

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta

SBÍRKA PŘÍKLADŮ Z OBECNÉ ALGEBRY

BAKALÁŘSKÁ PRÁCE

Martina Kukačková

České Budějovice, prosinec 2007

Prohlašuji, že jsem bakalářskou práci zpracovala samostatně a použitou literaturu jsem citovala.

Děkuji vedoucímu této bakalářské práce, kterým byl doc. RNDr. Pavel Tlustý, CSc, za dohled, pomoc a konzultaci při jejím vzniku a zpracování.

Prohlašuji, že v souladu s § 476 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce (a to v nezkrácené podobě) pedagogickou fakultou, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejich internetových stránkách.

V Českých Budějovicích 04.12.2007

Martina Kukačková

Anotace

Cílem práce je vytvořit učební pomůcku použitelnou pro studenty předmětu Algebra III na pedagogické fakultě v Českých Budějovicích.

Obsahem tohoto předmětu je zopakování základních znalostí v oblasti dělitelnosti, prvočísel a nalezení efektivnějších metod výpočtů za pomoci několika významných matematických vět.

Měl by poskytnout zejména studentům kombinovaného studia dostatečné množství látky sloužící k pochopení, osvojení a procvičení studované problematiky.

Annotation

The aim of this work is to create a teaching aid suitable for students of the Algebra III subject at the Pedagogical Faculty of the University of South Bohemia in České Budějovice.

The content of this subject is focused on repeating the basic knowledges in the area of divisibility, prime numbers and finding more effective calculation methods with the help of several important mathematical sentences.

The subject should provide primarily students of combined studies with sufficient knowledge to be able to understand, master and practice the studied area.

Obsah

1. Čísla	6
2. Dělitelnost v oboru celých čísel	9
2.1. Největší společný dělitel	12
2.2. Nejmenší společný násobek	12
3. Eukleidův algoritmus	15
4. Prvočísla	17
5. Erathostenovo síto	21
6. Kritéria dělitelnosti v desítkové číselné soustavě	22
7. Vyjádření čísla v číselné soustavě o základu z	26
7.1. Sčítání soustav o základu vyšším než $z = 10$	28
7.2. Násobení soustav o základu různém od $z = 10$	28
8. Užití dělitelnosti, kongruence	30
9. Eulerova věta	38
9.1. Eulerova věta	39
10. Malá Fermatova věta	41
11. Wilsonova věta	43
12. Lineární neurčité (Diofantské) rovnice	44
 Použitá literatura	 49

Úvod

Začátek této bakalářské práce je záměrně poněkud pozvolnější. V celé první kapitole se věnuji číslům, jejich zvláštnostem a zákonitostem, které nám většinou unikají. Jejich výčet zdaleka není konečný a pro pokračování práce nejsou nezbytná, nicméně podle mého jsou velice zajímavá.

Ve druhé a třetí kapitole si nejdříve zopakujeme znalosti týkající se dělitelnosti čísel a naučíme se použití Euklidova algoritmu.

Čtvrtá a pátá kapitola je věnována prvočíslům, jejich vlastnostem a dále se seznámíme s algoritmem zvaným Erathostenovo síto, který slouží k nalezení prvočísel.

V šesté kapitole si zopakujeme kritéria dělitelnosti v desítkové soustavě a ukážeme si několik jejich praktických využití.

Sedmá kapitola nám připomene jak převody čísel mezi soustavami o základu z tak i sčítání a násobení v těchto soustavách.

Od sedmé do desáté kapitoly se budeme věnovat užití dělitelnosti, seznámíme se s pojmem kongruence a naučíme se věty několika Velkých matematiků, které nám odhalí další zákonitosti v užití čísel a umožní snazší výpočet kongruencí.

Poslední kapitola se zabývá lineárními neurčitými (Diofantskými) rovnicemi o dvou neznámých, naučíme se zde postup jejich výpočtu a použití těchto výpočtů v běžném životě.

1. Číslo

- **Abundantní** číslo je takové číslo n , pro které platí $\sigma(n) > 2n$, $\sigma(n)$ je součet všech kladných dělitelů čísla n . Hodnota $\sigma(n) - 2n$ se nazývá abundance čísla n .

Příklad: 12 má součet dělitelů $1 + 2 + 3 + 4 + 6 + 12 = 28$, $28 > 2 \cdot 12$.

Jeho abundance je $28 - 2 \cdot 12 = 4$.

- **Automorfní** číslo je číslo, jehož každá mocnina končí tímto číslem.

Příklad: 5, 6, 76... .

- **Cyklické** číslo je číslo, které při násobení každým číslem od 1 do počtu jeho číslic dává číslo, které vznikne cyklickou záměnou jeho číslic.

Příklad: 142 857... .

$$1 \cdot 142\,857 = 142\,857$$

$$2 \cdot 142\,857 = 285\,714$$

$$3 \cdot 142\,857 = 428\,571$$

$$4 \cdot 142\,857 = 571\,428$$

$$5 \cdot 142\,857 = 714\,285$$

$$6 \cdot 142\,857 = 857\,142$$

- **Deficientní** číslo je takové číslo, které je větší než součet jeho vlastních dělitelů.

Příklad: nejmenším deficientním číslem je číslo 2

- **Dokonalé** číslo je takové přirozené číslo, které se rovná součtu všech svých dělitelů mimo sebe sama.

Příklad: nejmenším dokonalým číslem je 6, součet jeho dělitelů je $1 + 2 + 3 = 6$.

