \le n \text{ a } (k,n) = 1\}$ 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*

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

Dôkaz. Nech $r_1, \dots, r_k$ sú všetky navzájom rôzne prirodzené čísla také, že pre každé $i = 1, \dots, k$ $1 \le r_i \le n$ 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 $a.r_i \equiv l_i\,(mod\ n)$. 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 $ar_i \equiv ar_{i'}\,(mod\ n)$ a pretože $(a,n) = 1$, dostávame $r_i \equiv r_{i'}\,(mod\ n)$. Pretože $1 \le r_i, r_{i'} \le n$, $|r_i - r_{i'}| \le n - 1$, a preto $r_i = r_{i'}$ a teda $i = i'$. Teda ak $i \ne i'$, tak $l_i \ne l_{i'}$ t.j. $\{l_1, \dots, l_k\}$ má k prvkov, a preto $\{l_1, \dots, l_k\} = \{r_1, \dots, r_k\}$. Potom $l_1.l_2 \dots l_k = r_1.r_2 \dots r_k$.

[3] Euler 1707-1783

Obsah

1 Deliteľnosť v obore celých čísel **3**
1.1 Základné pojmy a ich vlastnosti . . . 3
1.2 Prvočísla . . . 9
1.3 Číselné sústavy . . . 12
1.4 Kongruencie . . . 14
1.4.1 Pojem kongruentnosti *mod n*, základné vlastnosti . . . 14
1.4.2 Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel . . . 16
1.5 Eulerova funkcia a Eulerova veta . . . 18
1.5.1 Použitie Eulerovej vety v kryptografii (šifrovaní) . . . 21
1.6 Lineárne kongruencie s jednou neznámou . . . 22
1.7 Aritmetické funkcie φ, τ, σ . . . 24
1.8 Doplnky. Lagrangeova a Wilsonova veta. . . . 26

2 *g*-adické rozvoje reálnych čísel. Kritéria iracionálnosti. **29**
2.1 *g*-adický rozvoj . . . 29
2.2 Kritériá racionálnosti . . . 31

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 $n \in N$ 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 $q' \leq q$ (prípad $q \leq q'$ 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 $k = k'$. □

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 $N_{a,b} = \{n \in \mathbb{N}; n \mid a$ 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 ohraničená 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 $d' = d$. □

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 $d = d'$. □

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

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

$$n = f(10) \equiv f(-1) = c_0 - c_1 + c_2 - \ldots + (-1)^k c_k \,(mod\ 11)$$

Preto

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

□

Príklad. $11 \mid 25\,916 \Leftrightarrow 11 \mid 6 - 1 + 9 - 5 + 2 = 11$. Teda $11 \mid 25916$.

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

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 $f(x) = (c_0 + c_1 10 + c_2 10^2) + (c_3 + c_4 10 + c_5 10^2)x + (c_6 + c_7 10 + c_8 10^2)x^2 + \ldots$
$f(10^3) = n$, $f(-1) = q$.

$$10^3 \equiv -1 \,(mod\ 7),$$

lebo $10^3 - (-1) = 1001 = 143.7 = 7.11.13$. $n = f(10^3) \equiv f(-1) = q \,(mod\ 7)$. Preto

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

$$10^3 \equiv -1 \,(mod\ 11)$$

$$n = f(10^3) \equiv f(-1) = q \,(mod\ 11)$$

Teda $11 \mid m \;\Leftrightarrow\; 11 \mid q$.

Podobne pre 13, pretože $10^3 \equiv -1 \,(mod\ 13)$. □

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 $n = c_k g^k + \ldots + c_1 g + c_0 (= (c_k \ldots c_1 c_0)_g)$ je prirodzené číslo vyjadrené v g-adickej sústave. Potom platí:*

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

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

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

(b) Pre každé prvočíslo p je ($\mathbb{Z}/mod\ p, \oplus, \odot$) pole.

Príklad. ($\mathbb{Z}/mod\ 3, \oplus, \odot$) je pole.
$[1]_3 + [2]_3 = [3]_3 = [0]_3$
$[2]_3.[2]_3 = [4]_3 = [1]_3$
Vidíme, že toto pole je „ v podstate“ totožné s poľom $(Z_3, +, \cdot)$.

Cvičenia

1. Nájdite poslednú cifru čísla a) $213^{174} + 25^{17}$, b) $99^{99} + (7^{17})^{17}$, c) $127^{37} + 45^{131} + 109^{18}$.
2. Nájdite všetky prirodzené čísla n, pre ktoré a) $7 \mid 2^n - 1$, b) $7 \mid 2^n + 1$.
3. Nech $a, b \in \mathbb{Z}$. Dokážte, že $19 \mid 10a + b \Leftrightarrow 19 \mid a + 2b$.
4. Overte, či $19 \mid 539828$ s využitím predchádzajúcej úlohy.
5. Nech $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$. Dokážte, že ak $f(4)$ aj $f(5)$ je nepárne číslo, tak rovnica $ax^2 + bx + c = 0$ nemá celočíselné korene.
6. Dokážte, že pre každé $n \in \mathbb{N}$ platí: Ak $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, $k \in \mathbb{N}$ a pre každé $i = 1, \ldots, n$ $a_i \equiv b_i\,(mod\ k)$, tak $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n\,(mod\ k)$ a $a_1 \ldots a_n \equiv b_1 \ldots b_n\,(mod\ k)$.
7. Určte poslednú cifru čísla $n = 22.51 + 698^5$ pri jeho vyjadrení v päťkovej a v sedmičkovej sústave.
8. Ak $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$, $m \mid n$ a $a \equiv b\,(mod\ n)$, tak $a \equiv b\,(mod\ m)$. Dokážte!
9. Aký je zvyšok 167^{452} po delení 11?

1.4.2 Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel

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

Dôkaz.
$$c_k + \ldots + c_1 + c_0 = c_k 1^k + \ldots + c_1 1 + c_0$$
Zoberme polynóm $f(x) = c_k x^k + \ldots + c_1 x + c_0$. Zrejme $c_i \in \mathbb{N}_0 \subseteq \mathbb{Z}$. Potom $n = f(10)$, $c_k + \ldots + c_1 + c_0 = f(1)$. Platí $10 \equiv 1\,(mod\ 9)$. Potom podľa 1.4.2(6)
$$n = f(10) \equiv f(1) = c_k + \ldots + c_1 + c_0\,(mod\ 9).$$
Potom $9 \mid n \Leftrightarrow 9 \mid c_k + \ldots + c_1 + c_0$, lebo čísla kongruentné modulo 9 dávajú pri delení číslom 9 rovnaké zvyšky.

