UNIVERZITA PALACKÉHO V OLOMOUCI
Přírodovědecká fakulta
Katedra algebry a geometrie

BAKALÁŘSKÁ PRÁCE

Dělitelnost v oboru celých čísel na středních školách

Vedoucí bakalářské práce:
RNDr. Jaroslav Švrček, CSc.
Rok odevzdání: 2015

Vypracoval:
Tomáš Riemel
F-M, III. ročník

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně pod vedením pana RNDr. Jaroslava Švrčka, CSc., s použitím uvedené literatury.

V Olomouci 15. dubna 2015 .....

Poděkování

Rád bych poděkoval vedoucímu bakalářské práce panu RNDr. Jaroslavu Švrčkovi, CSc., za spolupráci i za čas, který mi věnoval při konzultacích.

Obsah

Seznam použitých symbolů

$\mathbb{N} = \{1, 2, 3, \dots\}$ ..... množina všech přirozených čísel

$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ ..... množina všech nezáporných celých čísel

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ ..... množina všech celých čísel

$\mathbb{R}$ ..... množina všech reálných čísel

$\emptyset$ ..... prázdná množina

$a \in T$ ..... prvek a náleží množině T

$a \,|\, b$ ..... číslo a dělí číslo b

$a \nmid b$ ..... číslo a nedělí číslo b

$D(a, b)$ ..... největší společný dělitel čísel a, b

$n(a, b)$ ..... nejmenší společný násobek čísel a, b

$|M|$ ..... počet prvků konečné množiny M

$\sum$ ..... sumační znak

$\square$ ..... konec řešení příkladu (důkazu)

Úvod

Cílem této bakalářské práce je vytvořit ucelený soubor poznatků z dělitelnosti v oboru celých čísel, který může mj. sloužit jako učební pomůcka ve výběrových seminářích z matematiky na gymnáziích a jiných středních školách. Dělitelnost v oboru celých čísel se jako samostatná látka na středních školách nevyučuje, neboť není součástí rámcových vzdělávacích programů (RVP) na středních školách. I přesto se při výuce matematiky na středních školách očekává, že poznatky z dělitelnosti v oboru celých čísel žáci znají a umí je používat. Jedno z možných využití této bakalářské práce, jak bylo výše uvedeno, je vytvoření opěrného materiálu základních poznatků dělitelnosti a jeho aplikací při řešení nadstandardních úloh z matematiky i některých běžných úloh jiným a netradičním způsobem pro žáky středních škol.

Práce je rozdělena do tří kapitol, které jsou dále rozděleny do dalších částí. První kapitola je věnována dělitelnosti v oboru celých čísel, druhá číselným funkcím a třetí diofantovským rovnicím. V každé kapitole lze nalézt ukázky aplikací poznatků při řešení úloh (úlohy řešené i neřešené týkající se dané problematiky) či jednoduché důkazy. Příklady jsou vždy setříděny od jednodušších po obtížnější, přičemž neřešené příklady na konci každé kapitoly by měl být žák schopen vyřešit na základě znalosti řešení úloh řešených dříve.

Celá práce je vysázená systémem LaTeX.

1 Dělitelnost v oboru celých čísel

Na počátku bakalářské práce nejprve zavedeme pojem *číselná kongruence*, která má zásadní význam při řešení úloh týkajících se dělitelnosti celých čísel a zavádí se pro zjednodušení výpočtů. Po zavedení pojmu číselná kongruence uvedeme několik základních tvrzení, ve kterých budou prezentovány základní vlastnosti číselných kongruencí. Prezentované vlastnosti budeme dále využívat při řešení navazujících příkladů uvedených vždy na konci každé kapitoly.

Uveďme nejprve následující, poměrně známou, (motivační) úlohu.

Úloha

Žáci na základní škole nastoupili v tělocvičně do jedné řady. Pokud žáky uspořádáme do dvou řad, bude nám přebývat jeden žák. Pokud žáky uspořádáme do tří řad, zbydou nám dva žáci. Pokud žáky postupně uspořádáme do čtyř, pěti a šesti řad, zbydou nám postupně tři, čtyři a pět žáků. Pokud žáky uspořádáme do sedmi řad, nebude přebývat žádný žák. Jaký je *minimální* počet žáků v tělocvičně?[1]

1.1 Číselné kongruence

Definice 1.1.1

Nechť $a, b \in \mathbb{Z}$. Řekneme, že *číslo* b *dělí číslo* a, právě když existuje číslo $t \in \mathbb{Z}$, pro něž platí $a = tb$. Symbolicky značíme $b \mid a$. Pokud neexistuje žádné číslo $t \in \mathbb{Z}$, pro něž platí $a = tb$, řekneme, že *číslo* b *nedělí číslo* a, což symbolicky zapisujeme $b \nmid a$.

Definice 1.1.2

Nechť $n \in \mathbb{N}$, $(n \neq 1)$, a dále $a, b \in \mathbb{Z}$. Řekneme, že číslo a je *kongruentní* s číslem b podle modulu n (modulo n), právě když $n \mid (a - b)$ a píšeme symbolicky

$$a \equiv b \pmod{n}. \tag{1}$$

Vztah (1) se nazývá *číselná kongruence*. Čísla a, b budeme nazývat *levou a pravou stranou číselné kongruence* (1).

[1] Řešení příkladu je možné nalézt v části 1.4 na straně 26.

Úmluva. V celém dalším textu budeme vždy uvažovat číselné kongruence podle modulu $n \neq 1$.

Dále zde vyslovíme některé důležité věty o číselných kongruencích, v nichž jsou popsány vlastnosti číselných kongruencí. Jejich detailní důkazy lze najít např. v [3].

Věta 1.1.3

Nechť $a, b, c \in \mathbb{Z}$. Potom pro každé $n \in \mathbb{N}$ platí:

(i) $a \equiv a \pmod{n}$. (2)

(ii) Pokud $a \equiv b \pmod{n}$, pak je i $b \equiv a \pmod{n}$. (3)

(iii) Pokud $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, pak je i $a \equiv c \pmod{n}$. (4)

Věta 1.1.4

Nechť $a, b, c \in \mathbb{Z}$ a $n \in \mathbb{N}$. Je-li $a \equiv b \pmod{n}$, pak platí:

(i) $a + c \equiv b + c \pmod{n}$. (5)

(ii) $a - c \equiv b - c \pmod{n}$. (6)

(iii) $ac \equiv bc \pmod{n}$. (7)

Věta 1.1.5

Nechť $a, b, c, d \in \mathbb{Z}$ a $n \in \mathbb{N}$. Je-li $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, pak platí:

(i) $a + c \equiv b + d \pmod{n}$. (8)

(ii) $a - c \equiv b - d \pmod{n}$. (9)

(iii) $ac \equiv bd \pmod{n}$. (10)

Věta 1.1.6

Nechť $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$. Je-li $a \equiv b \pmod{n}$, pak pro každé $k \in \mathbb{N}$ platí

$$a^k \equiv b^k \pmod{n}. \tag{11}$$

Věta 1.1.7

Nechť $a, b, c \in \mathbb{Z}, n \in \mathbb{N}$ a největší společný dělitel $D(c, n) = 1$.
Jestliže platí

$$ac \equiv bc \pmod{n},$$

pak také

$$a \equiv b \pmod{n}. \tag{12}$$

Ve výše uvedených větách (1.1.3 – 1.1.7) jsou popsány základní vlastnosti číselných kongruencí. Vztahy (2) – (12) budeme používát při řešení příkladů, v nichž budeme na tyto vztahy odkazovat.

V níže popsaném příkladě ukážeme využití číselných kongruencí při počítání s vysokými čísly.

Příklad 1

Určete zbytky čísel 4, 4^2, 4^3, 4^4, 4^5 při dělení číslem 23.

Řešení. Evidentně platí následující číselné kongruence

$$\begin{aligned} 4 &\equiv 4 \pmod{23}, \\ 4^2 &\equiv 16 \pmod{23}, \\ 4^3 = 64 &\equiv 18 \pmod{23}, \\ 4^4 = 256 &\equiv 3 \pmod{23}, \\ 4^5 = 1024 &\equiv 12 \pmod{23}. \end{aligned}$$

Závěr. Pravé strany pěti výše uvedených kongruencí dávají odpovídající zbytky při dělení číslem 23. □

V příkladu 1 jsme vyšší mocniny nahradili pomocí číselné kongruence jejich zbytkem (při dělení daným modulem). Tento postup se hojně využívá při řešení následujících úloh.

Příklad 2

Najděte zbytek při dělení čísla 64^{13} číslem 15.

Řešení. Předně si uvědomme, že $16 \equiv 1 \pmod{15}$. Dále ze vztahů (7) a (11) plyne

$$64^{13} = (4 \cdot 16)^{13} = 4^{13} \cdot 16^{13} \equiv 4^{13} \cdot 1^{13} = (4 \cdot 1)^{13} = 4^{13} \pmod{15}.$$

Použijeme-li dále vztah (7), dostaneme na základě vztahu (11)

$$64^{13} \equiv 4^{13} = 4^3 \cdot 4^3 \cdot 4^3 \cdot 4^3 \cdot 4 \pmod{15},$$

$$64^{13} \equiv 64 \cdot 64 \cdot 64 \cdot 64 \cdot 4 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \pmod{15}.$$

Využijeme výsledek předchozího výpočtu a číselné kongruence $16 \equiv 1 \pmod{15}$. Nakonec použijeme vztah (7) a vztah (11)

$$64^{13} \equiv 4^5 = 4^3 \cdot 4^2 = 64 \cdot 16 \equiv 4 \cdot 1 = 4 \pmod{15}.$$

Závěr. Zbytek při dělení čísla 64^{13} číslem 15 je tedy 4. □

Příklad 3

Dokažte, že číslo $97^{99} + 99^{97}$ je dělitelné číslem 49.

Řešení. Nejprve určíme zbytky při dělení číslem 49 u obou sčítanců. Pokud vyjde číslo kongruentní s číslem 0, tak je daný součet dělitelný číslem 49. Všimněme si, že

$$97 \equiv -1 \pmod{49}.$$

Využitím vztahu (11) dále máme

$$97^{99} \equiv (-1)^{99} = -1 \pmod{49}. \tag{K1}$$

Nyní užijeme číselnou kongruenci $99 \equiv 1 \pmod{49}$ a dále vztah (11)

$$99^{97} \equiv 1^{97} = 1 \pmod{49}. \tag{K2}$$

Sečtením číselných kongruencí (K1) a (K2) na základě vztahu (8) získáme

$$97^{99} + 99^{97} \equiv -1 + 1 = 0 \pmod{49}.$$

Dané číslo je tudíž dělitelné číslem 49, což jsme chtěli dokázat. □

Další příklady.