Jiným známým dokonalým číslem je 28, v současné době je známo 30 dokonalých čísel, poslední číslo vypočetli v Houstonu a má 130 099 číslic.

- **Fibonacci** čísla tvoří posloupnost čísel 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89... . kde každé číslo (kromě prvních dvou) je součtem dvou předcházejících.

Fibonacciho čísla se vyskytují v přírodě, například listy na stoncích rostlin bývají uspořádány tak, že spirálovitě stoupají, přičemž počet listů mezi dvěma listy, které vyrůstají přesně nad sebou, je roven některému Fibonacciovu číslu.

- **Iracionální** číslo je číslo, které nelze vyjádřit jako podíl dvou celých čísel. Desetinný rozvoj těchto čísel je nekonečný a neperiodický.

Příklad: $\sqrt{2}$, π ...

- **Magické** číslo je číslo, které je zároveň číslem **abundantním** a není součtem některých svých dělitelů.

Příklad: nejmenší magické číslo je 70...má dělitele 1, 2, 5, 7, 10, 14, 35, 70, jejich součet je 144, jde tedy o abundantní číslo. Žádná kombinace dělitelů však nedává součet 70, takže je to číslo magické.

Ověřte, že čísla 836, 4 030, 5 830, 7 192, 9 272 jsou magická.

- **Palindromické** číslo je číslo, které se nezmění, napíše-li se pozpátku

Příklad: 11, 111, 12 321, 2 867 682...

Vezmeme - li jakékoli číslo, přičteme k němu jeho zrcadlový obraz, totéž uděláme s výsledkem atd., dostaneme dříve-či později palindromické číslo.

$18 + 81 = 99$; $68 + 86 = 154$, $154 + 451 = 605$, $605 + 506 = 1\,111$.

Z čísel menších než 100 potřebujeme nejvíce kroků u 89, kde až po 24 krocích dostaneme palindromické číslo 8 813 200 023 188, **ověřte správnost výpočtu.**

- **Polygonální** číslo je číslo, které dostaneme jako počet bodů, jež tvoří pravidelné schéma tvaru mnohoúhelníka. Nejjednodušší polygonální čísla jsou *trojúhelníková čísla* 1, 3, 6, 10, 15, 21... , která dostáváme jako počty bodů ve schématech tvaru pravidelného trojúhelníka:

```

      *
    *
  *
*

```

atd.

Z podobně utvořených pětiúhelníků dostaneme čísla 1, 5, 12, 22, 35... ,

šestiúhelníková čísla 1, 6, 15, 28, 45... .

Jinak dostaneme trojúhelníková čísla postupným sčítáním čísel 1, 2, 3, 4, 5... ,

pětiúhelníková čísla sčítáním čísel 1, 4, 7, 10, 13... (ob tři čísla), šestiúhelníková

čísla sčítáním čísel 1, 5, 9, 13, 17... (ob čtyři čísla).

- **Pospolitá** čísla tvoří uzavřený řetězec čísel, v němž každé číslo je součtem všech dělitelů čísla předcházejícího (vyjma čísla samého).

Příklad: součet dělitelů čísla **12 496** je $1 + 2 + 4 + 8 + 11 + 16 + 22 + 44 + 71 +$

$+ 88 + 142 + 176 + 284 + 568 + 781 + 1136 + 1562 + 3124 + 6248 = 14\,288$,

součet dělitelů 14 288 je $1 + 2 + 4 + 8 + 16 + 19 + 38 + 47 + 76 + 94 + 152 + 188 +$

$+ 304 + 376 + 752 + 893 + 1786 + 3572 + 7144 = 15\,472$,

součet dělitelů 15 472 je $1 + 2 + 4 + 8 + 16 + 967 + 1934 + 3868 + 7736 = 14\,536$,

součet dělitelů 14 536 je $1 + 2 + 4 + 8 + 23 + 46 + 79 + 92 + 158 + 184 + 316 +$

$+ 632 + 1817 + 3634 + 7268 = 14\,264$,

a součet dělitelů 14 264 je $1 + 2 + 4 + 8 + 1783 + 3566 + 7132 = \mathbf{12\,496}$.

Tato čísla tvoří pětici pospolitých čísel.

- **Repunit** je číslo složené ze samých jedniček, tj. 11, 111, 1 111... .

Příklad: $11^2 = 121$, $111^2 = 12\,321$, $1\,111^2 = 1\,234\,321$ atd.

- **Spřátelená** čísla se nazývají taková dvě různá přirozená čísla a , b , jejichž součet všech vlastních dělitelů čísla a se rovná číslu b a naopak.

Příklad: 220 a 284

součet dělitelů čísla **220** = $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = \mathbf{284}$

součet dělitelů čísla **284** = $1 + 2 + 4 + 71 + 142 = \mathbf{220}$

2. Dělitelnost v oboru celých čísel

Definice 2. 1:

V oboru $\mathbb{Z}$ pro libovolnou dvojici celých čísel $a, b \neq 0$ definujeme:

Číslo a je dělitelné číslem b , jestliže existuje takové číslo c , pro které platí $a = bc$, tj. když číslo a je násobkem čísla b a píšeme $b \mid a$.

Jestliže platí $a \neq bc$, pak není číslo a dělitelem čísla b a číslo b není násobkem čísla a . Můžeme také říci, že číslo b není dělitelné číslem a nebo že číslo a nedělí číslo b . Píšeme $a \nmid b$.