Platí tiež $10 \equiv 1\,(mod\ 3)$, a preto $n = f(10) \equiv f(1) = c_k + \ldots + c_1 + c_0\,(mod\ 3)$. Teda
$$3 \mid n \;\Leftrightarrow\; 3 \mid c_k + \ldots + c_1 + c_0.$$
□

Príklad. $3 \mid 149\,688 \Leftrightarrow 3 \mid 36 \Leftrightarrow 3 \mid 9$

Veta 1.1.7 (výpočet najväčšieho spoločeného deliteľa). *Nech $a, b \in Z$, $a \neq 0$ 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
$$a_1 = b_2 a_2 + a_3, \qquad 0 \leq a_3 < a_2, \qquad (a_1, a_2) = (a_2, a_3).$$
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
$$a_{k-1} = b_k a_k + a_{k+1}, \qquad 0 \leq a_{k+1} < a_k \text{ a } a_k > 0,$$
tak existujú b_{k+1}, a_{k+2} tak, že
$$a_k = b_{k+1} a_{k+1} + a_{k+2}, \qquad 0 \leq a_{k+2} < a_{k+1}.$$
Týmto dostaneme klesajúcu postupnosť $a_1 > a_2 > \ldots > a_k > a_{k+1} > \ldots$ celých nezáporných čísel, ktorá nemôže byť nekonečná. Preto existuje $l \in \mathbb{N}$ tak, že $a_l > 0$ a $a_{l+1} = 0$.
$$a_{l-2} = b_{l-1} a_{l-1} + a_l$$
$$a_{l-1} = b_l a_l + 0.$$
Potom $a_l = (a_{l-1}, a_l) = (a_{l-2}, a_{l-1}) = \ldots = (a_2, a_1) = (a_1, a_0) = (a, b)$.

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

(2) Využijeme Euklidov algoritmus, kde $a_l = (a_0, a_1)$. $a_l = a_{l-2} + (-b_{l-1})a_{l-1} = a_{l-2} + (-b_{l-1})(a_{l-3} + (-b_{l-2})a_{l-2}) = (-b_{l-1})a_{l-3} + (1 + b_{l-1}b_{l-2})a_{l-2} = \ldots = ua_0 + va_1$, $u, v \in \mathbb{Z}$, 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. a) Určte $d = (-819, 792)$ a nájdite u, v také, že $d = u(-819) + v792$.
$|-819| = 819$, $|792| = 792$

$$\begin{array}{ll}
819 : 792 = 1 & 819 = 1.792 + 27 \\
\ \ 27 & \\
792 : 27 = 29 & 792 = 29.27 + 9 \\
252 & \\
\ \ 9 & \\
\ \ 27 : 9 = 3 & (-819, 792) = 9 \\
\ \ 0 &
\end{array}$$

$9 = 792 + (-29).27 = 792 + (-29)(810 + (-1)792) = (-29)819 + (1 + 29)792 = 29(-819) + 30.792$
b) Vyjadrite číslo $\frac{819}{792}$ v základnom tvare, t.j. v tvare $r = \frac{a}{b}$, kde $(a, b) = 1$ a $b \neq 0$.
$(819, 792) = 9, 819 : 9 = 91, 792 : 9 = 88, (91, 88) = 1, \underline{\underline{r = \frac{91}{88}}}$
c) Nájdite aspoň jedno celočíselné riešenie rovnice $819x + 792y = 27$.
$819.(-27) + 792.30 = 9 \qquad /.3$
$819.(-87) + 792.90 = 27$
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 riešnie má tvar $(-87 - 88k, 90 + 91k)$. Množina všetkých riešení je $\{(-87 - 88k, 90 + 91k); k \in \mathbb{Z}\}$.

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

(1) Ak $(a, b) = 1$ a $a \mid bc$, tak $a \mid c$.

(2) Ak $(a, b) = 1$, $a \mid c$, $b \mid c$, tak $ab \mid c$.

(3) Ak $(a, b) = 1$, $(a, c) = 1$, tak $(a, bc) = 1$.

(4) Ak $(a, b) = 1$, $m, n \in \mathbb{N}$, tak $(a^m, b^n) = 1$.

(5) Ak $(a, b) = d$, $a = a'd$, $b = b'd$, tak $(a', b') = 1$.

Dôkaz. (1) 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 $a \mid c$.

(2) 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 $ab \mid c$.

(3) Existujú $u, v, u', v' \in \mathbb{Z}$ tak, že $1 = ua + vb$, $1 = u'a + v'c$. Potom $1 = 1.1 = (ua + vb)(u'a + v'c) = (uu'a + vbu' + uv'c)a + vv'bc$, $uu'a + vbu' + uv'c, vv' \in \mathbb{Z}$. 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 $1 = (a, bc)$.

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

(5) 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 $(a', b') = 1$. $\square$

Uvažujme o kongruentnosti *mod* 5. Je to relácia ekvivalencie na $\mathbb{Z}$. Podľa predchádzajúcej vety, časť (8) platí, že $a \equiv b\,(mod\ 5)$ 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 $a \equiv b\,(mod\ 5)$. Ak $c \notin [1]_5$ a $a \in [1]_5$, tak $c \not\equiv a\,(mod\ 5)$.

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 *mod* 5, ktoré sa nazývajú zvyškové triedy *mod* 5. Ak prvky c, resp. d patria do rôznych zvyškových tried, tak $c \not\equiv d\,(mod\ 5)$. Je zrejmé, že $Z = [0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$ 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 $[a]_n = \{c \in \mathbb{Z}; c \equiv a\,(mod\ n)\}$ sa nazýva *zvyšková trieda modulo n*.

Príklad. a) $[1]_5 = \{1 + 5z; z \in \mathbb{Z}\}$, lebo $a \equiv 1\,(mod\ 5) \Leftrightarrow a - 1 = 5z \Leftrightarrow a = 1 + 5z$
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 $a \equiv a\,(mod\ n)$.
d) $[0]_n = \{n.z; z \in \mathbb{Z}\}$ - všetky čísla deliteľné n
$[1]_n = \{1 + n.z; z \in \mathbb{Z}\}$ - všetky čísla, ktorých zvyšok po delení n je 1
$[2]_n = \{2 + n.z; z \in \mathbb{Z}\}$
$\vdots$
$[n - 1]_n = \{(n - 1) + n.z; z \in \mathbb{Z}\}$
$[n]_n = [0]_n$, $[n + 1]_n = [1]_n, \ldots [-1]_n = [n - 1]_n, \ldots$
Zrejme platí $[0]_n \cup [1]_n \cup \ldots \cup [n - 1]_n = \mathbb{Z}$.

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

(1) $a \equiv b\,(mod\ n) \Leftrightarrow [a]_n = [b]_n$

(2) $a \not\equiv b\,(mod\ n) \Leftrightarrow [a]_n \cap [b]_n = \emptyset$

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

Dôkaz. (1) $\boxed{\Rightarrow}$ Nech $c \in [a]_n$. Potom $c \equiv a\,(mod\ n)$. Pretože $a \equiv b\,(mod\ n)$ dostávame $c \equiv b\,(mod\ n)$ a teda $c \in [b]_n$. Dokázali sme, že $[a]_n \subseteq [b]_n$. Podobne sa ukáže, že $[b]_n \subseteq [a]_n$.
$\boxed{\Leftarrow}$ $[a]_n = [b]_n \Rightarrow b \in [a]_n \Rightarrow a \equiv b\,(mod\ n)$.
(2) $\boxed{\Rightarrow}$ Nech $[a]_n \cap [b]_n \neq \emptyset$. Potom existuje $c \in [a]_n \cap [b]_n$ a teda $c \equiv a\,(mod\ n)$, $c \equiv b\,(mod\ n)$. Potom $a \equiv b\,(mod\ n)$, čo je spor. Teda $[a]_n \cap [b]_n = \emptyset$.
$\boxed{\Leftarrow}$ Ak $a \equiv b\,(mod\ n)$, tak $[a]_n = [b]_n$ a teda $[a]_n \cap [b]_n \neq \emptyset$ (lebo $a \in [a]_n \cap [b]_n$).
(3) Pre každé $a \in \mathbb{Z}$ existuje $k \in \{0, \ldots, n - 1\}$ tak, že $a \equiv k\,(mod\ n)$ (pozri vetu 1.4.2(7)). Teda $[a]_n = [k]_n$. $\square$

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

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

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. *(a) Pre každé $n \in \mathbb{N}$ je $(\mathbb{Z}/mod\ n, \oplus)$ komutatívna grupa.*

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: $a \equiv b\,(mod\ n)$.

