1 Deliteľnosť v obore celých čísel

1.1 Základné pojmy a ich vlastnosti

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 $a \mid b$).

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* $d, d' \in Z$ $a \mid d.b \pm d'.c$.

(10) Ak $a \mid b$ *a* $b \neq 0$, *tak* $|a| \leq |b|$.

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 $0 \leq q < n$.*

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 $(a, b) = 1$ ($(a, b) \neq 1$).

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.*

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

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*

$$d = ra + sb.$$

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* $(a',b')=1$.

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: $[a,b]$.

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* $(a,b)[a,b]=|a||b|$.

1.2 Prvočísla

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 $m=kl$).

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* $m,n \in \mathbb{N}$ $(p^m,q^n)=1$.

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

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

Veta 1.2.5. *Množina všetkých prvočísel je nekonečná.*

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* $0 \leq t_i \leq l_i$.

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*

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

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*

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

1.3 Číselné sústavy

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 $c_0, \ldots, c_k \in \mathbb{N}_0$ tak, že pre všetky $i \in \{0, \ldots, k\}$ $c_i \leq g-1$, $c_k \neq 0$ a $n = c_k g^k + \ldots 1 + c_1 g + c_0$. Toto vyjadrenie je jednoznačné.*

1.4 Kongruencie

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

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* $0 \leq k, l < n$, *tak* $a \equiv b \,(mod\ n) \Leftrightarrow k = l$.

(9) Ak $a \equiv b \,(mod\ n)$, *tak* $(a, n) = (b, n)$.

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.*

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 $[a]_n = [k]_n$.

Veta 1.4.5. *(a) Pre každé $n \in \mathbb{N}$ je $(\mathbb{Z}/mod\ n, \oplus)$ komutatívna grupa.*

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

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.*

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

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 $q = c_0 + c_1 10 + c_2 10^2 - (c_3 + c_4 10 + c_5 10^2) + (c_6 + c_7 10 + c_8 10^2) - \ldots = c_2 c_1 c_0 - c_5 c_4 c_3 + c_8 c_7 c_6 - \ldots$.*

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:*

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

1.5 Eulerova funkcia a Eulerova veta

Definícia 1.5.1 (Eulerova[1] funkcia). Zobrazenie $\varphi\colon \mathbb{N} \to \mathbb{R}$, 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.)

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

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

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

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

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

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*

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

1.6 Lineárne kongruencie s jednou neznámou

Definícia 1.6.1. Zvyšková trieda $[c]_n$ modulo n sa nazýva *riešením* lineárnej kongruencie $a.x \equiv b\,(mod\ n)$ ak $a.c \equiv b\,(mod\ n)$.

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.

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 $f(m.n) = f(m).f(n)$,

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

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.

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

[1] Euler 1707-1783

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

Veta 1.7.6. *Pre Eulerovu funkciu φ platí:*

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

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.*

1.8 Doplnky. Lagrangeova a Wilsonova veta.

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 $i = 1, \ldots, n$

$$p \mid a_i.$$

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

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

2 g-adické rozvoje reálnych čísel. Kritéria iracionálnosti.

2.1 g-adický rozvoj

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

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.

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.*

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 $k^n = m$.*

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 $r = 10^z$.*