Př. 2. 1:

Na základě uvedené definice můžeme říci, že číslo 3 je dělitelem čísla 12, nebo že číslo 12 je násobkem čísla 3, nebo že číslo 12 je dělitelné číslem 3, nebo že číslo 3 dělí číslo 12. Všechny čtyři formulace jsou ekvivalentní, tj. existuje takové celé číslo c , pro které platí $3c = 12$. Skutečnost, že číslo 3 je dělitelem čísla 12, zapisujeme $3 \mid 12$.

Naproti tomu číslo 5 není dělitelem čísla 12, číslo 12 není násobkem čísla 5, číslo 12 není dělitelné číslem 5 a číslo 5 nedělí číslo 12, neboť pro každé celé číslo c platí $5c \neq 12$. Zapišeme $5 \nmid 12$.

Definice 2. 2:

Je-li $a = 0$ a b libovolné celé číslo, je $a = bc$ pro $c = 0$. To znamená, že číslo 0 je násobkem kteréhokoli celého čísla. Je-li $b = 0$, pak $bc = 0$, takže číslo 0 je dělitelem jediného celého čísla, a to 0.

Je-li a libovolné celé číslo a $b = 1$, je $a = bc$ pro $c = a$. Proto číslo 1 (-1) je dělitelem kteréhokoli celého čísla. Je-li $a = 1$, pak rovnost $a = bc$ lze splnit jen pro $b = 1, c = 1$ ($b = -1, c = -1$). Proto číslo 1 (-1) je násobkem pouze čísel 1 (-1). Je-li $a = b$, pak rovnost $a = bc$ platí jen pro $c = 1$, takže každé celé číslo je dělitelné samo sebou (a číslem k sobě opačným).

Pro libovolná čísla a, b, c platí:

$$(a \mid b \wedge b \mid c) \Rightarrow a \mid c$$

$$(a \mid b \wedge a \mid c) \Rightarrow a \mid (b + c) \wedge a \mid (b - c)$$

$$c \neq 0 \Rightarrow (a \mid b \Leftrightarrow ac \mid bc)$$

$$(a \mid b \wedge b > 0) \Rightarrow a \leq b$$

Věta 2. 1:

Věta o dělení celých čísel se zbytkem.

Pro libovolně zvolená čísla $a \in \mathbb{Z}, b \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}, r \in \{0, 1, \dots, b - 1\}$ tak, že $a = qb + r$.

Důkaz:

Dokažme nejprve existenci čísel q, r . Předpokládejme, že přirozené číslo b je dáno pevně a dokažme větu pro libovolné $a \in \mathbb{Z}$.

Nejprve budeme předpokládat, že $a \in \mathbb{N}_0$ a existenci čísel q, r dokážeme indukcí:

Je-li $0 \leq a < b$, stačí volit $q = 0, r = a$ a rovnost $a = qb + r$ platí.

Předpokládejme nyní, že $a \geq b$ a že jsme existenci čísel q, r dokázali pro všechna $a' \in \{0, 1, 2, \dots, a - 1\}$. Speciálně pro $a' = a - b$ tedy existují q', r' tak, že:

$$a' = q'b + r' \text{ a přitom } r' \in \{0, 1, \dots, b - 1\}.$$

Zvolíme-li $q = q' + 1, r = r'$, platí:

$$a = a' + b = (q'b + r') + b = ((q - 1) \cdot b + r') + b = qb + r,$$

což jsme chtěli dokázat.

Existenci čísel q, r jsme tedy dokázali pro libovolné $a \geq 0$. Je-li naopak $a < 0$, pak ke každému číslu $-a$ podle výše dokázaného existují $q \in \mathbb{Z}, r \in \{0, 1, \dots, b-1\}$ tak, že:

$$-a = q'b + r', \text{ tedy } a = -q'b - r'.$$

Je-li $r' = 0$, položíme $r = 0, q = -q'$; je-li $r' > 0$, položíme $r = b - r', q = -q' - 1$. V obou případech $a = qb + r$, a tedy čísla q, r s požadovanými vlastnostmi existují pro každé $a \in \mathbb{Z}, b \in \mathbb{N}$.

Nyní dokážeme jednoznačnost.

Předpokládejme, že pro některá čísla $q_1, q_2 \in \mathbb{Z}; r_1, r_2 \in \{0, 1, \dots, b-1\}$ platí:

$$a = q_1 b + r_1 = q_2 b + r_2.$$

Úpravou dostaneme $r_1 - r_2 = (q_2 - q_1)b$, a tedy $b \mid r_1 - r_2$. Ovšem z $0 \leq r_1 < b, 0 \leq r_2 < b$ plyne $-b < r_1 - r_2 < b$, odkud plyne $r_1 - r_2 = 0$. Pak ale i $(q_2 - q_1)b = 0$, a proto $q_1 = q_2, r_1 = r_2$.

Čísla q, r jsou tedy určena jednoznačně. Tím je důkaz ukončen.

Číslo q , resp. r z věty se nazývá (neúplný) podíl, resp. zbytek při dělení čísla a číslem b se zbytkem.

Je vhodné též si uvědomit, že číslo b dělí číslo a , právě když zbytek r je roven nule.

Př. 2. 2:

Dokažte, že jsou-li zbytky po dělení čísel $a, b \in \mathbb{Z}$ číslem $m \in \mathbb{N}$ jedna, je jedna i zbytek po dělení čísla ab číslem m .

Řešení:

Pro libovolné $a, b \in \mathbb{Z}$ existují $s, t \in \mathbb{Z}$ tak, že $a = sm + 1, b = tm + 1$.