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

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

(1) $a \equiv a\,(mod\ n)$

(2) Ak $a \equiv b\,(mod\ n)$, tak $b \equiv a\,(mod\ n)$.

(3) Ak $a \equiv b\,(mod\ n)$, $b \equiv c\,(mod\ n)$, tak $a \equiv c\,(mod\ n)$.

(4) Ak $a \equiv b\,(mod\ n)$ a $c \equiv d\,(mod\ n)$, tak $a \pm c \equiv b \pm d\,(mod\ n)$ a $a.c \equiv b.d\,(mod\ n)$.

(5) Al $a.c \equiv b.c\,(mod\ n)$ a $(c, n) = 1$, tak $a \equiv b\,(mod\ n)$.

(6) Ak $f(x) = a_k x^k + \ldots + a_1 x + a_0$, $a_i \in \mathbb{Z}$ a $c \equiv d\,(mod\ n)$, tak $f(c) \equiv f(d)\,(mod\ n)$.

(7) Pre každé $a \in \mathbb{Z}$ existuje práve jedno $l \in \{0, 1, \ldots, n-1\}$ také, že $a \equiv l\,(mod\ n)$.

(8) Ak $a = a'n + k$, $b = b'n + l$ a $0 \le k, l < n$, tak $a \equiv b\,(mod\ n) \Leftrightarrow k = l$.

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

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

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

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

$\boxed{\Leftarrow}$ $a \equiv k\,(mod\ n)$, $b \equiv l\,(mod\ n)$. Ak $k = l$, tak $a \equiv b\,(mod\ n)$.

(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 $d \le d'$. Podobne sa ukáže, že $d' \le d$. □

Definícia 1.1.9. 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 1.1.10.

(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 $k \le k'$ a súčasne $k' \le k$ 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 $d|a'||b'| = [a, b] = k$. □

Príklad. Určte $c = [-819, 792]$.
Vieme, že $(-819, 792) = 9$. Potom $c = \frac{819.792}{9} = 792.91 = 72\,072$.
Teda $[-819, 792] = 72\,072$

Cvičenia

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21*. Dokážte, že ak $(a, b) = 1$, tak existuje $N \in \mathbb{N}$ tak, že všetky prirodzené čísla n väčšie ako N možno zapísať v tvare $n = au + bv$, kde $u, v \in \mathbb{N}$.

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

Jednoznačnosť. Nech $n = c_k g^k + \ldots + c_1 g + c_0 = d_m g^m + \ldots + d_1 g + d_0$, $k, m \in \mathbb{N}_0$, 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

$$n = c_k g^k + \ldots + c_0 \leq (g-1)g^k + \ldots + (g-1) =$$
$$= (g-1)(g^k + \ldots + 1) = g^{k+1} - 1 < g^{k+1} \leq g^m \leq d_m g^m + \ldots + d_0 = n$$

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

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

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

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

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

Príklad. Vyjadrite číslo 356 v sedmičkovej sústave.

$356 : 7 = 50$ $\qquad$ $356 = 50.7 + 6$
6
$50 : 7 = 7$ $\qquad$ $50 = 7.7 + 1$
1 $\qquad$ $356 = (7.7 + 1).7 + 6 = 7^3 + 1.7 + 6$
$7 : 7 = 1 < 7$ $\qquad$ $= 1.7^3 + 0.7^2 + 1.7 + 6 = (1016)_7$
0

Vyjadrite 356 v päťkovej sústave.

$356 : 5 = 71$ $\qquad$ $71 : 5 = 14$ $\qquad$ $14 : 5 = 2 < 5$
1 $\qquad$ 1 $\qquad$ 4

$356 = (2411)_5$

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 $n = (a_1 a_0)_{10} = (a_1 a_0 2)_3$.

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

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

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

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

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

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

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

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

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

21. Vypočítajte počet deliteľov čísla 324000.

22*. Koľko čísel menších ako 3^n5^m je s číslom 3^n5^m nesúdeliteľných?

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

24*. 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

$203 = 2.10^2+0.10+3.10^0 \qquad 0 \leq 2,0,3 < 10$
$203 = 4.7^2+1.7+0.7^0 = (410)_7 \quad 0 \leq 4,1,0<7$
$13 = 1.2^3+1.2^2+1.2^0 = (1101)_2$

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 $n = c_kg^k+\dots+c_1g+c_0$. 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

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

Zrejme $l \geq 0$, pretože ak $l<0$, tak $l \leq -1$, a preto $l.q \leq -g$ a potom $n = l.g+c_0 \leq -g+c_0 < 0$ … 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 $l<l.g \leq l.g+c_0 = n$. 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 $l = b_kg^k+\dots+b_1g+b_0$. Potom

$$n = l.g+c_0 = b_kg^{k+1}+\dots+b_0g+c_0.$$

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, … sú prvočísla. $2^{216\,091}-1=$ v r. 1985 najväčšie známe prvočíslo, má 65 050 cifier 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 $m=p_1\dots p_r\dots p_{r+s}$, $r+s \in \mathbb{N}$, 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 $n=p_1\dots p_k=q_1\dots q_l$, $k,l \in \mathbb{N}$, $p_1,\dots,p_k,q_1,\dots,q_k$ 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 $m \in \mathbb{N}$ $n=p_1m$.
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 $\sigma'\colon \{2,\dots,k\} \to \{1,\dots,i-1,i+1,\dots,l\}$ také, že $\forall j \in \{2,\dots,k\}$ $q_{\sigma'(j)}=p_j$ (zrejme $k-1=l-1$). Potom ale zobrazenie $\sigma\colon \{1,\dots,k\} \to \{1,\dots,l\}$; $\sigma(1)=i$ 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) $n \geq 2$ $n = p_1, \ldots, p_k = q_1^{k_1} \ldots q_m^{l_m}$, $q_1, \ldots, q_m$ sú navzájom rôzne prvočísla, $l_1, \ldots, l_m \in \mathbb{N}$ je *kanonický rozklad* čísla n na prvočísla.

Veta 1.2.5. *Množina všetkých prvočísel je nekonečná.*

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

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

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

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

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

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

Dôkaz. Cvičenie. $\square$

Príklad. Určte (5445,2625) aj [5445,2625]
Riešenie:
$5445 = 3^2.5.11^2 = 3^2.5.7^0.11^2$
$2625 = 3.5^3.7 = 3.5^3.7.11^0$
$(5445, 2625) = 3.5.7^0.11^0 = 15$
$[5445, 2625] = 3^2.5^3.7.11^2 = 952\,875$

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

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

Poznámka. V teórii čísel existuje rad dodnes nevyriešených problémov, známych už viacero storočí. 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.