Příklad 4

Určete zbytek při dělení čísla 2^{30} číslem 7. [zb. 1]

Příklad 5

Najděte zbytek při dělení čísla 3^{15} číslem 12. [zb. 3]

Příklad 6

Najděte zbytek při dělení čísla $2^{44\,444}$ číslem 7. [zb. 4]

Příklad 7

Rozhodněte, zda je číslo $5^{11} + 7^2$ dělitelné číslem 6. [zb. 0]

1.2 Kritéria dělitelnosti

V této podkapitole vyslovíme a vysvětlíme kritéria dělitelnosti čísly $3, 4, 7, 8, 9$, 11 a 13. Mnozí určitě znají ze střední školy, že dané číslo je dělitelné číslem 3, právě když součet všech číslic daného čísla je dělitelný 3. Na základní i střední škole se využívá uvedená poučka, ale nevysvětluje se, jakým způsobem se k ní došlo. Proto cílem části bude objasnit známá kritéria dělitelnosti čísly $3, 4, 8, 9$ a 11 (pomocí číselných kongruencí) a zároveň ukázat, jak získat kritéria dělitelnosti pro dané číslo. V našem případě pro osvětlení postupu tvorby kritérií číselných dělitelností použijeme čísla 7 a 13.

Pro připomenutí zde uvedeme definici dekadického zápisu přirozeného čísla.

Definice 1.2.1

Nechť $n \in \mathbb{N}$ a $k \in \mathbb{N}_0$. Zápis čísla n ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0,$$

kde každé $a_i \in \{0, 1, 2, \ldots, 9\}$ pro $i \in \{0, 1, 2, \ldots, k\}$, přičemž $a_k \neq 0$, nazýváme *dekadický zápis čísla* n (*zápis čísla* n *v desítkové soustavě*). Čísla a_i nazýváme *číslice*. Součet všech jeho číslic a_i budeme značit $s(n)$.

Definice 1.2.2

Nechť číslo $n \in \mathbb{N}$ je zapsáno v desítkové soustavě ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0.$$

Součet $a_0+a_2+a_4+\ldots$ nazýváme *součet všech číslic na sudých pozicích* a budeme dále značit s_0. Součet $a_1 + a_3 + a_5 + \ldots$ nazýváme *součet všech číslic na lichých pozicích* a budeme jej značit s_1.

1.2.1 Kritérium dělitelnosti číslem 3

V této části si objasníme kritérium dělitelnosti číslem 3. Uvažujme přirozené číslo n zapsané (v desítkové soustavě) ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0.$$

Předně si uvědomme, že $10 \equiv 1 \pmod 3$ a dále na základě vztahu (11) z části 1.1 pro libovolné $k \in \mathbb{N}$ rovněž platí $10^k \equiv 1^k = 1 \pmod 3$, tedy

$$\begin{aligned} 10^0 &\equiv 1 \pmod 3, \\ 10^1 &\equiv 1 \pmod 3, \\ 10^2 &\equiv 1 \pmod 3, \\ &\vdots \\ 10^k &\equiv 1 \pmod 3. \end{aligned}$$

Nyní použijeme opakovaně vztah (7) z části 1.1 na číslo n pro nahrazení mocnin 10 číslem 1

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0 \equiv s(n) \pmod 3.$$

Odtud plyne, že číslo n dává stejný zbytek při dělení číslem 3 jako součet všech jeho číslic. Symbolicky zapsáno:

$$n \equiv s(n) \pmod 3.$$

Z předchozího řádku již plyne známé kritérium dělitelnosti číslem 3, viz následující věta.

Věta 1.2.1.1 (kritérium dělitelnosti číslem 3)

Přirozené číslo n je dělitelné třemi, právě když je součet všech jeho číslic dělitelný třemi. Symbolicky zapsáno: $3 \mid n \Leftrightarrow 3 \mid s(n)$.

Poznámka 1. Analogickým způsobem lze odvodit i kritérium dělitelnosti číslem 9. Číslo je dělitelné číslem 9, právě když je součet všech jeho číslic dělitelný 9. Symbolicky pak: $9 \mid n \Leftrightarrow 9 \mid s(n)$.

Poznámka 2. Číslo 6 lze zapsat ve tvaru $6 = 2 \cdot 3$. Snadno lze odvodit, že dané číslo je dělitelné číslem 6, právě když je současně dělitelné nesoudělnými čísly 2 a 3. Tento postup lze aplikovat na každé složené číslo.

1.2.2 Kritérium dělitelnosti číslem 4

V této části si objasníme kritérium dělitelnosti číslem 4. Mějme tedy libovolné přirozené číslo n zapsané (v desítkové soustavě) ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0.$$

Předně si uvědomme, že $10^2 = 100 \equiv 0 \pmod 4$ a dále na základě vztahu (11) z části 1.1 pro $k \geq 2$ rovněž platí $10^k \equiv 0 \pmod 4$. Nyní použijeme opakovaně vztah (7) z části 1.1 pro nahrazení mocnin čísla 10 číslem 0, získáme tak podmínku (kritérium) dělitelnosti číslem 4

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0 \equiv 10 \cdot a_1 + a_0 \pmod 4.$$

Z předchozího řádku plyne známé kritérium dělitelnosti číslem 4.

Věta 1.2.2.1 (kritérium dělitelnosti číslem 4)

Přirozené číslo n je dělitelné čtyřmi, právě když je jeho poslední dvojčíslí dělitelné čtyřmi. Symbolicky zapsáno: $4 \mid n \Leftrightarrow 4 \mid (10 \cdot a_1 + a_0)$.

Poznámka. Podobným způsobem lze odvodit i dělitelnost číslem 8. Číslo je dělitelné osmi, právě když je jeho poslední trojčíslí dělitelné osmi. Symbolicky zapsáno: $8 \mid n \Leftrightarrow 8 \mid (100 \cdot a_2 + 10 \cdot a_1 + a_0)$. Analogicky lze odvodit i dělitelnost pro libovolné číslo ve tvaru 2^n.

1.2.3 Kritérium dělitelnosti číslem 7

V této části si objasníme tvorbu kritérií dělitelnosti danými čísly. Na ukázku postupu tvorby kritérií použijeme nejprve číslo 7. Mějme tedy libovolné přirozené číslo n zapsané (v desítkové soustavě) ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0.$$

Při tvorbě kritérií se snažíme najít určité pravidlo či pravidelnost, která se nám vyskytuje u mocnin čísla 10 nahrazených číselnou kongruencí podle daného modulu. V našem případě hledáme určitou pravidelnost při nahrazování mocnin čísla 10 zbytky při dělení číslem 7. Nejprve začneme s první mocninou, pak s druhou, atd., dokud nenajdeme určitou opakující se pravidelnost.
Předně si uvědomme, že $10 \equiv 3 \pmod 7$. Na základě vztahu (11) z části 1.1 platí $10^2 \equiv 3^2 \equiv 2 \pmod 7$ a $10^3 = 10^2 \cdot 10 \equiv 2 \cdot 3 = 6 \equiv -1 \pmod 7$. Dále na základě vztahu (11) z části 1.1 a kongruence $10^3 \equiv -1 \pmod 7$ pro každé $k \geq 3$ rovněž platí

$$10^k = 10^3 \cdot 10^{k-3} \equiv -10^{k-3} \pmod 7.$$

Zaveďme následující označení

$$\begin{aligned} t_0 &= a_0 + a_6 + a_{12} + \ldots, \\ t_1 &= a_1 + a_7 + a_{13} + \ldots, \\ t_2 &= a_2 + a_8 + a_{14} + \ldots, \\ t_3 &= a_3 + a_9 + a_{15} + \ldots, \\ t_4 &= a_4 + a_{10} + a_{16} + \ldots, \\ t_5 &= a_5 + a_{11} + a_{17} + \ldots \end{aligned}$$

Nyní použijeme opakovaně vztah (7) z části 1.1 pro nahrazení mocnin čísla 10, získáme tak podmínku (kritérium) dělitelnosti číslem 7

$$\begin{aligned} n \equiv a_0 + 3 \cdot a_1 + 2 \cdot a_2 - a_3 - 3 \cdot a_4 - 2 \cdot a_5 + a_6 + \ldots = \\ = t_0 + 3 \cdot t_1 + 2 \cdot t_2 - t_3 - 3 \cdot t_4 - 2 \cdot t_5 = \\ = (t_0 - t_3) + 3 \cdot (t_1 - t_4) + 2 \cdot (t_2 - t_5) \pmod 7. \end{aligned}$$

V následující větě formulujeme kritérium dělitelnosti číslem 7.

Věta 1.2.3.1 (kritérium dělitelnosti číslem 7)

Přirozené číslo n je dělitelné sedmi, právě když je dělitelný sedmi výraz

$$(t_0 - t_3) + 3 \cdot (t_1 - t_4) + 2 \cdot (t_2 - t_5).$$

Symbolicky pak: $7 \mid n \Leftrightarrow 7 \mid (t_0 - t_3) + 3 \cdot (t_1 - t_4) + 2 \cdot (t_2 - t_5)$.

1.2.4 Kritérium dělitelnosti číslem 11

V této části si objasníme kritérium dělitelnosti číslem 11. Mějme tedy libovolné přirozené číslo n zapsané v desítkové soustavě ve tvaru

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0.$$

Předně si uvědomme, že $10 \equiv -1 \pmod{11}$. Na základě vztahu (11) z části 1.1 pro každé $k \in \mathbb{N}$ rovněž platí $10^k \equiv (-1)^k \pmod{11}$, tedy

$$\begin{aligned} 10^0 &\equiv 1 \pmod{11}, \\ 10^1 &\equiv -1 \pmod{11}, \\ 10^2 &\equiv 1 \pmod{11}, \\ 10^3 &\equiv -1 \pmod{11}, \\ &\vdots \end{aligned}$$

Podle definice 1.2.2 máme označení pro součet všech číslic na sudých a lichých pozicích.

$$\begin{aligned} s_0 &= a_0 + a_2 + a_4 + \ldots \\ s_1 &= a_1 + a_3 + a_5 + \ldots \end{aligned}$$

Nyní využijeme opakovaně vztah (7) z části 1.1 pro nahrazení mocnin čísla 10 čísly -1 a 1

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_1 \cdot 10 + a_0 \equiv s_0 - s_1 \pmod{11}.$$

Číslo n dává stejný zbytek při dělení číslem 11 jako rozdíl součtů všech jeho číslic na sudých pozicích a všech číslic na lichých pozicích. Symbolicky zapsáno:

$$n \equiv s_0 - s_1 \pmod{11}.$$

Z předchozího řádku plyne známé kritérium dělitelnosti číslem 11.

Věta 1.2.4.1 (kritérium dělitelnosti číslem 11)

Přirozené číslo n je dělitelné jedenácti, právě když rozdíl součtu všech číslic na sudých pozicích a součtu všech číslic na lichých pozicích je dělitelný jedenácti. Symbolicky zapsáno: $11 \mid n \Leftrightarrow 11 \mid (s_0 - s_1)$.