Vynásobením dostaneme vyjádření:

$ab = (sm + 1)(tm + 1) = (stm + s + t)m + 1 = qm + r$, kde $q = stm + s + t, r = 1$, které je zřejmě jednoznačné, a tedy zbytek po dělení čísla ab číslem m je jedna.

2. 1 Největší společný dělitel:

Společným dělitelem čísel $n_1, n_2, \dots, n_k \in \mathbb{N}$ nazveme takové přirozené číslo, jež je dělitelem každého z nich. Ten ze společných dělitelů, který je větší než všichni ostatní dělitelé, se nazývá největším společným dělitelem NSD, značíme $D(n_1, n_2, \dots, n_k)$.

Př. 2. 3:

Určete $D(1\,284, 144)$.

$$1\,284 = 2 \cdot 642 = 2 \cdot 2 \cdot 321 = 2 \cdot 2 \cdot 3 \cdot 107 = 2^2 \cdot 3 \cdot 107.$$

$$144 = 2 \cdot 72 = 2 \cdot 2 \cdot 36 = 2 \cdot 2 \cdot 2 \cdot 18 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^4 \cdot 3^2.$$

$$D = 2^2 \cdot 3 = 12.$$

Definice 2. 3:

Čísla $n_1, n_2, \dots, n_k \in \mathbb{N}$ se nazývají nesoudělná, jestliže platí $D(n_1, n_2, \dots, n_k) = 1$.

Čísla $n_1, n_2, \dots, n_k \in \mathbb{N}$ se nazývají po dvou nesoudělná, jestliže pro každé i, j takové, že $1 \leq i < j \leq n$ platí $D(n_i, n_j) = 1$.

2. 2 Nejmenší společný násobek:

společný násobek přirozených čísel $a_1, a_2, \dots, a_k$ nazýváme přirozené číslo, jež je násobkem každého z nich. Ten ze společných násobků, který je menší než kterýkoliv jiný společný násobek, se nazývá nejmenší společný násobek NSN, značíme $n(a_1, a_2, \dots, a_k)$.

Věta 2. 2:

Pro libovolná celá čísla a, b platí:

$$D(a, b) \cdot n(a, b) = a \cdot b.$$

Př. 2. 4:

Určete $n(900, 588)$.

Řešení:

$$D(900, 588) \Rightarrow 900 = 450 \cdot 2 = 225 \cdot 2 \cdot 2 = 45 \cdot 5 \cdot 2 \cdot 2 = 9 \cdot 5 \cdot 5 \cdot 2 \cdot 2 = 2^2 \cdot 3^2 \cdot 5^2.$$

$$\Rightarrow 588 = 294 \cdot 2 = 147 \cdot 2 \cdot 2 = 21 \cdot 7 \cdot 2 \cdot 2 = 2^2 \cdot 3 \cdot 7^2.$$

$$D = 2^2 \cdot 3 = 12.$$

$$12 \cdot n = 900 \cdot 588 \Rightarrow n = 529\,200 \mid 12 = \underline{44\,100}.$$

Příklady k procvičení:**Př. 2. 5:**

Druhá mocnina každého lichého čísla zmenšená o číslo 1 je dělitelná číslem 8. Dokažte.

Př. 2. 6:

Součet druhých mocnin dvou libovolných lichých čísel je dělitelný 2, ale není dělitelný 4. Dokažte.

Př. 2. 7:

Mějme čtyři za sebou následující celá čísla a vytvořme součiny každých dvou z těchto čísel. Potom součet všech těchto součinů zvětšený o číslo 1 je dělitelný číslem 12. Dokažte.

Př. 2. 8:

Ukažte, že čísla $n(n + 1)(2n + 1)$ a $n^3 + 5n$ jsou dělitelná 6 pro každé celé číslo n .

Př. 2. 9:

Není-li a dělitelné třemi, je třemi dělitelné číslo $a^2 - 1$. Dokažte.

Př. 2. 10:

Necht' celá čísla a , b jsou buď obě násobkem tří, nebo necht' žádné z nich není násobkem tří. Pak je rozdíl $a^2 - b^2$ násobkem tří. Dokažte.

Př. 2. 11:

Může být součet druhých mocnin čtyř po sobě následujících celých čísel druhou mocninou celého čísla?

Př. 2. 12:

Rozdíl druhých mocnin dvou libovolných lichých čísel je násobkem čísla 8. Dokažte.

3. Eukleidův algoritmus

Věta 3. 1:

Eukleidův algoritmus je početní postup, jehož pomocí určujeme největšího společného dělitele dvou přirozených čísel.

Nechť $a, b \neq 0$ jsou přirozená čísla. Pak existují celá čísla $r_1, r_2, \dots, r_n, q_0, q_1, \dots, q_n$ tak, že $r_n = D(a, b)$ a

$$a = q_0 \cdot b + r_1,$$

$$b = q_1 \cdot r_1 + r_2,$$

.

.

.

$$r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n,$$

$$r_{n-1} = q_n \cdot r_n.$$

Z poslední rovnosti plyne, že $r_n \mid r_{n-1}$, z předposlední, že $r_n \mid r_{n-2}$, atd., až nakonec ze druhé $r_n \mid b$ a z první dostaneme $r_n \mid a$. Tím jsme dokázali, že r_n je největší dělitel čísel a, b .

Př. 3. 1:

Určete $D(1\,284, 144)$.

Řešení:

$$1\,284 = 8 \cdot 144 + 132,$$

$$144 = 132 \cdot 1 + \underline{12},$$

$$132 = \underline{12} \cdot 11 + 0.$$

$$D(1\,284, 144) = 12.$$

Př. 3. 2:

Určete $D(2^{63} - 1, 2^{91} - 1)$.