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

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. ($M_n = 2^n - 1$ - Mersenovo číslo[1]) [$M_{11} = 2^{11} - 1 = 2047$ nie je prvočíslo, $23 \mid M_{11}$.]
6. Dokážte, že ak $2^n + 1$ ($n \in \mathbb{N}$) je prvočíslo, tak existuje $m \in \mathbb{N}_0$ tak, že $n = 2^m$. Ukážte na príklade, že obrátený výrok neplatí. ($F_n = 2^{2^n} + 1$ - Fermatove čísla) [$F_5 = 2^{32} + 1$ nie je prvočíslo,[2] $641 \mid F_5$.]
7. Dokážte, že pre každé $k \in \mathbb{N}$ existuje k po sebe nasledujúcich prirodzených čísel, ktoré sú všetky zložené čísla.
8. Dokážte, že pre každé $n \in \mathbb{N}$, $n > 2$ existuje prvočíslo p také, že $n < p < n!$
9. a) Dokážte, že ak $p > 3$ je prvočíslo, tak existuje $k \in \mathbb{N}_0$, pre ktoré $p = 6k + 1$ alebo $p = 6k + 5$.
   b) Nájdite všetky prvočísla p také, že $p + 2$ aj $p + 10$ sú tiež prvočísla.
10. Nech $a, b \in \mathbb{N}$, $a > 0$, $b > 0$ a $a.b = p_1^{l_1} \ldots p_k^{l_k}$ je kanonický rozklad. Potom $a = p_1^{t_1} \ldots p_k^{t_k}$, $b = p_1^{s_1} \ldots p_k^{s_k}$, kde pre každé i $0 \leq t_i, s_i \leq l_i$. Dokážte, že $(a, b) = p_1^{u_1} \ldots p_k^{u_k}$, kde $u_i = \min\{t_i, s_i\}$ pre všetky $i = 1, \ldots, k$ a $[a, b] = p_1^{v_1} \ldots p_k^{v_k}$, kde $v_i = \max\{t_i, s_i\}$ pre všetky $i = 1, \ldots, k$.
11. Nájdite kanonické rozklady čísel 4725, 3718, 3234 a určte (4725,3718), [4725,3718], (3718,3234), [3718, 3234].

[1] mních Mersenne 1644
[2] Euler 1930

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] J.B.Dynkin a kol.: *Matematické hlavolamy,* Alfa, Bratislava.

Pretože pre každé $i = 1, \dots, k$ $ar_i \equiv l_i\,(mod\ n)$, podľa vety 1.4.2(4)

$$ar_1.ar_2 \dots ar_k \equiv l_1.l_2 \dots l_k\,(mod\ n),$$

a teda

$$a^k r_1.r_2 \dots r_k \equiv r_1.r_2 \dots r_k\,(mod\ n).$$

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) $a^k \equiv 1\,(mod\ n)$. Teda $a^{\varphi(n)} \equiv 1\,(mod\ n)$. □

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

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

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

$$a^p \equiv a\,(mod\ p).$$

Dôkaz. Pre každé $a \in \mathbb{Z}$ platí $p \mid a$ alebo $p \nmid a$. Ak $p \mid a$, tak $a \equiv 0\,(mod\ p)$ a potom $a^p \equiv 0^p = 0\,(mod\ p)$. Teda $a^p \equiv a\,(mod\ p)$.
Ak $p \nmid a$, tak $a^{p-1} \equiv 1\,(mod\ p)$, $a \equiv a\,(mod\ p)$ a teda $a^p \equiv a\,(mod\ p)$. □

Príklad.

1. Dokážte, že pre každé $n \in \mathbb{N}$ platí, že $15 \mid n^5 - n$.
   Riešenie: $n^5 \equiv n\,(mod\ 5)$, a preto $5 \mid n^5 - n$.
   $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n^3 - n)(n^2 + 1)$. $n^3 \equiv n\,(mod\ 3)$, 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 $15 = 3.5 \mid n^5 - n$.

2. Dokážte, že ak p je prvočíslo a $a \in \mathbb{Z}$ také, že $p \nmid a$ (t.j. $a \not\equiv 0\,(mod\ p)$), tak existuje $b \in \mathbb{Z}$ také, že $a.b \equiv 1\,(mod\ p)$.
   Riešenie: $a^{p-1} \equiv 1\,(mod\ p)$, $p - 1 \geq 1$. Stačí zobrať $b = a^{p-2}$. Potom $a.b = a.a^{p-2} = a^{p-1} \equiv 1\,(mod\ p)$.

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 $n^{\varphi(13)} \equiv 1\,(mod\ 13)$, t.j. $n^{12} \equiv 1\,(mod\ 13)$. 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 $i = 1, \dots, k$ $p_i \nmid m_i$. 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 $\varphi_{p_1,\dots,p_k} = \varphi(n)$.

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 $1.p_{j_0}, 2.p_{j_0}, \dots, l.p_{j_0}, \dots, \frac{n}{p_{j_0}}.p_{j_0}$, ich počet je $\frac{n_0}{p_{j_0}}$. Ak $i \in \{1, \dots, j_0 - 1\}$, tak $p_i \mid l.p_{j_0} \Leftrightarrow p_i \mid l$, ekvivalentne $p_i \nmid l.p_{j_0} \Leftrightarrow p_i \nmid l$. 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 $n = p_1^{l_1} \dots p_k^{l_j}$, 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,

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

□

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. $\boxed{\Rightarrow}$ Nech $r > 1$, $r = \frac{a}{b}$, $a, b \in \mathbb{N}$, $a > b$, $(a, b) = 1$ a nech $\log \frac{a}{b} \in \mathbb{Q}$. Potom $10^{\frac{c}{d}} = \frac{a}{b}$ a teda $10^c = \left(\frac{a}{b}\right)^d$. Po úprave, $10^c.b^d = a^d$. 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. $a = 2^u.5^v$ je kanonický rozklad a, $u, v \in \mathbb{N}$. Potom $a^d = 2^{ud}.5^{vd} = 2^c.5^c$, z čoho dostávame, že $ud = c = vd$. Pretože $(c, d) = 1$ a $d \mid c$, platí $(c, d) = d = 1$. Teda $10^u = a = \frac{a}{b} = r$.

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 $r = 10^0$.

$\boxed{\Leftarrow}$ Zrejmé. $\log 10^z = z \in \mathbb{Q}$ □

Cvičenia

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

2. Nech $r = \frac{c}{d}$, $(c, d) = 1$, $d, c \in \mathbb{Z}$, je racionálny koreň rovnice $a_k x^k + a_{k-1} x^{k-1} + \dots a_0 = 0$, 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. Nájdite 5-adický rozvoj nasledujúcich čísel: $\frac{35}{11}$, $\frac{13}{9}$, $\frac{1}{24}$.

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

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

$r = 2,\underbrace{123}_{\text{predperióda}}4545\underbrace{\overline{45}}_{\text{základná perióda}}\ldots$

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 $r = (c_0, c_1 \ldots c_n \ldots)_g$ čísla r je periodický.*

Dôkaz. Ak $r = (c_0, c_1 \ldots c_n c_{n+1} \ldots)_g$ je g-adický rozvoj r, tak $g^n.r = g_0 g^n + c_1 g^{n-1} + \ldots + c_n + \frac{c_{n+1}}{g} + \frac{c_{n+2}}{g^2} + \ldots$ a $[g^n r] = c_0 g^n + \ldots + c_n$. Teda $g^n r - [g^n r] = \frac{c_{n+1}}{g} + \frac{c_{n+2}}{g^2} + \ldots = (0, c_{n+1} c_{n+2} \ldots)_g$.