1.2.5 Kritérium dělitelnosti číslem 13

Analogicky jako v předchozích částech se budeme snažit najít určité pravidlo při dělení číslem 13. Předně si uvědomme, že $10 \equiv -3 \pmod{13}$. Na základě vztahu (11) z části 1.1 platí $10^2 \equiv (-3)^2 = 9 \equiv -4 \pmod{13}$ a $10^3 = 10^2 \cdot 10 \equiv$ $\equiv 9 \cdot (-3) = -27 \equiv -1 \pmod{13}$. Na základě vztahu (11) z části 1.1 pro každé $k \geq 3$ rovněž platí $10^k \equiv 10^3 \cdot 10^{k-3} \equiv -10^{k-3} \pmod{13}$. Použijme označení $t_0 - t_5$ definované v části 1.2.3. Využijeme-li opakovaně vztah (7) z části 1.1 pro nahrazení mocnin čísla 10, získáme tak podmínku (kritérium) dělitelnosti číslem 13

$$\begin{aligned} n \equiv a_0 - 3 \cdot a_1 - 4 \cdot a_2 - a_3 + 3 \cdot a_4 + 4 \cdot a_5 + a_6 + \ldots = \\ = t_0 - 3 \cdot t_1 - 4 \cdot t_2 - t_3 + 3 \cdot t_4 + 4 \cdot t_5 = \\ = (t_0 - t_3) - 3 \cdot (t_1 - t_4) - 4 \cdot (t_2 - t_5) \pmod{13}. \end{aligned}$$

V následující větě formulujeme kritérium dělitelnosti číslem 13.

Věta 1.2.5.1 (kritérium dělitelnosti číslem 13)

Přirozené číslo n je dělitelné třinácti, právě když je dělitelný třinácti výraz

$$(t_0 - t_3) - 3 \cdot (t_1 - t_4) - 4 \cdot (t_2 - t_5).$$

Symbolicky pak: $13 \mid n \Leftrightarrow 13 \mid (t_0 - t_3) - 3 \cdot (t_1 - t_4) - 4 \cdot (t_2 - t_5)$.

Příklad 8

Za použití kritérií dělitelnosti ověřte, zda je číslo 28 985 dělitelné číslem 11.

Řešení. Pro ověřování dělitelnosti daného čísla daným modulem stačí ukázat, že dané číslo je s využitím číselných kongruencí podle kritérií dělitelnosti kongruentní s číslem 0. Pokud tomu tak není, dané číslo není dělitelné daným modulem. V našem případě máme číslo 28 985. Nejprve si dané číslo zapíšeme v desítkové soustavě a na základě kritéria dělitelnosti číslem 11 (viz věta 1.2.4.1) nahradíme jednotlivé mocniny čísla 10:

$$28\,985 = 2\cdot 10^4+8\cdot 10^3+9\cdot 10^2+8\cdot 10+5 \equiv (5+9+2)-(8+8) = 0 \equiv 0 \pmod{11}$$

Závěr. Číslo 28 985 je dělitelné číslem 11. □

Příklad 9

Zjistěte (s použitím vhodného kritéria), zda je číslo 123 456 789 101 112 dělitelné číslem 3.

Řešení. Pro ověřování dělitelnosti daného čísla daným modulem stačí opět ukázat, že dané číslo je s využitím číselných kongruencí podle kritérií dělitelnosti kongruentní s číslem 0. Pokud tomu tak není, dané číslo není dělitelné daným modulem. V našem případě máme číslo 123 456 789 101 112. Dané číslo zapíšeme v desítkové soustavě a na základě kritéria dělitelnosti číslem 3 (viz věta 1.2.1.1) nahradíme jednotlivé mocniny čísla 10:

$$\begin{aligned}123\,456\,789\,101\,112 &= 1\cdot 10^{14}+2\cdot 10^{13}+3\cdot 10^{12}+4\cdot 10^{11}+5\cdot 10^{10}+6\cdot 10^9+\\ &+7\cdot 10^8+8\cdot 10^7+9\cdot 10^6+1\cdot 10^5+0\cdot 10^4+1\cdot 10^3+1\cdot 10^2+1\cdot 10^1+2\equiv\\ &\equiv 1+2+3+4+5+6+7+8+9+1+0+1+1+1+2 = 51 \equiv 0 \pmod{3}\end{aligned}$$

Závěr. Číslo 123 456 789 101 112 je dělitelné číslem 3. □

Příklad 10

Rozhodněte (s použitím vhodného kritéria dělitelnosti), zda je číslo 18 795 dělitelné číslem 7.

Řešení. Budeme postupovat stejně jako v předchozím případě. Máme číslo 18 795. Nejprve si dané číslo zapíšeme v desítkové soustavě a na základě kritéria dělitelnosti číslem 7 (viz věta 1.2.3.1) nahradíme jednotlivé mocniny čísla 10:

$$18\,795 = 1 \cdot 10^4 + 8 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10 + 5 \equiv$$
$$\equiv (5 - 8) + 3 \cdot (9 - 1) + 2 \cdot 7 = 35 \equiv 0 \pmod 7$$

Závěr. Číslo 18 795 je tedy dělitelné číslem 7. □

Příklad 11

Dokažte, že platí $6 \mid (n^3 + 11n)$ pro libovolné $n \in \mathbb{N}$.

Řešení. Zvolme si libovolné $n \in \mathbb{N}$. V poznámce 2 v části 1.2.1 je napsáno, že libovolné přirozené číslo n je dělitelné číslem 6, právě když je zároveň dělitelné čísly 2 a 3. Mějme součin čísla n a jeho následujícího přirozeného čísla $n + 1$, pak daný součin $n(n + 1)$ je dělitelný dvěma. Neboť buď je číslo n sudé nebo je sudé číslo $n + 1$, a proto je daný součin dělitelný dvěma. Pokud tento součin ještě vynásobíme číslem $n + 2$, získáme číslo, které je dělitelné třemi. Neboť v součinu tří po sobě jdoucích přirozených čísel je jedno násobkem čísla 3 a tudíž je daný součin dělitelný třemi. Povšimněme si nyní, že součin tří po sobě jdoucích přirozených čísel je dělitelný dvěma i třemi, tudíž je dělitelný i šesti dle poznámky 2 na straně 13. Vytvořme si následující součin tří po sobě jdoucích čísel (předpokládejme, že $n \neq 1$):

$$(n - 1) \cdot n \cdot (n + 1) = n^3 - n$$

Tento součin je dělitelný šesti. Využijme nyní číselné kongruence $11 \equiv -1 \pmod 6$ a vztahů (7) a (8) z části 1.1:

$$n^3 - n = n \cdot (n^2 - 1) \equiv n \cdot (n^2 + 11) = n^3 + 11n \pmod 6$$

Číslo $n^3 - n$ dává stejný zbytek při dělení šesti jako číslo $n^3 + 11n$. Jelikož $6 \mid (n^3 - n)$, pak také $6 \mid (n^3 + 11n)$. Tím je důkaz uzavřen. □

Podobně lze řešit následující příklady.

Příklad 12

Pomocí kritérií dělitelnosti zjistěte, zda je číslo 35 961 dělitelné číslem 3.

[zb. 0]

Příklad 13

Pomocí kritérií dělitelnosti zjistěte, zda je číslo 862 464 dělitelné číslem 4.

[zb. 0]

Příklad 14

S využitím kritérií dělitelnosti zjistěte, zda je číslo 15 325 dělitelné číslem 11.

[zb. 2]

Příklad 15

Pomocí kritérií dělitelnosti zjistěte, zda je číslo 249 354 dělitelné číslem 7.

[zb. 0]

1.3 Kongruenční rovnice 1. stupně

V této části se budeme zabývat pojmem *kongruenční rovnice*. Nejprve tento pojem definujeme a pak s ním budeme dále pracovat. V rámci této práce se omezíme pouze na kongruenční rovnice 1. stupně a jejich soustavy.

Definice 1.3.1

Nechť $n \in \mathbb{N}$ a nechť $p \in \{0,\, 1,\, 2, \ldots,\, n-1\}$. Uvažujme n množin $\mathcal{Z}_0, \mathcal{Z}_1, \ldots,$ $\mathcal{Z}_{n-1}$ tak, že do množiny $\mathcal{Z}_p$ patří všechna celá čísla, která jsou kongruentní s číslem p podle modulu n. Tyto množiny se nazývají *zbytkové třídy podle modulu* n.

Definice 1.3.2

Nechť $n \in \mathbb{N}$, $p \in \{0,\, 1,\, 2, \ldots,\, n-1\}$ a dále nechť $\mathcal{Z}_p$ je zbytková třída čísla p podle modulu n. Jakýkoliv prvek z dané zbytkové třídy podle modulu n nazýváme *reprezentant zbytkové třídy* $\mathcal{Z}_p$ *podle modulu* n. Prvky ze stejné zbytkové třídy podle daného modulu jsou ekvivalentní vzhledem k uvažovanému modulu n.

Definice 1.3.3

Nechť $n \in \mathbb{N}$. Libovolnou soustavu n celých čísel , kterou získáme, vezmeme-li z každé zbytkové třídy $\mathcal{Z}_0, \mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_{n-1}$ podle modulu n po jednom prvku, budeme nazývat *úplná soustava zbytků podle modulu n*.

Poznámka. Výše uvedené definice (1.3.1 – 1.3.3) lze najít např. v [3] a následující definici 1.3.4 lze nalézt např. v [8].

Definice 1.3.4

Každá rovnice ve tvaru

$$ax \equiv b \pmod{n}, \tag{13}$$

kde x je neznámá, $x \in \mathbb{Z}$, a, b jsou daná celá čísla a $a \not\equiv 0$, se nazývá *kongruenční rovnice 1. stupně*. Řešit danou lineární rovnici znamená najít všechna vyhovující celá čísla x ze zbytkové třídy vzhledem k danému modulu.

Věta 1.3.5 (viz např. v [8])

Při řešení kongruenčních rovnic 1. stupně nastane vždy právě jedna z možností:

1. Je-li $D(a, n) = 1$, pak má rovnice (13) jediné řešení.
2. Je-li $D(a, n) = c > 1$, pak platí
   (i) pro $c \nmid b$ rovnice (13) není řešitelná.
   (ii) pro $c \mid b$ má rovnice (13) právě c řešení.

Poznámka. Při úpravách kongruenčních rovnic musíme dávat pozor na skutečnost, že při násobení obou stran rovnice číslem, které je soudělné s daným modulem, nemusíme vždy dostat ekvivalentní rovnice. (Tato skutečnost plyne např. z tzv. malé Fermatovy věty uvedené na straně 34). Např.

$$x - 1 \equiv 0 \pmod{5} \quad \text{a} \quad 5x - 5 \equiv 0 \pmod{5}$$

První rovnice má právě jedno řešení a druhá je identická (x může být libovolné číslo patřící do úplné soustavy zbytků podle modulu 5), tudíž nejsou ekvivalentní.

Příklad 16

V oboru celých čísel řešte rovnici $3x \equiv 5 \pmod 7$.