Řešení:

$$2^{91} - 1 = 2^{28} \cdot (2^{63} - 1) + 2^{28} - 1,$$

$$2^{63} - 1 = (2^{35} + 2^7) \cdot (2^{28} - 1) + 2^7 - 1,$$

$$2^{28} - 1 = (2^{21} + 2^{14} + 2^7 + 1) \cdot (2^7 - 1),$$

$$D(2^{63} - 1, 2^{91} - 1) = 2^7 - 1 = 127.$$

Př. 3. 3:

Najděte $D(93, 72)$, dále najdi taková celá čísla x a y , aby $D(93, 72) = x \cdot 72 + y \cdot 93$.

Řešení:

$$93 = 1 \cdot 72 + 21,$$

$$72 = 3 \cdot 21 + 9,$$

$$21 = 2 \cdot 9 + \underline{3},$$

$$D(93, 72) = 3.$$

Pro nalezení x a y využijeme předešlé výpočty, postupujeme však odzadu:

$$D(93, 72) = 3 = 21 - 2 \cdot 9 = (93 - 72) - 2 \cdot (72 - 3 \cdot 21) =$$

$$= (93 - 72) - 2 \cdot (72 - 3 \cdot (93 - 72)) = 93 - 72 - 2 \cdot (72 - 3 \cdot 93 + 3 \cdot 72) =$$

$$= 93 - 72 - 2 \cdot 72 + 6 \cdot 93 - 6 \cdot 72 = \underline{7} \cdot 93 - \underline{9} \cdot 72.$$

Hledaná čísla jsou tedy $x = -9, y = 7$.

Příklady k procvičení:**Př. 3. 4:**

Určete $D(900, 588)$.

[12]

Př. 3. 5:

Určete $D(450, 294)$.

[6]

Př. 3. 6:

Najděte celá čísla x a y tak, aby $x \cdot 18 + y \cdot 25 = 1$.

[7, -5]

4. Prvočísla

Definice 4. 1:

Přirozené číslo $p > 1$, se nazývá prvočíslu, jestliže p nemá přirozené dělitele různé od 1 a p .

Přirozené číslo n , $n > 1$, se nazývá složené, právě když není prvočíslem, tj. má alespoň jednoho přirozeného dělitele různého od 1 a n .

Platí:

- Všechna prvočísla, kromě čísla 2, jsou lichá.
- Každé složené číslo n má alespoň jednoho přirozeného (prvočíselného) dělitele $p \leq \sqrt{n}$, tj. není-li přirozené číslo $n > 1$ dělitelné žádným prvočíslem $p \leq \sqrt{n}$, pak n je prvočíslu.
- Existují dvojice prvočísel s rozdílem 2. Takové dvojice nazýváme **prvočíselná dvojčata**. Jsou to např. čísla 3, 5; 5, 7; 11, 13... .
Mezi kladnými přirozenými čísly menšími než $3 \cdot 10^6$ existuje 152 892 takových dvojic. Zatím však nikdo nedokázal, zda takových dvojic je, nebo není nekonečně mnoho.

Př. 4. 1:

Číslo 13 má při dělení dvěma zbytek 1, při dělení 3 zbytek 1, při dělení pěti zbytek 3 atd. Beze zbytku je dělitelné pouze 1 a 13. Proto je 13 prvočíslu.

Číslo 24 je dělitelné čísly 1, 2, 3, 4, 6, 8, 12, 24 - proto není prvočíslem.

Věta 4. 1:

(Základní věta aritmetiky).

Pro každé přirozené číslo $n \neq 1$ existují různá prvočísla $p_1, p_2, \dots, p_m$

a přirozená čísla $k_1, k_2, \dots, k_m$ splňující

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}.$$

- tomuto vyjádření se říká prvočíselný rozklad
- zápis je jednoznačný až na pořadí činitelů

Důkaz:

Nejprve indukcí dokážeme existenci rozkladu.

Je-li n prvočíslo, rozklad zřejmě existuje. Dále předpokládejme, že n je složené a že rozklad existuje pro všechna menší čísla. Můžeme tedy napsat $n = a \cdot b$ pro $a, b < n$.

Podle indukčního předpokladu existuje prvočíselný rozklad jak pro a , tak i pro b , a jejich složením získáme rozklad čísla n .

Jednoznačnost rozkladu také dokážeme indukcí.

Nechť n je nejmenší číslo s nejednoznačným rozkladem; uvažujme tedy dva různé prvočíselné rozklady $n = p_1^{k_1} \cdot \dots \cdot p_m^{k_m} = q_1^{l_1} \cdot \dots \cdot q_r^{l_r}$.

Protože $p_1 \mid n = q_1^{l_1} \cdot \dots \cdot q_r^{l_r}$, podle předchozího důsledku existuje i takové, že $p_1 \mid q_i$. Jelikož q_i je prvočíslo, pak tedy $p_1 = q_i$.

Dále uvažujme číslo $n \mid p_1$, to je menší než n , přitom má také dva různé rozklady, a to: $p_1^{k_1-1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m} = q_1^{l_1} \cdot \dots \cdot q_{i-1}^{l_{i-1}} \cdot q_r^{l_r}$.
Což je spor s původním předpokladem.

Věta 4. 2:

Prvočísel je nekonečně mnoho.