$\boxed{\Leftarrow}$ Nech teraz $r = (c_0, c_1, \ldots, c_m d_1, \ldots, d_k d_1, \ldots, d_k \ldots)_g$ má periodický g-adický rozvoj s predperiódou $c_1, \ldots, c_m$ a periódou $d_1, \ldots, d_k$.

$$\text{Potom } g^m.r - [g^m.r] = 0, d_1 \ldots d_k d_1 \ldots d_k \ldots$$
$$\text{a } g^{m+k}.r - [g^{m+k}.r] = 0, d_1 \ldots d_k d_1 \ldots d_k \ldots$$
$$\text{Teda } g^m r - [g^m r] = g^{m+k} r - [g^{m+k} r]. \text{ Potom}$$
$$(g^{m+k} - g^m) r = [g^{m+k} r] - [g^m r] \text{ a teda}$$
$$r = \frac{[g^{m+k} r] - [g^m r]}{g^{m+k} - g^m} \in \mathbb{Q}.$$

$\boxed{\Rightarrow}$ Nech $r \in \mathbb{Q}_0^+$, $r = (c_0, c_1 c_2 \ldots c_n \ldots)_g$. $c_0 = [r] \in \mathbb{N}_0$ a $r - c_0 = \frac{a}{b} \in \mathbb{Q} \cap [0, 1)$, $r - c_0 = (0, c_1 c_2 \ldots c_n \ldots)_g$. Ak $a = 0$, tak $r = (c_0, 00 \ldots 0 \ldots)_g$ má periodický rozvoj. Ak $a \neq 0$, tak $\frac{a}{b} > 0$ a a, b možno zvoliť tak, že $a > 0$ aj $b > 0$. Stačí dokázať, že g-adický rozvoj $\frac{a}{b}$ je periodický.

$\frac{a}{b} = (0, c_1 c_2 \ldots c_n \ldots)_g$

$\forall n \in \mathbb{N}$ $v_n = g^n \frac{a}{b} - [g^n \frac{a}{b}] = (0, c_{n+1} c_{n+2} \ldots)_g$ 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 $v_n.b \in \{0, 1, \ldots, b-1\}$ a potom $v_n \in \{0, \frac{1}{b}, \ldots, \frac{b-1}{b}\}$ - 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

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

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

Príklad. Vyjadrite číslo $r = 2,21123123123\ldots$ v tvare $\frac{z}{n}$, $z \in \mathbb{Z}$, $n \in \mathbb{N}$.
$m = 2$ (dĺžka predperiódy) $k = 3$ (dĺžka periódy)
$r = \frac{[10^{m+k} r] - [10^m r]}{10^m (10^k - 1)}$
$r = \frac{[10^5 r] - [10^2 r]}{10^2 (10^3 - 1)} = \frac{221123 - 221}{100.999} = \frac{220902}{99900} = \frac{36817}{16650}$

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. $\boxed{\Rightarrow}$ 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 $b^n.m = a^n$. Pretože $(a, b) = 1$, platí aj $(a^n, b^n) = 1$. Číslo a^n delí $b^n.m$, $(a^n, b^n) = 1$ a preto $a^n \mid m$. Potom $m = l.a^n$. Teda platí $b^n.l.a^n = a^n$, z čoho dostaneme $b^n.l = 1$. Potom ale $b \mid 1$ a preto $b = 1$. Teda máme $m = a^n$, $a \in \mathbb{N}$.

$\boxed{\Leftarrow}$ Zrejmé. $\sqrt[n]{m} = \sqrt[n]{k^n} = k \in \mathbb{N} \subseteq Q$ □

Cvičenia

1. Dokážte, že platí:
   a) $42 \mid n^7 - n$ pre každé $n \in \mathbb{Z}$,
   b) $7 \mid n^{6k} - 1$ pre každé $k \in \mathbb{N}$ a $n \in \mathbb{Z}$také, že $(n, 7) = 1$,
   c) $n^{13} - n$, $n \in \mathbb{Z}$ je deliteľné každým z čísel 2,3,5,7,13.
2. Ak p, q sú prvočísla, $p \neq q$, tak pre každé celé číslo a platí: $p.q \mid a^{p.q} - a^p - a^q + a$.
3. Nájdite všetky riešenia rovnice $2^m - 3^n = 1$ v obore prirodzených čísel.
4. Dokážte, že ak $n \in \mathbb{N}$ a $(10, n) = 1$, tak existuje $k \in \mathbb{N}$ tak, že $k.n = 99\ldots 9$ - má všetky cifry rovné 9.
5. Dokážte, že pre každé $n \in \mathbb{N}$ platí:
   a) $n^{10} = 11k$ alebo $n^{10} = 11k + 1$
   b) $n^{12} = 13k$ alebo $n^{12} = 13k + 1$
   c) $n^{20} = 25k$ alebo $25k + 1$
6. Nech $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a, n) = 1$. Nech k je najmenšie prirodzené číslo, pre ktoré $a^k \equiv 1\,(mod\ n)$. Potom pre každé $l \in \mathbb{N}$ také, že $a^l \equiv 1\,(mod\ n)$ platí, že $k \mid l$. Špeciálne, $k \mid \varphi(n)$. Dokážte!
7. Nájdite najmenšie prirodzené číslo n tak, aby
   a) $253^n \equiv 1\,(mod\ 257)$
   b) $2^n \equiv 1\,(mod\ 257)$.
8. Dokážte, že ak p, q sú prvočísla a $p \neq q$, tak $p^{q-1} + q^{p-1} \equiv 1\,(mod\ pq)$ a $p^q + q^p \equiv p + q\,(mod\ pq)$.
9. Na príklade ukážte, že ak $(a, n) > 1$, tak nemusí platiť $a^{\varphi(n)} \equiv 1\,(mod\ n)$.
10. Nájdite najmenšie prirodzené číslo, pre ktoré platí $6x \equiv 1\,(mod\ 35)$.

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

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 je prirodzené číslo, pre ktoré $(k, p-1) = 1$. Potom existuje q tak, že $k.q \equiv 1\,(mod\ (p-1))$, $q \in \{1, \ldots, p-2\}$, 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 $q \in \{0, \ldots, p-2\}$, že $q' \equiv q\,(mod\ p-1)$. Zrejme $k.q' \equiv 1\,(mod\ p-1)$ a potom aj $k.q \equiv 1\,(mod\ p-1)$.)

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

Ak teda je dané prvočíslo $p > 2$ a prirodzené číslo k, $(k, p-1) = 1$, (k sa nazýva kľúč šifry), $a \in \{1, \ldots, p-2\}$ a poznáme číslo b, pre ktoré $b \equiv a^k\,(mod\ p)$, tak pomocou k a p vieme určiť q a aj $a \equiv b^q\,(mod\ p)$, pričom ak $0 < a < p-2$, 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. Najprv nahradíme písmená číslami: $A \to 00$, $B \to 01$, $C \to 02$, $D \to 03$, $E \to 04$, $F \to 05$, $G \to 06$, $H \to 07$, $I \to 08$, $J \to 09$, $K \to 10$, $L \to 11$, $M \to 12$, $N \to 13$, $O \to 14$, $P \to 15$, $Q \to 16$, $R \to 17$, $\ldots$, $Z \to 25$. Teda FIRE prepíšeme na 05081704 a rozdelíme na 2 bloky po 4 cifry (=2 písmená).
0508 1704
Teraz máme

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

Zašifrovaný text je teda 2713 3726.

Pre odšifrovanie určíme q také, že $61q \equiv 1\,(mod\ 5800)$, je to číslo $q = 1141$. Potom určíme, že

$$\begin{aligned} 2713^{1141} &\equiv 508\,(mod\ 5801)\\ 3726^{1141} &\equiv 1704\,(mod\ 5801) \end{aligned}$$

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 počítať (v 80-tych rokoch) vyžadovalo 75 rokov, pre 200-ciferné prvočíslo dokonca 4.10^9 rokov.