Řešení. Snadno se vidí, že $D(3,7) = 1$. Je třeba uvažovat případ 1 z věty 1.3.5. Dále chceme dělit celou rovnici číslem 3. Jelikož $D(3,7) = 1$, je úprava korektní a nemění počet řešení. Abychom toho dosáhli, budeme přičítat (odečítat) modul 7 k číslu 5 (dle vztahů (8) a (9) v části 1.1), dokud nezískáme číslo, jenž je dělitelné číslem 3. V našem případě jsme nalezli číslo 12. Proto číslo 5 nahradíme pomocí číselné kongruence číslem 12 a dořešíme na základě vztahu (12) z části 1.1

$$\begin{aligned} 3x &\equiv \ 5 \pmod 7, \\ 3x &\equiv 12 \pmod 7, \\ x &\equiv \ 4 \pmod 7. \end{aligned}$$

Závěr. Zadaná kongruenční rovnice má jediné řešení a tím je zbytková třída $\mathcal{Z}_4$, což je jinak zapsáno $x = 4 + 7k$, kde $k \in \mathbb{Z}$. □

Příklad 17

V oboru celých čísel řešte následující rovnici $10x \equiv 4 \pmod{15}$.

Řešení. Uvědomme si, že $D(10,15) = 5$. Jelikož $5 \nmid 4$, dostáváme případ 2(i) z věty 1.3.5.

Závěr. Daná kongruenční rovnice *nemá řešení v oboru celých čísel.* □

Příklad 18

V oboru celých čísel řešte následující rovnici $4x \equiv 8 \pmod{22}$.

Řešení. Uvědomme si, že $D(4,22) = 2 = d$. Jelikož $2 \mid 8$, má daná *rovnice právě d řešení*, a to na základě případu 2(ii) z věty 1.3.5. Danou rovnici můžeme dělit 2 a převést na následující tvar

$$2x \equiv 4 \pmod{11}.$$

Pozor musíme dát na skutečnost, že jsme rovnici převedli do nového modulu. Dále řešíme rovnici stejně jako případ 1 z věty 1.3.5. Chceme dělit celou rovnici

číslem 2. Jelikož $D(2, 11) = 1$, je úprava korektní a nemění počet řešení. Abychom toho dosáhli, budeme přičítat (odečítat) modul 11 k číslu 2 (dle vztahů (8) a (9) v části 1.1), dokud nezískáme číslo, které je dělitelné číslem 2. V našem případě jsme nalezli číslo 26. Číslo 4 tudíž nahradíme pomocí číselné kongruence číslem 26 a řešíme na základě vztahu (12) z části 1.1

$$2x \equiv 26 \pmod{11}.$$

Nyní využijeme vztah (1) z části 1.1

$$x \equiv 13 \equiv 2 \pmod{11}.$$

Získané řešení musíme převést do původního modulu. Postupujeme následovně. Číslo t volíme z úplné soustavy zbytků podle modulu d. Zde $t \in \{0, 1\}$. Řešení původní rovnice je ve tvaru $x \in \{2+11t,\ t \in \{0, 1\}\}$.[2] Řešením původní rovnice jsou zbytky 2 a 13, které jsme získali po dosazení všech čísel za t z dané úplné soustavy zbytků podle modulu d. Ovšem všechna řešení původní rovnice jsou všechna celá čísla, která jsou kongruentní s čísly 2 a 13.

Závěr. Všechna řešení zadané kongruenční rovnice jsou zbytkové třídy $\mathcal{Z}_2$ a $\mathcal{Z}_{13}$ podle modulu 22. □

Podobné příklady.

Příklad 19

V oboru celých čísel řešte rovnici $11x \equiv 2 \pmod{9}$. $[\mathcal{Z}_1]$

Příklad 20

V oboru celých čísel řešte rovnici $13x \equiv 11 \pmod{26}$. $[\emptyset]$

Příklad 21

V oboru celých čísel řešte rovnici $21x \equiv 19 \pmod{40}$. $[\mathcal{Z}_{39}]$

Příklad 22

V oboru celých čísel řešte rovnici $12x \equiv 9 \pmod{21}$. $[\mathcal{Z}_6, \mathcal{Z}_{13}, \mathcal{Z}_{20}]$

[2] Číslo 11 není náhodně zvolené. Je to hodnota nového modulu v upravené rovnici.

1.4 Soustavy kongruenčních rovnic 1. stupně, čínská věta o zbytcích

Při řešení úloh se často můžeme setkat nejenom s kongruenčními rovnicemi 1. stupně, nýbrž i s jejich soustavami

$$\left.\begin{array}{ll} a_1x \equiv b_1 & (\mathrm{mod}\ n_1), \\ a_2x \equiv b_2 & (\mathrm{mod}\ n_2), \\ a_3x \equiv b_3 & (\mathrm{mod}\ n_3), \\ & \vdots \\ a_kx \equiv b_k & (\mathrm{mod}\ n_k). \end{array}\right\} \tag{14}$$

Definice 1.4.1

Soustava konguenčních rovnic 1. stupně (14) *má řešení*, právě když má řešení každá kongruenční rovnice 1. stupně této soustavy.

Poznámka. Pokud je soustava (14) řešitelná, pak ji lze zapsat ve tvaru

$$\left.\begin{array}{ll} x \equiv c_1 & (\mathrm{mod}\ n_1), \\ x \equiv c_2 & (\mathrm{mod}\ n_2), \\ x \equiv c_3 & (\mathrm{mod}\ n_3), \\ & \vdots \\ x \equiv c_k & (\mathrm{mod}\ n_k). \end{array}\right\} \tag{15}$$

Tvrzení 1.4.2

Řešení soustavy konruenčních rovnic 1. stupně (15) lze vždy hledat ve tvaru

$$x \equiv d \pmod{n(n_1, n_2, \ldots, n_k)},$$

kde $n(n_1, n_2, \ldots, n_k)$ je nejmenší společný násobek čísel $n_1, n_2, \ldots, n_k$.

Důkaz tohoto tvrzení lze nalézt např. v [8].

Zajímavým poznatkem z teorie čísel je následující věta 1.4.3, která se využívá např. v algoritmech pro zpracování velkých čísel.

Věta 1.4.3 (čínská věta o zbytcích)

Nechť $n_1, n_2, \ldots, n_k$ jsou po dvou nesoudělná přirozená čísla a $c_1, c_2, \ldots, c_k$ libovolná k-tice celých čísel. Pak je soustava lineárních rovnic (15) řešitelná a její řešení lze nalézt v modulu $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Důkaz této věty lze nalézt např. v [6].

Příklad 23

V oboru celých čísel řešte následující soustavu kongruenčních rovnic

$$x \equiv 3 \pmod{9},$$
$$x \equiv 6 \pmod{15}.$$

Řešení. Nejprve podle tvrzení 1.4.2 zjistíme, v jakém modulu máme hledat výslednou neznámou x. Jelikož $n(9, 15) = 45$, budeme hledat řešení dané soustavy rovnic v modulo 45. Dále z první rovnice dostáváme $x = 3 + 9k$, kde $k \in \mathbb{Z}$. Dosazením do druhé rovnice dostáváme

$$3 + 9k \equiv 6 \pmod{15}.$$

Nyní využijeme vztah (6) z části 1.1

$$9k \equiv 3 \pmod{15}.$$

Dostali jsme kongruenční rovnici 1. stupně, kde neznámou je k. Konkrétně se jedná o případ 2(ii) z věty 1.3.5, neboť $D(9, 15) = 3$ a $3 \mid 3$. Řešíme ji podobně jako příklad 18

$$9k \equiv 3 \pmod{15},$$
$$3k \equiv 1 \pmod{5}.$$

Následně podle vztahu (8) z části 1.1 upravíme rovnici do následujícího tvaru a vyřešíme jako případ 1 z věty 1.3.5

$$3k \equiv 6 \pmod{5},$$
$$k \equiv 2 \pmod{5}.$$

Což se dá přepsat ve tvaru $k = 2 + 5p$, kde $p \in \mathbb{Z}$. Po dosazení k do x získáme $x = 21 + 45p$. Jinak zápsano

$$x \equiv 21 \pmod{45}.$$

Závěr. Řešení dané soustavy kongruenčních rovnic je $x = 21 + 45p$, kde $p \in \mathbb{Z}$, což se dá zapsat $x \in \mathcal{Z}_{21}$ podle modulu 45. □

Příklad 24

V oboru celých čísel řešte následující soustavu kongruenčních rovnic

$$\left.\begin{aligned} x &\equiv 1 \pmod{2}, \\ x &\equiv 0 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 4 \pmod{7}. \end{aligned}\right\} \tag{16}$$

Řešení. Předně si uvědomme, že čísla $2, 3, 5$ a 7 jsou po dvou nesoudělná čísla. Podle čínské věty o zbytcích (věta 1.4.3) je soustava kongruenčních rovnic (16) řešitelná a řešení lze nalézt v modulu $210 = 2 \cdot 3 \cdot 5 \cdot 7$. První rovnici soustavy (16) můžeme zapsat ve tvaru $x = 1 + 2p$, kde $p \in \mathbb{Z}$. Dosazením x do druhé rovnice získáme

$$1 + 2p \equiv 0 \pmod{3}.$$

Využitím vztahu (6) a (8) z části 1.1 získáme kongruenční rovnici 1. stupně a řešíme ji podobně jako případ 1 z věty 1.3.5, neboť $D(2, 3) = 1$

$$\begin{aligned} 2p &\equiv -1 \pmod{3}, \\ 2p &\equiv \ \ 2 \pmod{3}, \\ p &\equiv \ \ 1 \pmod{3}. \end{aligned}$$

Jinak zapsáno $p = 1 + 3q$, kde $q \in \mathbb{Z}$. Po dosazení p za x dostaneme $x = 3 + 6q$. Opět dosadíme x do třetí rovnice

$$3 + 6q \equiv 3 \pmod{5}.$$

Nyní využijeme vztah (6) z části 1.1

$$6q \equiv 0 \pmod 5.$$

Dostali jsme kongruenční rovnici 1. stupně, kde neznámou je q. Podle vztahu (8) z části 1.1 upravíme rovnici do následujícího tvaru a řešíme ji podobně jako případ 1 z věty 1.3.5, neboť $D(6,5) = 1$

$$\begin{aligned} 6q &\equiv 0 \pmod 5, \\ q &\equiv 0 \pmod 5. \end{aligned}$$

Získali jsme tak rovnost $q = 5r$, kde $r \in \mathbb{Z}$. Dosazením q za x dostáváme $x = 3 + 30r$. Opět dosadíme za x do poslední rovnice soustavy (16)

$$3 + 30r \equiv 4 \pmod 7.$$

Nyní využijeme vztah (6) z části 1.1

$$30r \equiv 1 \pmod 7.$$

Dostali jsme kongruenční rovnici 1. stupně, kde neznámou je r. Konkrétně se jedná o případ 1 z věty 1.3.5, neboť $D(30,7) = 1$

$$\begin{aligned} 30r &\equiv 120 \pmod 7, \\ r &\equiv 4 \pmod 7. \end{aligned}$$

Získali jsme tak rovnost $r = 4 + 7s$, kde $s \in \mathbb{Z}$. Dosazením r za x dostáváme $x = 123 + 210s$.

Závěr. Řešení dané soustavy kongruenčních rovnic je $x = 123 + 210s$, kde $s \in \mathbb{Z}$, což se dá zapsat $x \in \mathcal{Z}_{123}$ podle modulu 210. □

Nyní máme vše potřebné k tomu, abychom mohli vyřešit (*motivační*) *úlohu* z části 1.1.