Důkaz sporem:

Nechť existuje jen konečně mnoho prvočísel. Označme je $p_1, p_2, \dots, p_n$. Potom číslo $x = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ není dělitelné žádným z těchto prvočísel, jelikož při dělení dostaneme vždy zbytek 1. Tím pádem číslo x musí být buď prvočíslo, nebo musí být dělitelné nějakým jiným prvočíslem. To ale znamená, že množina prvočísel z počátku důkazu nebyla úplná, což je spor s předpokladem.

Př. 4. 2:

Nalezněte všechna $k \in \mathbb{N}$, pro která je mezi deseti po sobě jdoucími čísly $k + 1, k + 2, \dots, k + 10$ nejvíce prvočísel.

Řešení:

Postupně zjistíme, že pro $k = 0$ jsou 4 prvočísla (2, 3, 5, 7), pro $k = 1$ je 5 prvočísel (2, 3, 5, 7, 11), pro $k = 2$ jsou 4 prvočísla (3, 5, 7, 11). Pro $k \geq 3$ není mezi zkoumanými čísly prvočíslo 3, máme vždy 10 čísel, z nichž je 5 sudých a 5 lichých, z nichž nejméně jedno bude vždy násobkem 3. Zbývají tedy vždy nejvýše 4 prvočísla. Hledanému k tedy vyhovuje pouze číslice 1.

Příklady k procvičení:**Př. 4. 3:**

Najděte všechna čtyřciferná čísla $a_3 a_2 a_1 a_0$, která jsou druhou mocninou přirozeného čísla.

[7 744]

Př. 4. 4:

Jestliže je p prvočíslo, je číslo $p^4 + 24$ složené. Dokažte.

Př. 4. 5:

Je-li $p > 3$ prvočíslo je číslo $p^2 - 1$ násobkem čísla 24. Dokažte.

Př. 4. 6:

Zjistěte, které číslo splňuje následující podmínky: hledané číslo má právě čtyři různé dělitele (včetně sebe a čísla jedna). Přitom dva dělitele jsou dvojciferná čísla, která mají tu vlastnost, že jedno vznikne z druhého přehozením číslic. Rozdílem těchto dvojciferných dělitelů je číslo dělitelné osmnácti. Uveďte všechny možnosti.

[403, 1 207, 2 701, 7 663]

Př. 4. 7:

První číslice hledaného čísla je největším prvočíslem, které se dá zapsat jednou číslicí. Následují pak dvě čtyřčíslí. Obě jsou vytvořena stejně – máme dvojciferné číslo, mezi jehož cifry jsou vloženy dvě nuly (např. 51 $\rightarrow$ 5001) a zároveň pro toto čtyřciferné číslo platí, že když ho vydělíme 91, dostaneme dvojciferné číslo, z kterého bylo naše čtyřčíslí utvořeno. Pro druhé čtyřčíslí dále platí, že je pětikrát větší než to, které následuje hned za prvočíslem. Najdi hledané číslo.

[710 015 005]

5. Eratosthenovo síto

Eratosthenovo síto je jednoduchý algoritmus pro nalezení všech prvočísel menších než zadaná horní mez.

Algoritmus funguje „prosíváním“ čísel - na počátku posloupnost obsahuje všechna čísla v daném rozsahu (2, 3, 4, ..., n).

Poté se opakovaně první číslo z posloupnosti vyjme, toto číslo je prvočíslem a odstraní se všechny násobky tohoto čísla (což jsou čísla složená).

Tak se pokračuje do doby, než je z posloupnosti odstraněno poslední číslo, nebo ve chvíli, kdy je jako prvočíslo označeno číslo vyšší než odmocnina nejvyššího čísla – v takové chvíli už všechna zbývajících čísla jsou nutně prvočísla.

Př. 5. 1:

Zjistěte, zda je číslo 187 prvočíslo.

Řešení:

$\sqrt{187} \leq 13,7 \dots$ hledaná prvočísla jsou menší nebo rovna 13 (13, 11, 7, 5, 3, 2).

Pokud jde číslo 187 vydělit některým z prvočísel menším než 13, nebo 13-ti, pak není číslo 187 prvočíslem.

$$\frac{187}{11} = 17, \text{ tudíž není prvočíslem.}$$

Příklady k procvičení:

Př. 5. 2:

Ověřte pomocí Eratosthenova síta, zda je 823 prvočíslo.

6. Kritéria dělitelnosti v desítkové soustavě

Definice 6. 1:

Číselnou soustavou nazveme množinu určitých znaků, která slouží ke zobrazení čísel. Každé přirozené číslo a lze jednoznačně vyjádřit ve tvaru:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

kde $a_n, a_{n-1}, \dots, a_0 \in \mathbb{N}$

Kritéria dělitelnosti přirozenými čísly n :

- pro $n = 2 \Rightarrow$ končí - li a_0 některou z číslic 0, 2, 4, 6, 8.
- pro $n = 3 \Rightarrow$ je-li ciferný součet $a_n + a_{n-1} + \dots + a_1 + a_0$ dělitelný 3
(Př.: číslo 228 $\Leftrightarrow 2 + 2 + 8 = 12 \Leftrightarrow 3 / 12$)
- pro $n = 4 \Rightarrow$ je-li poslední dvojčíslí $a_1 \cdot 10 + a_0$ dělitelné 4 (**612**, **1 008**)
- pro $n = 5 \Rightarrow$ je-li $a_0 = 5$ nebo 0
- pro $n = 6 \Rightarrow$ je-li číslo a_0 sudé a zároveň $a_n + a_{n-1} + \dots + a_1 + a_0$ dělitelný 3
(Př.: číslo 924 $\Leftrightarrow$ je sudé, $9 + 2 + 4 = 15 \Leftrightarrow 3 / 15$)
- pro $n = 7 \Rightarrow$ číslo a_0 vynásobím 2 a odečtu od čísel zbývajících. Je-li po konečném počtu kroků číslo dělitelné 7, je pak celé číslo dělitelné 7.