1.6 Lineárne kongruencie s jednou neznámou

Lineárna kongruencia modulo n s jednou neznámou má tvar

$$a.x \equiv b\,(mod\ n),$$

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 $a.x \equiv b\,(mod\ n)$ ak $a.c \equiv b\,(mod\ n)$.

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

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 $a.x \equiv b\,(mod\ n)$ má riešenie $\Leftrightarrow$ $d \mid b$

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

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

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

Nech $\{k \in \mathbb{N}; c_k \neq c'_k\} \neq \emptyset$ a m je najmenší prvok tejto množiny, t.j. ak $l < m$, tak $c_l = c'_l$. Potom $c_0 + \frac{c_1}{g} + \ldots + \frac{c_l}{g^l} = c'_0 + \frac{c'_1}{g} + \ldots + \frac{c'_l}{g^l}$ a preto aj

$$\sum_{k=m}^{\infty} \frac{c_k}{g^k} = \sum_{k=m}^{\infty} \frac{c'_k}{g^k} \quad / \cdot \frac{1}{g^m}$$

$$s = c_m + \sum_{k=m+1}^{\infty} \frac{c_k}{g^{k-m}} = c'_m + \sum_{k=m+1}^{\infty} \frac{c'_k}{g^{k-m}}.$$

Pretože množiny K, K' sú nekonečné, existujú $l, l' \geq m+1$ tak, že $c_l < g-1$, resp. $c'_l < g-1$.

Potom, podobne ako v predošlej časti dôkazu, ukážeme, že

$$\sum_{k=m+1}^{\infty} \frac{c_k}{g^{k-m}} = \frac{c_{m+1}}{g} + \frac{c_{m+1}}{g^2} + \ldots < \frac{g-1}{g} + \frac{g-1}{g^2} + \ldots = 1$$

a teda $c_m = [s]$.

Podobne, $\sum_{k=m+1}^{\infty} \frac{c'_k}{g^{k-m}} < 1$ a preto $c'_m = [s]$. Teda $c_m = c'_m$ $\ldots$ spor.

Preto $\{k \in \mathbb{N}, c_k \neq c'_k\} = \emptyset$, t.j. pre každé $k \in \mathbb{N}$ $c_k = c'_k$. $\square$

Nech $r \in \mathbb{R}_0^+$, $g \in \mathbb{N}$, $g \geq 2$. Vyjadrenie $r = c_0 + \sum\limits_{k=1}^{\infty} \frac{c_k}{g^k}$ z predošlej vety sa nazýva *g-adický rozvoj* čísla r a zapisuje sa aj v tvare $r = (c_0, c_1 c_2 \ldots c_n \ldots)_g$.

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

$$\begin{array}{lll} \dfrac{19}{3} = 6 + \dfrac{1}{3}, & c_0 = 6, & r_1 = \dfrac{1}{3}\\[2ex] 5r_1 = \dfrac{5}{3}, & c_1 = \left[\dfrac{5}{3}\right] = 1, & r_2 = 5r_1 - c_1 = \dfrac{2}{3}\\[2ex] 5r_2 = \dfrac{10}{3}, & c_2 = \left[\dfrac{10}{3}\right] = 3, & r_3 = 5r_2 - c_2 = \dfrac{1}{3}\\[2ex] 5r_3 = \dfrac{5}{3}, & c_3 = \left[\dfrac{5}{3}\right] = 1, & r_4 = 5r_3 - c_3 = \dfrac{2}{3}\\[2ex] 5r_4 = \dfrac{10}{3}, & c_4 = \left[\dfrac{10}{3}\right] = 3, & \ldots \end{array}$$

$\frac{19}{3} = 6 + \frac{1}{5} + \frac{3}{5^2} + \frac{1}{5^3} + \frac{3}{5^4} + \ldots = (6, 1313\overline{13}\ldots)_5$.

Poznámka. Ak $r < 0$, tak $-r > 0$ a existuje g-adický rozvoj $-r = (c_0, c_1 c_2 \ldots c_n \ldots)_g$. Potom vyjadrenie pre r je $r = -(c_0, c_1 c_2 \ldots c_n \ldots)_g$.

2.2 Kritériá racionálnosti

Definícia 2.2.1. Nech $r \in \mathbb{R}_0^+$, $g \in \mathbb{N}$, $g \geq 2$. g-adický rozvoj $r = (c_0, c_1 \ldots c_n \ldots)_g$ 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 $c_{k+l} = c_l$. Nech m, k sú najmenšie také čísla. Potom $r = (c_0, c_1 \ldots c_m d_1 \ldots d_k d_1 \ldots d_k \ldots)_g$, pričom postupnosť $c_1, \ldots, c_m$ sa nazýva *predperióda* a postupnosť $d_1, \ldots, d_k$ *(základná) perióda g-adického rozvoja* čísla r.

$gr_{k+1} = c_{k+1} + r_{k+2}$ a $r = c_0 + r_1$. Teda

$$\begin{aligned} r = c_0 + r_1 = c_0 + \frac{gr_1}{g} = c_0 + \frac{c_1 + r_2}{g} = c_0 + \frac{c_1}{g} + \frac{r_2}{g} = \\ = c_0 + \frac{c_1}{g} + \frac{gr_2}{g^2} = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \frac{r_3}{g^2} = \ldots = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n} + \frac{r_{n+1}}{g^n} \end{aligned}$$

Označme $s_n = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n}$. Potom $0 \le r - s_n = \frac{r_{n+1}}{g^n} < \frac{1}{g^n}$. Pretože $\lim\limits_{n\to\infty} \frac{1}{g^n} = 0$, platí $\lim\limits_{n\to\infty} s_n = r$. Pritom $\lim\limits_{n\to\infty} s_n = c_0 + \sum\limits_{k=1}^{\infty} \frac{c_k}{g^k}$ a teda

$$r = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n} + \ldots = c_0 + \sum_{k=1}^{\infty} \frac{c_k}{g^k}.$$

Nech $K = \{k \in \mathbb{N}; c_k < g-1\}$ je konečná. Potom K má najväčší prvok k_0. Teda pre každé $n \ge k_0 + 1$ je $c_n = g - 1$. Z toho potom dostávame:

$$\begin{aligned} 0 \le \frac{r_{k_0+1}}{g^{k_0}} = r - \left(c_0 + \frac{c_1}{g} + \ldots + \frac{c_{k_0}}{g^{k_0}}\right) = \sum_{n=k_0+1}^{\infty} \frac{c_n}{g^n} = \\ = \sum_{n=k_0+1}^{\infty} \frac{g-1}{g^n} = \frac{g-1}{g^{k_0+1}} + \frac{g-1}{g^{k_0+2}} + \ldots + \frac{g-1}{g^{k_0+m}} + \ldots = \frac{g-1}{g^{k_0}} \left(\frac{1}{g} + \frac{1}{g^2} + \ldots + \frac{1}{g^m} + \ldots\right) = \\ = \frac{g-1}{g^{k_0}} \frac{\frac{1}{g}}{1 - \frac{1}{g}} = \frac{g-1}{g^{k_0}} = \frac{g-1}{g^{k_0}} \cdot \frac{1}{g-1} = \frac{1}{g^{k_0}} \end{aligned}$$

Teda $\frac{r_{k_0+1}}{g^{k_0}} = \frac{1}{g^{k_0}}$, a preto $r_{k_0+1} = 1$, čo je spor (pre každé $n \in \mathbb{N}$ je totiž $r_n < 1$). Teda K je nekonečná množina.