Řešení úlohy ze strany 7. Zadání úlohy si nejdříve zapíšeme ve tvaru následující soustavy kongruenčních rovnic 1. stupně

$$\left.\begin{aligned} x &\equiv 1 \pmod 2,\\ x &\equiv 2 \pmod 3,\\ x &\equiv 3 \pmod 4,\\ x &\equiv 4 \pmod 5,\\ x &\equiv 5 \pmod 6,\\ x &\equiv 0 \pmod 7. \end{aligned}\right\} \tag{17}$$

Nejprve podle tvrzení 1.4.2 zjistíme v jakém modulu máme hledat výslednou neznámou x. Jelikož $n(2,3,4,5,6,7) = 420$, budeme hledat řešení dané soustavy rovnic podle modulu 420. První rovnici soustavy (17) můžeme zapsat ve tvaru $x = 1 + 2p$, kde $p \in \mathbb{Z}$. Dosazením x do druhé rovnice dostaneme kongruenční rovnici

$$1 + 2p \equiv 2 \pmod 3.$$

Využitím vztahů (6) a (8) z části 1.1 získáme kongruenční rovnici 1. stupně a řešíme ji podobně jako případ 1 z věty 1.3.5, neboť $D(2,3) = 1$

$$\begin{aligned} 2p &\equiv 1 \pmod 3,\\ 2p &\equiv 4 \pmod 3,\\ p &\equiv 2 \pmod 3. \end{aligned}$$

Jinak zapsáno $p = 2 + 3q$, kde $q \in \mathbb{Z}$. Po dosazení p za x dostaneme $x = 5 + 6q$. Dále opět dosadíme x do třetí rovnice

$$5 + 6q \equiv 3 \pmod 4.$$

Nyní využijeme vztah (6) z části 1.1

$$6q \equiv -2 \pmod 4.$$

Dostali jsme tak kongruenční rovnici 1. stupně, kde neznámou je q. Konkrétně se jedná o případ 2(ii) z věty 1.3.5, neboť $D(6,4) = 2$ a $2 \mid (-2)$. Řešíme ji podobně jako příklad 18

$$\begin{aligned} 6q &\equiv -2 \pmod 4,\\ 3q &\equiv -1 \pmod 2. \end{aligned}$$

Následně dle vztahu (8) z části 1.1 upravíme rovnici $3q \equiv -1 \pmod 2$ do následujícího tvaru a řešíme ji podobně jako případ 1 z věty 1.3.5, tj.

$$3q \equiv 3 \pmod 2,$$
$$q \equiv 1 \pmod 2.$$

Získali jsme tím rovnost $q = 1 + 2r$, kde $r \in \mathbb{Z}$. Dosazením q za x dostáváme $x = 11 + 12r$. Opět dosadíme za x do čtvrté rovnice soustavy (17)

$$11 + 12r \equiv 4 \pmod 5.$$

Nyní využijeme vztah (6) z části 1.1

$$12r \equiv -7 \pmod 5.$$

Dostali jsme kongruenční rovnici 1. stupně, kde neznámou je r. Konkrétně se jedná o případ 1 z věty 1.3.5, neboť $D(12, 5) = 1$

$$12r \equiv 48 \pmod 5,$$
$$r \equiv 4 \pmod 5.$$

Získali jsme tak rovnost $r = 4 + 5s$, kde $s \in \mathbb{Z}$. Dosazením r za x dostáváme $x = 59 + 60s$. Opětovným dosazením za x do páté rovnice soustavy (17) získáme

$$59 + 60s \equiv 5 \pmod 6.$$

Použitím vztahu (8) z části 1.1 dostáveme kongruenční rovnici $60s \equiv 60 \pmod 6$, která je splněna pro každé $s \in \mathbb{Z}$. Nyní stačí dosadit za x do poslední rovnice soustavy (17)

$$59 + 60s \equiv 0 \pmod 7.$$

Použitím vztahu (8) z části 1.1 dostáváme kongruenční rovnici 1. stupně, kde neznámou je s

$$60s \equiv 60 \pmod 7.$$

Konkrétně se jedná o případ 1 z věty 1.3.5, neboť $D(60, 7) = 1$

$$60s \equiv 60 \pmod 7,$$
$$s \equiv 1 \pmod 7.$$

Získali jsme tak rovnost $s = 1 + 7t$, kde $t \in \mathbb{Z}$. Dosazením s za x dostáváme

$$x = 119 + 420t.$$

Závěr. Nejmenší možný počet žáků, kteří jsou nastoupeni v tělocvičně je 119. □

Podobně lze řešit následující příklady.

Příklad 25

V oboru celých čísel řešte následující soustavu rovnic

$$\begin{aligned} x &\equiv 4 \pmod 7, \\ x &\equiv 2 \pmod 8, \\ x &\equiv -1 \pmod 9. \end{aligned}$$

$[x \equiv 242 \pmod{504}]$

Příklad 26

První trolejbus vyjíždí z depa v 8:00 a jeho okružní trať trvá 30 minut. Druhý trolejbus vyjíždí z depa o pět minut dříve než první a jeho okružní trať trvá 35 minut. Třetí trolejbus vyjíždí z depa v 8:10 a jeho okružní trasa trvá 40 minut. Kdy nejdříve se sjedou všechny tři trolejbusy v depu současně? [15:30]

Nápověda. Zadání úlohy lze přepsat do tvaru soustavy kongruenčních rovnic

$$\begin{aligned} x &\equiv 0 \pmod{30}, \\ x &\equiv -5 \pmod{35}, \\ x &\equiv 10 \pmod{40}. \end{aligned}$$

2 Číselné funkce

V této části představíme několik základních funkcí týkajících se teorie čísel. Zejména se jedná především o Eulerovu funkci, která je důležitá při řešení kongruenčních rovnic 1. stupně popsaných v části 1.3.

2.1 Základní pojmy

Pro uvedení do poznatků teorie čísel uvedeme následující definice a věty.

Definice 2.1.1

Přirozené číslo $n \in \mathbb{N}$ nazveme *prvočíslo*, právě když má právě dva navzájem různé dělitele a to 1 a n.

Poznámka. Číslo 1 tedy není prvočíslem.

Hledáním prvočísel se zabývali lidé již ve starověkém Řecku. Eratosthenés vypracoval jednoduchou metodu pro hledání prvočísel v řadě přirozených čísel, zvanou *Eratosthenovo síto*. Eratosthenés postupně bral všechna čísla a z posloupnosti všech přirozených čísel vyjmul všechny jejich násobky. Čísla, která mu na závěr zůstala, byla tak prvočísla. Pro hledání prvočísel platí následující věta.

Věta 2.1.2

Nechť $n \in \mathbb{N}$. Číslo n je složené, právě když je dělitelné některým prvočíslem $p \leq \sqrt{n}$.

Důkaz. Pokud číslo n je složené, pak má aspoň dva dělitele různé od 1 a n. Označme je x a y, tedy $n = x \cdot y$. Bez újmy na obecnosti můžeme předpokládat, že $x \leq y$, pak $n = x \cdot y \geq x^2$. Dostáváme tedy $x \leq \sqrt{n}$. □

Poznámka. Pro rozhodnutí, zda je číslo $n \in \mathbb{N}$ prvočíslem, stačí zjistit dělitelnost pouze prvočísly, která jsou menší nebo rovna číslu $\sqrt{n}$.

Definice 2.1.3

Zápis čísla $n \in \mathbb{N}$ ve tvaru

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},$$

kde čísla $p_1, p_2, \ldots, p_k$ jsou navzájem různá prvočísla a čísla $\alpha_1, \alpha_2, \ldots, \alpha_k$ jsou přirozená čísla, nazýváme *rozklad čísla n na prvočísla* (kanonický rozklad čísla n).

Otázku, zda je prvočísel konečně mnoho či nekonenčně mnoho, vyřešil rovněž ve starověku *Eukleides*.

Věta 2.1.4

Prvočísel je nekonečně mnoho.

Důkaz. Důkaz budeme provádět sporem, tedy, že prvočísel je konečně mnoho. Nechť $p_1, \ldots, p_n$ jsou všechna prvočísla. Uvažujme číslo $n = p_1 \cdot \ldots \cdot p_n + 1$, které je evidentně větší než jakékoliv prvočíslo $p_1, \ldots, p_n$. Kdyby toto číslo nebylo prvočíslem, pak by muselo být dělitelné některým prvočíslem p_i, kde $i \in \{1, 2, \ldots, n\}$. Toto číslo n ovšem dává při dělení každým p_i zbytek 1, což je spor. Číslo n je tedy nutně dalším prvočíslem. Tuto úvahu lze přitom libovolně krát opakovat. □

2.2 Eulerova funkce

Nechť $n \in \mathbb{N}$. *Eulerova funce* $\varphi(n)$ udává počet přirozených čísel menších než číslo n, která jsou navíc s číslem n nesoudělná. Symbolicky zapsáno:

$$\varphi(n) = |\ \{a \in \mathbb{N} \mid 0 < a \leq n, D(a, n) = 1\}\ |$$

Věta 2.2.1

Nechť m, $n \in \mathbb{N}$, $D(m, n) = 1$. Pak

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Věta 2.2.2

Nechť $p \in \mathbb{N}$ je prvočíslo, α je libovolné přirozené číslo a navíc $\alpha \neq 1$. Pak

a) $\varphi(p) = p - 1$,

b) $\varphi(p^\alpha) = (p - 1) \cdot p^{\alpha - 1}$.

Důkazy vět (2.2.1 – 2.2.2) jsou snadné a lze je nalézt např. v [5].

Věta 2.2.3

Nechť $n \in \mathbb{N}$, jehož kanonický rozklad na prvočísla je ve tvaru $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Pak platí

$$\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}),$$

přičemž navíc

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1},$$

kde $i \in \{1, 2, \ldots, k\}$.

Důkaz. Všimněme si, že prvočísla $p_1, p_2, \ldots, p_k$ jsou po dvou vzájemně nesoudělná. Tudíž dle věty 2.2.1 platí

$$\varphi(p_1 \cdot p_2 \cdot \ldots \cdot p_k) = \varphi(p_1) \cdot \varphi(p_2) \cdot \ldots \cdot \varphi(p_k).$$

S použitím věty 2.2.2 máme dokázánu první část věty. Tedy

$$\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}).$$

Nyní nám stačí dokázat druhou část věty. Všimněme si, že přirozená čísla menší než $p_i^{\alpha_i}$, která jsou s číslem n soudělná, jsou právě $p_i, 2 \cdot p_i, \ldots, p_i^{\alpha_i} \cdot p_i$. Těchto přirozených čísel je právě $p_i^{\alpha_i - 1}$. □

Věta 2.2.4

Nechť $n \in \mathbb{N}$, které lze zapsat jako kanonický rozklad na prvočísla $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Důkaz. Tato věta je důsledkem věty 2.2.3, podle které platí $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ pro každé prvočíslo p_i. Tedy $\varphi(n)$ lze zapsat ve tvaru

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Vytknutím jednotlivých $p_i^{\alpha_i}$ získáme tvrzení dokazované věty

$$\varphi(n) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

□

Příklad 27

Vypočtěte hodnotu $\varphi(675)$.