př: 138 309 241

$$13\ 830\ 924 - 1 \cdot 2 = 13\ 830\ 922$$

$$1\ 383\ 092 - 2 \cdot 2 = 1\ 383\ 088$$

$$138\ 308 - 2 \cdot 8 = 138\ 292$$

$$13\ 829 - 2 \cdot 2 = 13\ 825$$

$$1\ 382 - 2 \cdot 5 = 1\ 372$$

$$137 - 2 \cdot 2 = 133$$

$$13 - 2 \cdot 3 = 7$$

- pro $n = 8 \Rightarrow$ je-li poslední trojčíslí $a_2 \cdot 4 + a_1 \cdot 2 + a_0$ dělitelné 8
(Př.: číslo 12 **504** $\Leftrightarrow 5 \cdot 4 + 0 \cdot 2 + 4 = 24 \Leftrightarrow 8 / 24$)

- pro $n = 9 \Rightarrow$ je-li ciferný součet $a_n + a_{n-1} + \dots + a_1 + a_0$ dělitelný 9
(Př.: číslo 1 683 $\Rightarrow 1 + 6 + 8 + 3 = 18 \Rightarrow 9 / 18$)
- pro $n = 10 \Rightarrow$ je-li $a_0 = 0$
- pro $n = 11 \Rightarrow$ je-li $(\dots - a_5 + a_4 - a_3 + a_2 - a_1 + a_0) = 0$ nebo dělitelný 11, tj. rozdíl součtu číslic na sudém a lichém místě roven 0 nebo dělitelný jedenácti
(Př.: číslo 5 357 $\Rightarrow (5 + 5) - (3 + 7) = 0$;
číslo 919 292 $\Rightarrow (9 + 9 + 9) - (1 + 2 + 2) = 22 \Rightarrow 11 / 22$)
Této dělitelnosti se používá u rodných čísel, všechna vystavená rodná čísla musí být dělitelná 11.
- pro $n = 12 \Rightarrow$ jeho ciferný součet $a_n + a_{n-1} + \dots + a_1 + a_0$ musí být dělitelný 3 a zároveň $a_1 \cdot 10 + a_0$ dělitelné 4
(Př.: číslo 78 504 $\Rightarrow 7 + 8 + 5 + 0 + 4 = 24 \Rightarrow 3 / 24$ a zároveň $4 / 4$)
- pro $n = 13 \Rightarrow$ je-li $(\dots + (a_8 \cdot 10^8 + a_7 \cdot 10^7 + a_6 \cdot 10^6) - (a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3 \cdot 10^3) + (a_2 \cdot 10^2 + a_1 \cdot 10 + a_0))$ tj. rozdíl součtu lichých a sudých trojic cifer dělitelný třinácti
(Př.: číslo 2 022 046 $\Rightarrow 002 + 046 - 022 = 26$)
- pro $n = 25 \Rightarrow$ je-li $a_1 \cdot 10 + a_0$ dělitelné 25
(Př.: čísla 125, 15 475)
- pro $n = 100 \Rightarrow$ jsou-li poslední dvě číslice 0

Př. 6. 1:

Najděte všechna trojciferná čísla s touto podmínkou: napíšeme-li před hledané číslo stejnou číslici, jako je ta, která udává počet jednotek, dostaneme čtyřciferné číslo, které je o 18 menší než sedminásobek hledaného čísla.

Řešení:

Hledané číslo a je ve tvaru:

$$a = a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \text{ přitom je } 0 < a_2 \leq 9, 0 \leq a_1 \leq 9, 0 < a_0 \leq 9,$$

poznámka: a_2 nesmí být 0 $\Rightarrow$ nešlo by o trojciferné číslo, a_0 nesmí být 0 $\Rightarrow$ podle zadání má vzniknout napsáním číslice a_0 před číslo a číslo čtyřciferné.

Podmínku zapíšeme:

$$a_0 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 + 18 = 7 \cdot (a_2 \cdot 10^2 + a_1 \cdot 10 + a_0),$$

Upravíme:

$$1000 \cdot a_0 + 100 \cdot a_2 + 10 \cdot a_1 + 20 = 700 \cdot a_2 + 70 \cdot a_1 + 6 \cdot a_0 + 2.$$

V poslední rovnosti musí $10 / (6 \cdot a_0 + 2)$ což splňuje $a_0 = 3$, $a_0 = 8$.

Vyšetříme obě možnosti:

a) pro $a_0 = 3$ po úpravě dostaneme

$$10 \cdot a_2 + a_1 = 50.$$

To je možné splnit vzhledem k podmínce jen pro $a_1 = 0$ a $a_2 = 5$,
dostali jsme tedy číslo 503.

b) pro $a_0 = 8$ po úpravě dostaneme

$$60 \cdot a_2 + 6 \cdot a_1 = 797.$$

Jelikož 6 nedělí 797, neexistují celá čísla, která by splňovala tuto rovnost.

Máme tedy jediný možný výsledek $a = 503$, který dosadíme do podmínky:

$$3503 + 18 = 7 \cdot 503.$$

Výpočtem zjistíme, že číslo skutečně vyhovuje.

Příklady k procvičení:

Př. 6. 2:

Dvě trojciferná čísla jsou zapsána stejnými číslicemi v opačném pořadí. Dokažte, že jejich rozdíl je násobkem čísla 99.