Jednoznačnosť. Nech $r = c_0 + \sum\limits_{k=1}^{\infty} \frac{c_k}{g^k} = c_0' + \sum\limits_{k=1}^{\infty} \frac{c_k'}{g^k}$, $c_0, c_0' \in \mathbb{N}_0$, pre každé $k \in \mathbb{N}$ $c_k, c_k' \in \{0, 1, \ldots, g-1\}$ a $K = \{k \in \mathbb{N}; c_k < g-1\}$ aj $K' = \{k \in \mathbb{N}; c_k' < g-1\}$ sú nekonečné.

Nech $l \in K$. Potom $c_l < g - 1$ a

$$\frac{c_1}{g} + \ldots + \frac{c_l}{g^l} < \frac{g-1}{g} + \ldots + \frac{g-1}{g^l}.$$

Platí tiež

$$\sum_{k=l+1}^{\infty} \frac{c_k}{g^k} \le \sum_{k=l+1}^{\infty} \frac{g-1}{g^k},$$

lebo pre každé $k > l$ $c_k \le g - 1$.

Potom ale

$$\begin{aligned} 0 \le \sum_{k=1}^{\infty} \frac{c_k}{g^k} < \sum_{k=1}^{\infty} \frac{g-1}{g^k} = \frac{g-1}{g} + \ldots + \frac{g-1}{g^n} + \ldots = \\ = (g-1)\left(\frac{1}{g} + \ldots + \frac{1}{g^n} + \ldots\right) = (g-1)\frac{1}{g-1} = 1. \end{aligned}$$

Teda $c_0 \le c_0 + \sum\limits_{k=1}^{\infty} \frac{c_k}{g^k} < c_0 + 1$ a preto $c_0 = [r]$. Podobne sa ukáže, že $c_0' = [r]$ a teda $c_0 = c_0'$.

(2) Pretože $d \mid b$, existuje riešenie $[c_0]_n$ danej kongruencie. $d \mid n$ a preto existuje $l \in \mathbb{N}$ také, že $n = l.d$. Položme $c_1 = c_0 + l, c_2 = c_0 + 2l, \ldots c_{d-1} = c_0 + (d-1).l$. Dokážeme, že $[c_0]_n, [c_1]_n, \ldots, [c_{d-1}]_n$ sú navzájom rôzne riešenia danej kongruencie a že sú to všetky riešenia. $d \mid a$ a teda existuje $a' \in \mathbb{Z}$ tak, že $a = a'.d$. Pre každé $i = 0, \ldots, d-1$ $a.c_i = ac_0 + ai.l = ac_0 + a'idl = ac_0 + a'.i.n \equiv ac_0 \,(mod\ n)$, a preto $a.c_i \equiv b \,(mod\ n)$.

Teda pre každé $i = 0, \ldots, d-1$ $[c_i]_n$ je riešenie $a.x \equiv b \,(mod\ n)$. Nech $0 \le i < j \le d-1$. Potom $0 < c_j - c_i = (j-i)l \le jl < dl = n$, a preto $n \nmid c_j - c_i$. Teda $c_i \not\equiv c_j \,(mod\ n)$, t.j. $[c_i]_n \ne [c_j]_n$.

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

Príklad. 1. Vyriešte lineárnu kongruenciu $20x \equiv 28 \,(mod\ 12)$.
Riešenie. (20,12)=4, 4 | 28 a teda existujú práve 4 riešenia.

$$\begin{aligned} 4 &= (-1).20 + 2.12 \quad /.7 \\ 20(-7) + 14.12 &= 28 \\ 20(-7) &\equiv 28 \,(mod\ 12) \end{aligned}$$

$c_0 = -7$, $c_1 = -7 + 3 = -4$, $c_2 = -7 + 2.3 = -1$, $c_3 = -7 + 3.3 = 2$
Riešenia sú $[-7] = [5]$, $[-4] = [8]$, $[-1] = [11]$, $[2]$.
Pretože $20x \equiv 8x \,(mod\ 12)$ a $28 \equiv 4 \,(mod\ 12)$, je daná kongruencia ekvivalentná s kongruenciou $8x \equiv 4 \,(mod\ 12)$.
2. Vyriešte kongruenciu $15x \equiv -66 \,(mod\ 18)$.
(15,18)=3, 3 | −66 kongruencia má 3 riešenia.

$$\begin{aligned} -66 &\equiv 6 \,(mod\ 18) \\ 15x &\equiv 6 \,(mod\ 18) \\ 3 &= (-1).15 + 1.18 \\ 15.(-2) + 2.18 &= 6 \\ 15.(-2) &\equiv 6 \,(mod\ 18) \end{aligned}$$

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

Cvičenia

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

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

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

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

1.7 Aritmetické funkcie φ, τ, σ

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

(2) Aritmetická funkcia $f\colon \mathbb{N} \to \mathbb{R}$ 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 $f(m.n) = f(m).f(n)$,

Príklad. Eulerova funkcia φ je aritmetická funkcia a ukážeme, že je multiplikatívna.
Funkcia $\pi\colon \mathbb{N} \to \mathbb{R}$, $\pi(n)$ je počet všetkých prvočísel menších alebo rovných ako n je aritmetická funkcia, nie je multiplikatívna. $\pi(2) = 1$, $\pi(3) = 2$, $\pi(6) = 3$, $(2, 3) = 1$, $6 = 2.3$, $3 = \pi(6) \neq \pi(2).\pi(3) = 2$

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

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

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 $\sigma(p) = p + 1$.

$\tau, \sigma\colon \mathbb{N} \to \mathbb{R}$ 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) $\sigma(n) = \frac{p_1^{l_1+1}-1}{p_1-1} \cdot \dots \cdot \frac{p_k^{l_k+1}-1}{p_k-1} = (p_1^{l_1} + p_1^{l_1-1} + \dots p_1 + 1) \dots (p_k^{l_k} + p_k^{l_k-1} + \dots p_k + 1)$

Dôkaz. (1) $d \mid n \Leftrightarrow d = p_1^{t_1} \dots p_k^{t_k}$, kde $0 \le t_i \le l_i$ pre $i = 1, \dots, k$. Teda $\tau(n) = (t_1 + 1) \dots (t_k + 1)$.
(2) $(p_1^{l_1} + p_1^{l_1-1} + \dots p_1 + 1)(p_2^{l_2} + p_2^{l_2-1} + \dots p_2 + 1) \dots (p_k^{l_k} + p_k^{l_k-1} + \dots p_k + 1) = \sum\limits_{0 \le t_i \le l_i} p_1^{t_1} \dots p_k^{t_k} = \sum\limits_{d|n} d = \sigma(n)$ □

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

Kapitola 2

g-adické rozvoje reálnych čísel. Kritéria iracionálnosti.