Řešení. Tento příklad vyřešíme dvěma způsoby. První způsob bude pomocí věty 2.2.4 a druhý způsob řešení bude pomocí věty 2.2.1.

První způsob. Číslo 675 si nejprve rozložíme na prvočísla

$$675 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 3^3 \cdot 5^2.$$

Nyní využijeme věty 2.2.4 na výpočet $\varphi(675)$

$$\varphi(675) = 675 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 360.$$

Druhý způsob. Číslo 675 lze rozložit na součin $3^3 \cdot 5^2 = 27 \cdot 25$. Všimněme si, že $D(27, 25) = 1$, proto můžeme využít větu 2.2.1

$$\varphi(675) = \varphi(27) \cdot \varphi(25) = \varphi(3^3) \cdot \varphi(5^2).$$

Dále dle věty 2.2.2 platí $\varphi(3^3) = 2 \cdot 3^2 = 18$ a $\varphi(5^2) = 4 \cdot 5 = 20$. Proto můžeme psát

$$\varphi(675) = \varphi(3^3) \cdot \varphi(5^2) = 18 \cdot 20 = 360.$$

Oba dva způsoby řešení vedou ke stejnému výsledku a je zcela na čtenáři, který ze způsobů řešení bude využívat. □

Příklad 28

Dokažte, že pro každé $n \in \mathbb{N}$ platí $\varphi(8n + 4) = 2\varphi(2n + 1)$.

Řešení. Všimněme si, že $8n+4 = 4(2n+1)$, tedy $D(4, 2n+1) = 1$. Nyní využijeme větu 2.2.1

$$\varphi(8n + 4) = \varphi(4) \cdot \varphi(2n + 1).$$

Číslo 4 lze rozložit na prvočísla ve tvaru $4 = 2^2$. Podle věty 2.2.2 platí $\varphi(2^2) = 1 \cdot 2 = 2$. Proto můžeme psát

$$\varphi(8n + 4) = \varphi(4) \cdot \varphi(2n + 1) = 2\varphi(2n + 1).$$

Tím je důkaz uzavřen. □

Další příklady.

Příklad 29

Vypočtěte hodnotu $\varphi(6)$, $\varphi(14)$, $\varphi(17)$. [2, 6, 16]

Příklad 30

Pomocí věty 2.2.4 vypočtěte hodnotu $\varphi(810)$. [216]

Příklad 31

Dokažte, že pro každé $n \in \mathbb{N}$ platí $\varphi(18n) = 6\varphi(2n)$.

2.3 Využití funkce $\varphi(n)$ při řešení kongruenčních rovnic

V této části budeme zkoumat vztah mezi Eulerovou funkcí a kongruenčními rovnicemi 1. stupně. Jedná se o další možné řešení kongrunčních rovnic z části 1.3.

Věta 2.3.1 (Eulerova)

Nechť $a \in \mathbb{Z}$, $n \in \mathbb{N}$ a $D(a, n) = 1$. Pak

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

Důkaz této věty lze nalézt např. v [8].

Věta 2.3.2 (malá Fermatova)

Nechť $a \in \mathbb{Z}$, $p \in \mathbb{N}$ je prvočíslo a $D(a, p) = 1$. Pak

$$a^{p-1} \equiv 1 \pmod{p}. \tag{18}$$

Důkaz. Pokud je p prvočíslo, pak podle věty 2.2.2 $\varphi(p) = p - 1$. Tedy malá Fermatova věta je speciálním případem Eulerovy věty. □

Věta 2.3.3

Nechť $a \in \mathbb{Z}$, $p \in \mathbb{N}$ je prvočíslo. Pak

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

Důkaz. Pokud $p \mid a$, jsou obě strany kongruentní s 0 modulo p. Jinak tato věta přímo plyne z číselné kongruence (18) vynásobené číslem a. □

S Eulerovou funkcí a Eulerovou větou úzce souvisí pojem *řád čísla a* vzhledem k modulu n. Uvedeme jej v následující definici.

Definice 2.3.4

Nechť $a \in \mathbb{Z}$, $n \in \mathbb{N}$ a $D(a, n) = 1$. *Řádem čísla a vzhledem k modulu n* rozumíme nejmenší přirozené číslo m splňující podmínku

$$a^m \equiv 1 \pmod{n}.$$

Tuto definice lze nalézt např. v [5].

Příklad 32

Určete řád čísla 4 vzhledem k modulu 9.

Řešení. Podle definice 2.3.4 budeme hledat nejmenší přirozené číslo m, které splňuje $4^m \equiv 1 \pmod{9}$. Postupně proto probereme jednotlivá přirozená čísla. Platí

$$\begin{aligned} 4^1 = 4 &\not\equiv 1 \pmod{9}, \\ 4^2 = 16 \equiv 7 &\not\equiv 1 \pmod{9}, \\ 4^3 = 64 &\equiv 1 \pmod{9}. \end{aligned}$$

Z předchozího řádku plyne závěr.

Závěr. Řád čísla 4 vzhledem k modulu 9 je roven 3. □

Příklad 33

Určete řád čísla 2 vzhledem k modulu 5.

Řešení. Podle definice 2.3.4 hledáme nejmenší přirozené číslo m, které splňuje $2^m \equiv 1 \pmod 5$. Postupně proto probereme jednotlivá přirozená čísla. Platí

$$\begin{aligned} 2^1 = 2 &\not\equiv 1 \pmod 5, \\ 2^2 = 4 &\not\equiv 1 \pmod 5, \\ 2^3 = 8 \equiv 3 &\not\equiv 1 \pmod 5, \\ 2^4 = 16 &\equiv 1 \pmod 5. \end{aligned}$$

Z předchozího řádku plyne závěr.

Závěr. Řád čísla 2 vzhledem k modulu 5 je roven 4. □

Tvrzení 2.3.5

Nechť $ax \equiv b \pmod n$ je kongruenční rovnice 1. stupně. Pak ji lze přepsat do tvaru

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

Důkaz tohoto tvrzení lze najít např. v [8].

Příklad 34

Pomocí $\varphi(n)$ řešte v oboru celých čísel $2x \equiv 5 \pmod 7$.

Řešení. Pomocí tvrzení 2.3.5 si přepíšeme kongruenční rovnici $2x \equiv 5 \pmod 7$ do tvaru

$$x \equiv 2^{\varphi(7)-1} \cdot 5 \pmod 7. \tag{19}$$

Podle věty 2.2.2 platí $\varphi(7) = 6$, tedy můžeme psát

$$x \equiv 2^5 \cdot 5 \pmod 7. \tag{20}$$

Za použití vztahu (7) z části 1.1 upravíme rovnici (20) na tvar

$$x \equiv 2^5 \cdot 5 = 2^3 \cdot 4 \cdot 5 \equiv 1 \cdot 4 \cdot 5 \equiv 6 \pmod 7.$$

Závěr. Řešením kongruenční rovnice (19) je $x \equiv 6 \pmod 7$, jinak zapsáno $x \in \mathcal{Z}_6$ podle modulu 7. □

Příklad 35

Pomocí $\varphi(n)$ řešte v oboru celých čísel $11x \equiv 5 \pmod{15}$.

Řešení. Pomocí tvrzení 2.3.5 si přepíšeme kongruenční rovnici $11x \equiv 5 \pmod{15}$ do tvaru

$$x \equiv 11^{\varphi(15)-1} \cdot 5 \pmod{15}. \tag{21}$$

Podle věty 2.2.1 platí $\varphi(15) = \varphi(3) \cdot \varphi(5)$. Podle věty 2.2.2 dále platí $\varphi(3) = 2$ a $\varphi(5) = 4$. Můžeme tedy psát

$$x \equiv 11^7 \cdot 5 \pmod{15}. \tag{22}$$

Na základě vztahu (11) z části 1.1 dále platí

$$\begin{aligned} 11^1 &\equiv -4 \pmod{15}, \\ 11^2 &\equiv \ \ 1 \pmod{15}, \\ &\vdots \\ 11^7 &\equiv -4 \pmod{15}. \end{aligned}$$

Za použití vztahu (7) z části 1.1 upravíme rovnici (22) na tvar

$$x \equiv 11^7 \cdot 20 \equiv -4 \cdot 5 \equiv 10 \pmod{15}.$$

Závěr. Řešením kongruenční rovnice (21) je $x \equiv 10 \pmod{15}$, jinak zapsáno $x \in \mathcal{Z}_{10}$ podle modulu 15. □

Poznámka. Z uvedených příkladů (34, 35) lze vidět, že pro velké moduly Eulerova funkce nabývá velkých hodnot. Tato metoda tedy není pro velké moduly příliš efektivní.

Navazující úlohy.

Příklad 36

Určete řád čísla 3 vzhledem k modulu 7. [6]

Příklad 37

Pomocí $\varphi(n)$ řešte v oboru celých čísel $2x \equiv 1 \pmod{5}$. $[\mathcal{Z}_3]$

Příklad 38

Pomocí $\varphi(n)$ řešte v oboru celých čísel $6x \equiv 3 \pmod{11}$. $[\mathcal{Z}_6]$

2.4 Funkce $\sigma(n)$, $\tau(n)$ a $\pi(n)$

V teorii čísel se vyskytuje mnoho dalších funkcí než uvedená Eulerova funkce. V této části proto uvedeme některé významné funkce.

Nechť n je libovolné přirozené číslo. Funkci, která udává počet všech dělitelů čísla n, označujeme $\tau(n)$. Funkci, která udává součet všech dělitelů čísla n, označujeme $\sigma(n)$. Symbolicky zapsáno:

$$\tau(n) = |\{d \in \mathbb{N} \mid 0 < d \leq n,\, d \,|\, n\}|,$$

$$\sigma(n) = \sum d_i, \text{ kde } d_i \in \{d_i \in \mathbb{N} \mid 0 < d_i \leq n,\, d_i \,|\, n\}.$$

Věta 2.4.1

Nechť $n \in \mathbb{N}$ a $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ je kanonický rozklad čísla n. Pak

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1),$$

$$\sigma(n) = \frac{(p_1^{\alpha_1+1} - 1) \cdot (p_1^{\alpha_2+1} - 1) \cdot \ldots \cdot (p_k^{\alpha_k+1} - 1)}{(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)}.$$

Důkaz. Každý dělitel d čísla n lze zapsat ve tvaru $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, kde $0 \leq \beta_i \leq \alpha_i$. Pak lze napsat

$$\sigma(n) = \sum_{\beta_1,\ldots,\beta_k} p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k} = (1 + p_1 + \ldots + p_1^{\alpha_1}) \cdot \ldots \cdot (1 + p_k + \ldots + p_k^{\alpha_k}) =$$

$$= \frac{(p_1^{\alpha_1+1} - 1) \cdot \ldots \cdot (p_k^{\alpha_k+1} - 1)}{(p_1 - 1) \cdot \ldots \cdot (p_k - 1)}.$$

Číslo β_i lze vybrat právě $\alpha_i + 1$ způsoby. Tedy počet všech dělitelů čísla n je

$$(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

□

Příklad 39

Určete hodnoty $\tau(252)$ a $\sigma(252)$.