V tejto kapitole sa budeme zaoberať reálnymi číslami. Najprv pripomeňme pojem reálneho 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 $a.n \in \mathbb{Z}$).
Celé číslo z sa nazýva *celá časť* reálneho čísla a, ak platí: $z \le a < z + 1$. Označenie: $[a]$. Teda $[a] \in \mathbb{Z}$ a $[a] \le a < [a] + 1$.
Je zrejmé, že ak $a \ge 0$, tak $[a] \in \mathbb{N}_0$.
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

Veta 2.1.1. *Nech $g \in \mathbb{N}$, $g \ge 2$. Potom každé reálne číslo $r \in \mathbb{R}_0^+$ možno jednoznačne vyjadriť v tvare $r = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \dots + \frac{c_k}{g^k} + \dots = c_0 + \sum\limits_{k=1}^{\infty} \frac{c_k}{g^k}$, kde $c_0 \in \mathbb{N}_0$, pre každé $k \in \mathbb{N}$ $c_k \in \{0, 1, \dots, g-1\}$ a pre nekonečne veľa $k \in \mathbb{N}$ platí $c_k < g - 1$.*

Dôkaz. Existencia. Položme $c_0 = [r]$, $r_1 = r - c_0$. Zrejme $0 \le r_1 < 1$ a $r = c_0 + r_1$.
Ďalej, $c_1 = [g.r_1]$, $r_2 = g.r_1 - c_1$. Platí $0 \le r_2 < 1$, $gr_1 = c_1 + r_2$. Z $0 \le gr_1 < g$ vyplýva $0 \le [gr_1] < g$, t.j. $0 \le c_1 < g$.
$c_2 = [g.r_2]$, $r_3 = gr_2 - c_2$. Platí $0 \le r_3 < 1$, $gr_2 = c_2 + r_3$, $0 \le [gr_2] \le gr_2 < g$, t.j. $0 \le c_2 < g$.
Takto možno pokračovať matematickou indukciou, t.j. predpokladajme, že máme definované c_n, $0 \le c_n < g$, r_{n+1}, $0 \le r_{n+1} < 1$. Potom definujeme

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

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

Dôkaz. $\boxed{\Rightarrow}$ Pre $p = 2$ máme $1! = 1 \equiv -1\,(mod\ 2)$ a teda výrok platí. Nech $p > 2$. Polynóm

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - (x^{p-1}-1)$$

má celočíselné koeficienty a stupeň $f(x)$ je aspoň jedna a je menší alebo rovný ako $p-2$.

Pre každé $k \in \{1, \dots, p-1\}$ platí

$$f(k) = (k-1)\dots\underbrace{(k-k)}_{0}\dots(k-(p-1)) - (k^{p-1}-1) = -k^{p-1}+1.$$

Pretože $p \nmid k$, platí $(k,p) = 1$ a podľa Eulerovej vety $k^{p-1} \equiv 1\,(mod\ p)$. Potom ale

$$f(k) = -k^{p-1} + 1 \equiv 0\,(mod\ p).$$

Teda zvyškové triedy $[1]_p, [2]_p, \dots, [p-1]_p$ sú navzájom rôzne riešenia kongruencie $f(x) \equiv 0\,(mod\ p)$, a preto p delí všetky koeficienty $f(x)$. Absolútny koeficient $f(x)$ je číslo $(p-1)!+1$, a preto $p \mid (p-1)!+1$. Teda

$$(p-1)! \equiv -1\,(mod\ p).$$

$\boxed{\Leftarrow}$ Nech by p bolo zložené. Potom $p = m.n$, $1 < m, n < p$. Teda $p \mid m.n \mid (p-1)!$, pretože m aj n sa vyskytnú medzi činiteľmi vystupujúcimi v $(p-1)!$. Dostali sme $(p-1)! \equiv 0\,(mod\ p)$ a súčasne $(p-1)! \equiv -1\,(mod\ p)$, čo je spor. □

$p_1, \dots, p_k, q_1, \dots, q_s$ 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

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

Podľa vety 1.7.4
$\tau(m.n) = (l_1+1)\dots(l_k+1)(r_1+1)\dots(r_s+1) = \tau(m).\tau(n)$
$\sigma(m.n) = (p_1^{l_1} + p_1^{l_1-1} + \dots + p_1 + 1)\dots(p_k^{l_k} + p_k^{l_k-1} + \dots + p_k + 1)(q_1^{r_1} + q_1^{r_1-1} + \dots + q_1 + 1)\dots(q_s^{r_s} + q_s^{r_s-1} + \dots + q_s + 1) = \sigma(m).\sigma(n)$ □

Veta 1.7.6. *Pre Eulerovu funkciu φ platí:*

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

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

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

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

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

$$\sum_{d|n}\varphi(d) = (1+(p_1-1)+(p_1^2-p_1)+\dots+(p_1^{l_1}-p_1^{l_1-1})).$$
$$(1+(p_2-1)+(p_2^2-p_2)+\dots+(p_2^{l_2}-p_2^{l_2-1}))\dots$$
$$\dots(1+(p_k-1)+(p_k^2-p_k)+\dots+(p_k^{l_k}-p_k^{l_k-1})) = p_1^{l_1}\dots p_k^{l_k} = n.$$

□

Číslo $n \in \mathbb{N}$ sa nazýva *perfektné*, ak $\sigma(n) = 2n$, t.j. súčet vlastných deliteľov čísla n je rovný n. Perfektné čísla sú napríklad 6=1+2+3 ($\sigma(6) = 12$), 28 ($\sigma(28) = 56$), 496, 8 128 . 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 perfektné a každé párne perfektné 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 perfektné číslo. Potom $a = m.2^{n-1}$, $n \geq 2$, $m > 0$, m je nepárne. Pretože a je perfektné, platí

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

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

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

Teda m má len 2 kladných deliteľov, a preto m je prvočíslo. Potom $\frac{m}{2^n-1} = 1$, a 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 perfektných čísel je nekonečne veľa. V súčasnosti nie je známe ani jedno nepárne perfektné číslo. Je dokázené, 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 perfektné 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 $a.x \equiv b\,(mod\ p)$ je lineárna kongruencia. Ak $(a, p) = 1$, tak daná kongruencia má práve jedno riešenie. Ak teda $a.x \equiv b\,(mod\ p)$ 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,

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

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

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

$$f(x) \equiv 0\,(mod\ p)$$

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

$$p \mid a_i.$$

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

Pre $n = 1$ máme kongruenciu

$$a_1 x + a_0 \equiv 0\,(mod\ p).$$

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

$$a_1 c_0 \equiv a_1 c_1\,(mod\ p).$$

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

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

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

a kongruencia

$$a_{n+1} x^{n+1} + \ldots + a_1 x + a_0 \equiv 0\,(mod\ p)$$

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

$$f(c_i) \equiv 0\,(mod\ p).$$

Vydelíme polynóm $f(x)$ polynómom $x - c_0$ (so zvyškom) a dostaneme $f(x) = (x - c_0).g(x) + r$, kde $g(x) = b_n x^n + \ldots + b_0$, $r \in \mathbb{Z}$. 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 $f(c_i) = (c_i - c_0)g(c_i) + f(c_0) \equiv 0\,(mod\ p)$. Pretože $f(c_0) \equiv 0\,(mod\ p)$, dostávame $(c_i - c_0)g(c_i) \equiv 0\,(mod\ p)$ a teda $p \mid (c_i - c_0)g(c_i)$. Pretože $[c_i]_p \neq [c_0]_p$ platí $c_i \not\equiv c_0\,(mod\ p)$ a teda $p \nmid c_i - c_0$. Pretože p je prvočíslo, dostávame $p \mid g(c_i)$ a teda

$$g(c_i) \equiv 0\,(mod\ p).$$

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

Z platnosti

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

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

Ako dôsledok Lagrangeovej vety dostávame vetu Wilsonovu,[4] ktorú však ako prvý dokázal Lagrange.

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

$$(p - 1)! \equiv -1\,(mod\ p).$$

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