Řešení. Nejprve si číslo 252 rozložíme na prvočísla

$$252 = 2^2 \cdot 3^2 \cdot 7.$$

Podle věty 2.4.1 vypočteme jednotlivé funkce

$$\tau(252) = (2+1) \cdot (2+1) \cdot (1+1) = 18,$$

$$\sigma(252) = \frac{(2^3-1) \cdot (3^3-1) \cdot (7^2-1)}{(2-1) \cdot (3-1) \cdot (7-1)} = 728.$$

□

Poznámka. Všimněme si, že každé $n \in \mathbb{N}$ má aspoň dva dělitele, a to čísla 1 a n. Proto vždy platí nerovnost $\sigma(n) \geq n + 1$.

Pomocí funkce $\sigma(n)$ lze přirozená čísla roztřídit:

a) *deficitní čísla* - $\sigma(n) < 2n$, příkladem jsou všechna prvočísla,

b) *abundantní čísla* (nadbytečná čísla) - $\sigma(n) > 2n$, příkladem je číslo 975, které je nejmenší liché abundantní číslo,

c) *dokonalá čísla* (perfektní čísla) - $\sigma(n) = 2n$, číslo n je rovno součtu všech dělitelů čísla n různých od n.

Dokonalá čísla byla zkoumána již Pythagorejci, nejmenší dokonalé číslo je číslo 6. Dodnes je známo 48 dokonalých čísel. S dokonalými čísly se pojí následující věta.

Věta 2.4.2 (Eulerova)

Sudé číslo $n \in \mathbb{N}$ je dokonalé, právě když je ve tvaru

$$n = 2^{s-1} \cdot (2^s - 1),$$

kde $2^s - 1$ je *Mersenneovo prvočíslo.*

Dalším typem prvočísel jsou např. prvočísla ve tvaru $2^{2n} + 1$, které se nazývají *Fermatova prvočísla*.

S dokonalými čísly souvisí pojem spřátelená čísla.

Definice 2.4.3

Nechť $a, b \in \mathbb{N}$. Čísla a, b nazveme *spřátelená čísla*, pokud je součet dělitelů čísla a i b roven $a + b$. Symbolicky zapsáno:

$$\sigma(a) = \sigma(b) = a + b.$$

Spřátelená čísla znal již Pythagoras, konkrétně se jednalo o čísla 220 a 284. *Thabit*[3] vytvořil vzorec pro generování spřátelených čísel, popsaný v následující větě.

Věta 2.4.4 (Thabitův vzorec)

Pokud $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ a $r = 9 \cdot 2^{2n-1} - 1$ pro $n > 1$ jsou prvočísla, pak čísla $2^n \cdot p \cdot q$ a $2^n \cdot r$ jsou spřátelená.

Důkaz vět (2.4.2, 2.4.4) lze najít např. v [8].

Poslední uvedenou funkcí z teorie čísel je následující funkce $\pi(n)$.

Nechť $n \in \mathbb{N}$. Funkci, která udává počet prvočísel menších nebo rovných než číslo n, označujeme $\pi(n)$. Symbolicky pak:

$$\pi(n) = |\{p \in \mathbb{N} \mid 0 < p \leq n,\ p \text{ je prvočíslo}\}|.$$

Hadamard[4] v roce 1896 dokázal následující větu uvedenou např. v [8].

Věta 2.4.5 (zákon asymptotického rozdělení prvočísel)

Funkce $\pi(x)$ a $x/\ln(x)$ jsou asymptoticky ekvivalentní, tzn., že limita pro $x \to +\infty$ z podílu $\pi(x)$ a $x/\ln(x)$ je rovna 1.

Poznámka. Uvedená věta 2.4.5 uvádí odhad pro počet prvočísel menších nebo rovných číslu n.

[3] Thabit (826 – 901) – arabský matematik a astronom.

[4] Jacques Salomon Hadamard (1865 – 1963) – francouzský matematik.

Příklad 40

Odhadněte počet prvočísel menších nebo rovno číslu 1024.

Řešení. Pomocí věty 2.4.5 využijeme asymptotického odhadu funkční hodnoty $\pi(1024)$ funkční hodnotou $1024/\ln 1024$. Tedy $1024/\ln 1024 = 148$.

Závěr. Odhadovaný počet prvočísel menších nebo rovno číslu 1024 je roven 148. □

Navazující úlohy.

Příklad 41

Určete hodnoty $\tau(324)$ a $\sigma(324)$. [15, 847]

Příklad 42

Rozhodněte, zda je číslo 232 abundantní. [deficitní číslo]

Příklad 43

Odhadněte počet prvočísel menších nebo rovno číslu 235. [43]

3 Diofantovské rovnice

Řecký matematik *Diofantos* žijící v 3. století se zabýval řešením rovnic, v nichž připouštěl řešení pouze v oboru celých čísel. Na Diofantovu počest se těmto rovnicím říká *diofantovské* (*diofantické*) *rovnice*. Využití diofantovských rovnic lze nalézt například v řadě praktických úloh vedoucích k rovnicím, kde neceločíselná řešení nemusejí mít vždy konkrétní interpretaci.

3.1 Lineární diofantovské rovnice

Definice 3.1.1

Rovnice ve tvaru

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

kde $x_1, \ldots, x_n$ jsou neznámé, $a_1, \ldots, a_n, b \in \mathbb{Z}$ a zároveň $a_i \neq 0$ pro každé $i \in \{1, 2, \ldots, n\}$, se nazývá *lineární diofantovská* (*diofantická*) *rovnice*.

Definici 3.1.1 lze nalézt např. v [10].

Úmluva. Kvůli přehlednosti budeme značit neznámé ve tvaru $x, y, z, \ldots$ namísto $x_1, x_2, x_3, \ldots$

Poznámka. Všimněme si, že lineární diofantovské rovnice lze ekvivalentně přepsat do tvaru kongruenčních rovnic 1. stupně popsané v části 1.3. Příkladem může být lineární diofantovská rovnice o dvou neznámých $2x + 5y = 6$, kterou lze přepsat do tvaru $2x \equiv 6 \pmod 5$.

Věta 3.1.2

Lineární diofantovská rovnice $a_1x_1 + \ldots + a_nx_n = b$ je řešitelná, právě když $D(a_1, \ldots, a_n) \mid b$. Navíc řešení závisí na $n - 1$ nezávislých celočíselných parametrech.

Důkaz věty 3.1.2 lze nalézt např. v [8].

Příklad 44

V oboru celých čísel řešte diofantovskou rovnici $9x + 5y = 12$.

Řešení. Nejprve ověříme podle věty 3.1.2, zda daná diofantovská rovnice je řešitelná. $D(9, 5) = 1$ a $1 \mid 12$, tedy daná diofantovská rovnice má řešení a bude záviset na jednom celočíselném parametru. Dále si danou rovnici $9x + 5y = 12$ přepíšeme do tvaru kongruenční rovnice $9x \equiv 12 \pmod 5$, kterou řešíme na základě poznatků z části 1.3. Platí tak

$$\begin{aligned} 9x &\equiv 12 \pmod 5, \\ 9x &\equiv 27 \pmod 5, \\ x &\equiv 3 \pmod 5. \end{aligned}$$

Získali jsme tak rovnost $x = 3+5t$, kde $t \in \mathbb{Z}$. Dosazením x do rovnice $9x+5y = 12$ dostáváme

$$9(3 + 5t) + 5y = 12.$$

Úpravou získáme vztah

$$y = -3 - 9t.$$

Závěr. Řešením dané diofantovské rovnice jsou všechny uspořádané dvojice $(x, y) = (3 + 5t; -3 - 9t)$, kde $t \in \mathbb{Z}$. □

Příklad 45

V oboru celých čísel řešte diofantovskou rovnici $2x + 4y + 7z = 6$.

Řešení. Nejprve ověříme podle věty 3.1.2, zda je daná diofantovská rovnice řešitelná. $D(2, 4, 7) = 1$ a $1 \mid 6$, tedy daná diofantovská rovnice má řešení a bude záviset na dvou celočíselných parametrech. Dále si všimněme, že $D(2, 4) = 2$, tedy $7z \equiv 6 \pmod 2$. Tuto kongruenční rovnici řešíme na základě poznatků z části 1.3

$$\begin{aligned} 7z &\equiv 6 \pmod 2, \\ 7z &\equiv 14 \pmod 2, \\ z &\equiv 2 \pmod 2, \\ z &\equiv 0 \pmod 2. \end{aligned}$$

Získali jsme tak rovnost $z = 0 + 2t$, kde $t \in \mathbb{Z}$. Dosazením z do rovnice $2x + 4y + 7z = 6$ dostáváme

$$2x + 4y + 14t = 6.$$

Dále si danou diofantovskou rovnici $2x + 4y + 14t = 6$ přepíšeme do tvaru kongruenční rovnice $2x \equiv 6 - 14t \pmod 4$, kterou řešíme na základě poznatků z části 1.3

$$\begin{aligned} 2x &\equiv 6 - 14t \pmod 4, \\ x &\equiv 3 - 7t \pmod 2. \end{aligned}$$

Získali jsme tak rovnost $x = 3 - 7t + 2s$, kde $s \in \mathbb{Z}$. Dosazením x do rovnice $2x + 4y + 7z = 6$ dostáváme

$$2(3 - 7t + 2s) + 4y + 14t = 6.$$

Úpravou získáme vztah

$$y = -s.$$

Závěr. Řešením dané diofantovské rovnice jsou všechny uspořádané trojice čísel $(x, y, z) = (3 - 7t + 2s; -s; 2t)$, kde $t, s \in \mathbb{Z}$. □

Příklad 46

Jakých celočíselných hodnot mohou nabývat strany obdélníku o obvodu 12 cm?

Řešení. Zadání tohoto příkladu lze zapsat ve tvaru rovnice $2x + 2y = 12$. Opět ověříme podle věty 3.1.2, zda je daná diofantovská rovnice řešitelná. $D(2, 2) = 2$ a $2 \mid 12$, tedy daná diofantovská rovnice má řešení a bude záviset na jednom celočíselném parametru. Dále si danou diofantovskou rovnici $2x + 2y = 12$ přepíšeme do tvaru kongruenční rovnice $2x \equiv 12 \pmod 2$. Získali jsme identickou rovnici, která je podle malé Fermatovy věty (viz strana 34) splněna pro každé x z úplné

soustavy zbytků podle modulu 2. Tedy $x = 0 + 2t$ nebo $x = 1 + 2t$, kde $t \in \mathbb{Z}$. Mějme nejprve $x = 0 + 2t$. Dosazením x do rovnice $2x + 2y = 12$ dostáváme

$$4t + 2y = 12.$$

Úpravou získáme vztah

$$y = 6 - 2t.$$

Smysl dává pouze řešení, kde strany obdélníku jsou kladná celá čísla, proto získáváme nerovnosti $2t > 0$ a $6 - 2t > 0$. Z těchto dvou nerovností úpravou získáváme $0 < t < 3$. Strany obdélníku, za předpokladu, že $x = 0 + 2t$, kde $t \in \mathbb{Z}$, mohou nabývat hodnot ve tvaru uspořádaných dvojic $(x, y) \in \{(2; 4), (4; 2)\}$.

Nyní musíme vyřešit druhou možnost, tj. $x = 1 + 2t$, kde $t \in \mathbb{Z}$. Dosazením x do rovnice $2x + 2y = 12$ dostáváme

$$4t + 2 + 2y = 12.$$

Úpravou získáme vztah

$$y = 5 - 2t.$$

Smysl dává pouze řešení, kde strany obdélníku jsou kladná celá čísla, proto získáváme nerovnosti $1 + 2t > 0$ a $5 - 2t > 0$. Z těchto dvou nerovností úpravou získáváme $-\frac{1}{2} < t < \frac{5}{2}$. Strany obdélníku, za předpokladu, že $x = 1+2t$, kde $t \in \mathbb{Z}$, mohou nabývat hodnot ve tvaru uspořádaných dvojic $(x, y) \in \{(1; 5), (3; 3), (5; 1)\}$.

Závěr. Strany x, y obdélníku mohou nabývat hodnot ve tvaru uspořádaných dvojic $(x, y) \in \{(1; 5), (2; 4), (3; 3), (4; 2), (5; 1)\}$. □

Další příklady.

Příklad 47

V oboru celých čísel řešte diofantovskou rovnici $3x + 4y = 5$.

$$[(3 + 4t;\ -1 - 3t),\ t \in \mathbb{Z}]$$

Příklad 48

V oboru celých čísel řešte diofantovskou rovnici $2x + 6y + 9z = 10$.

$$[(5 - 9t + 3s;\ -s;\ 2t),\ t, s \in \mathbb{Z}]$$

Příklad 49

Jak je možné zaplatit 27 Kč pomocí mincí v hodnotě 2 Kč a 5 Kč?

$[(1;5), (6;3), (11;1)]$

3.2 Diofantovské rovnice řešené pomocí nerovností

Závěrem této práce, ve které jsme se zabývali dělitelností v oboru celých čísel, přidávám navíc část, která nesouvisí s číselnou dělitelností. V předchozí části jsme se zabývali lineárními diofantovskými rovnicemi. Ovšem někdy je potřeba řešit i složitější diofantovské rovnice, kde se na jedné straně rovnice vyskytují neznámé v jakýchkoliv mocninách a na straně druhé se může vyskytovat číslo celé či výraz vytvořený z určitých neznámých. V této části se zaměříme na metodu řešení diofantovských rovnic pomocí nerovností.

Příklad 50

V oboru celých čísel řešte diofantovskou rovnici $4x^2 + 5y^2 = 64$.

Řešení. Všimněme si, že pro libovolné $y \in \mathbb{Z}$ platí $y^2 \geq 0$, proto musí libovolné řešení dané rovnice splňovat

$$64 = 4x^2 + 5y^2 \geq 4x^2.$$

Z uvedené nerovnosti plyne $x^2 \leq 16$. Tedy $-4 \leq x \leq 4$, proto x^2 bude jedno z čísel $0, 1, 4, 9, 16$. Postupným dosazováním jednotlivých hodnot x^2 do rovnice $4x^2 + 5y^2 = 64$ získáme

$$\begin{aligned}
5y^2 &= 64 \quad \text{pro} \quad x^2 = \ \ 0,\\
5y^2 &= 60 \quad \text{pro} \quad x^2 = \ \ 1,\\
5y^2 &= 48 \quad \text{pro} \quad x^2 = \ \ 4,\\
5y^2 &= 28 \quad \text{pro} \quad x^2 = \ \ 9,\\
5y^2 &= \ \ 0 \quad \text{pro} \quad x^2 = 16.
\end{aligned}$$

Jelikož hledáme $y \in \mathbb{Z}$, vyhovuje pouze možnost pro $x^2 = 16$, kde $y = 0$ a $x = \pm 4$.

Závěr. Řešením dané diofantovské rovnice je uspořádáná dvojice $(x, y) \in \{(-4; 0), (4; 0)\}$. □

Příklad 51

V oboru přirozených čísel řešte diofantovskou rovnici $x + y + z = 6xyz$.

Řešení. Všimněme si, že neznámé x, y, z jsou zastoupeny v dané diofantovské rovnici symetricky, tudíž můžeme předpokládat $x \leq y \leq z$. Pak lze zapsat

$$6xyz = x + y + z \leq 3z.$$

Z uvedené nerovnosti plyne $xy \leq \frac{1}{2}$. Pro součin dvou libovolných přirozených čísel obecně platí nerovnost $xy \geq 1$. Z této nerovnosti plyne, že nerovnost $xy \leq \frac{1}{2}$ nemůže být splněna pro jakoukoliv dvojici přirozených čísel x, y.

Závěr. Daná diofantovská rovnice nemá řešení v oboru přirozených čísel. □

Příklad 52 (viz např. v [10])

V oboru celých čísel řešte diofantovskou rovnici $x^2 + xy + y^2 = x^2y^2$.

Řešení. Všimněme si, že neznámé x, y jsou zastoupeny v dané diofantovské rovnici symetricky, tudíž můžeme předpokládat $x^2 \leq y^2$ a tudíž platí $xy \leq y^2$. Nyní lze zapsat

$$x^2y^2 = x^2 + xy + y^2 \leq 3y^2.$$

Z uvedené nerovnosti plyne, že buď $y = 0$ nebo $x^2 \leq 3$. Tedy musíme rozebrat jednotlivé případy. Pokud $y = 0$, pak po dosazení do $x^2 + xy + y^2 = x^2y^2$, $x = 0$. Pokud $x^2 \leq 3$, pak postupným dosazováním jednotlivých hodnot x^2 do rovnice $x^2 + xy + y^2 = x^2y^2$ získáme

$$\begin{aligned} y &= 0 \text{ pro } x = 0, \\ y &= -1 \text{ pro } x = 1, \\ y &= 1 \text{ pro } x = -1. \end{aligned}$$

Závěr. Řešením dané diofantovské rovnice je uspořádáná dvojice $(x, y) \in \{(0; 0), (-1; 1), (1; -1)\}$. □

Další příklady.

Příklad 53

V oboru celých čísel řešte diofantovskou rovnici $5x^2 + 3y^2 = 82$. $[\emptyset]$

Příklad 54 (viz např. v [10])

V oboru přirozených čísel řešte diofantovskou rovnici $x + y + z = xyz$.

$[(1;2;3), (1;3;2), (2;1;3), (2;3;1), (3;1;2), (3;2;1)]$

Příklad 55

V oboru celých čísel řešte diofantovskou rovnici $x^2 + xy + y^2 = 3x^2y^2$.

$[(0;0), (1;1), (-1;-1)]$

Závěr

V bakalářské práci jsou shrnuty základní poznatky o dělitelnosti v oboru celých čísel. Zavedli jsme pojem číselná kongruence, na základě něhož jsme objasnili kritéria dělitelnosti čísly 3, 4, 7, 11 a 13. Dále jsou zde popsány kongruenční rovnice 1. stupně a jejich soustavy.

Ve druhé kapitole zabývající se číselnými funkcemi jsme zavedli Eulerovu funkci, která má zásadní význam při řešení kongruenčních rovnic. Zkoumali jsme zde také pojmy dokonalá a spřátelená čísla.

Třetí kapitola byla věnována diofantovským rovnicím a jejich řešením. Znalostí diofantovských rovnic žák střední školy získá způsobilost k řešení středoškolských úloh jinou a jistě netradiční cestou.

Celá bakalářská práce je koncipována tak, aby ji zvládl žák střední školy a mohl využít získané znalosti z této práce při řešení typových (i jiných) úloh uvedených na konci každé kapitoly. Ve středoškolské matematice se sice pojem číselná kongruence, jenž je stěžejní pro celou bakalářskou práci, běžně nevyskytuje, avšak znalost uvedeného pojmu žáka střední školy velmi obohacuje a umožňuje mu řešit řadu středoškolských úloh s hlubším porozuměním a často také mnohem rychleji.

Literatura

[1] Andreescu, T., Andrica, D.: *An Introduction to Diophantine Equations*. USA, 2002.

[2] Andreescu, T., Andrica, D.: *Number Theory* (*Structures, Examples and Problems*). USA, 2009.

[3] Apfelbeck, A.: *Kongruence*. ÚV MO v nakladatelství Mladá fronta, Praha, 1968.

[4] Botur, M.: *Úvod do aritmetiky*. VUP, Olomouc, 2011.

[5] Bulant, M.: *Algebra 2 - Teorie čísel* [online], [cit. 2015-03-25]. Dostupné na http://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-screen.pdf.

[6] Calábek, P.: *Čínská zbytková věta*. Matematika – fyzika – informatika, ročník 19, č. 8, str. 459 – 466.

[7] Dolinka, I.: *Elementarna teorija brojeva* (*moji omiljeni zadaci*). Društvo matematičara Srbije, Beograd, 2007.

[8] Halaš, R.: *Teorie čísel*. VUP, Olomouc, 2014, 2.vydání.

[9] Korec, I.: *Úlohy o veľkých číslach*. ÚV MO v nakladatelství Mladá fronta, Praha, 1988.

[10] Kučera, R., Herman, J., Šimša, J.: *Metody řešení matematických úloh* I. Masarykova univerzita, Brno, 2011, 3.vydání.

[11] Kučera, R., Herman, J., Šimša, J.: *Metody řešení matematických úloh* II. Masarykova univerzita, Brno, 1991.

[12] Marshall, D. C., Odell, E., Starbird, M.: *Number Theory Through Inquiry*. The Mathematical Association of America, USA, 2007.

[13] Mičić, V., Kadelburg, Z.: Uvod u teoriju brojeva. Materijali z mlade matematičave, sv. 15, Društvo matematičava SR Srbije, Beograd, 1989.

[14] Odvárko, O., Calda, E., Šedivý, J., Židek, S.: *Metody řešení matematických úloh*. Státní pedagogické nakladatelství, Praha, 1990.

[15] Sedláček, J.: *Co víme o přirozených číslech*. ÚV MO v nakladatelství Mladá fronta, Praha, 1965.

[16] Sierpiński, W.: *O rozwiazywaniu równań* (*W liczbach całkowitych*). Wydawnictwo naukowe PWN, Warszawa, 2009.

[17] Sierpiński, W.: *Biblioteczka matematyczna* (*200 zadań z elementarnej teorii liczb*). Państwowe zakłady wydawnictw szkolnych, Warszawa, 1964.

[18] Švrček, J.: *Gradované řetězce úloh v práci s matematickými talenty*. VUP, Olomouc, 2014.

[19] Švrček, J.: *Metody řešení soustav algebraických rovnic*. VUP, Olomouc, 2012.

[20] Veselý, F.: *O dělitelnosti čísel celých*. ÚV MO v nakladatelství Mladá fronta, Praha, 1966.

[21] Vinogradov, I. M.: Osnovy těorii čisel (rusky). Vyd. Nauka, Moskva, 1972.