Př. 6. 3:

Dokažte, že cyklickou záměnou číslic trojciferného čísla, které je dělitelné 37 (popř. 27) vznikne číslo, které je rovněž dělitelné 37 (popř. 27).

Př. 6. 4:

Dvojciferné číslo na pravé straně obdržíte záměnou cifer dvojciferného čísla v jeho levé části. Když od toho pravého čísla odečtete levé číslo, dostanete číslo, které se rovná polovině ciferného součtu celého čtyřciferného čísla.

Jaké je hledané čtyřciferné číslo?

[5 445]

Př. 6. 5:

Do herny zabloudil zvědavý turista. V peněženke měl pouze dvacetikoruny a koruny, dohromady jich nebylo ani 20 kusů. Vsadil v ruletě a vyhrál. Jeho výhra se rovnala šestinásobku hodnoty, kterou si přinesl do herny. Ihned z herny odešel a spočítal si, že má právě tolik dvacetikorunových bankovek, jako měl korunových mincí, a právě tolik korunových mincí, kolik měl dvacetikorunových bankovek. S jakou hodnotou peněz vstupoval turista do herny a s jakou hodnotou z ní odcházel?

[57, 342]

Př. 6. 6:

Když jsem vyšla z domova, měla jsem v kapse korunové a pětikorunové mince. Dohromady byla částka větší než 140 Kč a menší než 150 Kč. Utratila jsem třetinu svých peněz a zůstalo mi tolik korunových mincí, kolik jsem měla původně pětikorun, a tolik pětikorun, kolik jsem měla původně korun. Kolik mincí každého druhu jsem měla, když jsem vycházela z domova?

[144]

7. Vyjádření čísla v číselné soustavě o základu z

Kromě desítkové soustavy existují číselné soustavy o libovolném základu z , kde z je přirozené číslo větší než 1.

Definice 7. 1:

Každé přirozené číslo a se dá jednoznačně vyjádřit ve tvaru:

$$a = a_n z^n + a_{n-1} z^{n-1} + \dots + a_2 z^2 + a_1 z + a_0,$$

kde a_i, n jsou celá nezáporná čísla, pro něž platí $0 \leq a_i < z$ pro $i = 0, 1, 2, \dots, n, a_n \neq 0$.

Číslo vyjádřené v jiné číselné soustavě než desítkové zapisujeme stručně

$$a = (a_n a_{n-1} \dots a_2 a_1 a_0)_z.$$

Př. 7. 1:

Vyjádřete přirozené číslo a v číselné soustavě o základu $z > 1$.

Řešení:

Ke každému přirozenému číslu a existuje právě jedno takové přirozené číslo n , že $z^n \leq a < z^{n+1}$. Dělíme-li číslo a číslem z , vyjde neúplný podíl q_1 a zbytek, který označíme a_0 , takže:

$$a = q_1 z + a_0.$$

Dělíme-li dále číslo q_1 číslem z , vznikne neúplný podíl q_2 a zbytek $a_1, \dots$. Při k -tém kroku dělíme neúplný podíl q_{k-1} číslem z , čímž vznikne neúplný podíl q_k a zbytek a_{k-1} .

Postup končí po n krocích, kdy při n -tém kroku dostaneme:

$$q_{n-1} = q_n z + a_{n-1}.$$

Př. 7. 2:

Vyjádřete číslo $a = (123\,456)_{10}$ v soustavě $z = 7$.

Řešení:

$$123\,456 = 17\,636 \cdot 7 + \underline{4},$$

$$17\,636 = 2\,519 \cdot 7 + \underline{3},$$

$$2\,519 = 359 \cdot 7 + \underline{6},$$

$$359 = 51 \cdot 7 + \underline{2},$$

$$51 = 7 \cdot 7 + \underline{2},$$

$$7 = \underline{1} \cdot 7 + \underline{0},$$

$a_0 = 4, a_1 = 3, a_2 = 6, a_3 = 2, a_4 = 2, a_5 = 0, a_6 = 1$ a $(123\,456)_{10} = (1\,022\,634)_7$.

Př. 7. 3:

Převeďte výsledek z předchozího příkladu zpět do desítkové soustavy.

Řešení:

Při převodu čísla a z číselné soustavy o základu z do desítkové soustavy použijeme vyjádření $a = a_n z^n + a_{n-1} z^{n-1} + \dots + a_2 z^2 + a_1 z + a_0$:

$$\begin{aligned}(1\,022\,634)_7 &= 1 \cdot 7^6 + 0 \cdot 7^5 + 2 \cdot 7^4 + 2 \cdot 7^3 + 6 \cdot 7^2 + 3 \cdot 7^1 + 4 \cdot 7^0 = \\ &= 117\,649 + 4\,802 + 686 + 294 + 21 + 4 = 123\,456.\end{aligned}$$

Př. 7. 4:

Vyjádřete číslo $a = (3\,528)_{10}$ v soustavě $z = 16$.

Řešení:

V soustavách $z > 10$ používáme pro číslice $10 = A, 11 = B, 12 = C, \dots$.

$$3\,528 = 220 \cdot 16 + \underline{8},$$

$$220 = \underline{13} \cdot 16 + \underline{12}.$$

Protože $13 = D, 12 = C$, $(3\,528)_{10} = (DC8)_{16}$.

$$\text{Zk: } 13 \cdot 16^2 + 12 \cdot 16^1 + 8 \cdot 16^0 = 3\,328 + 192 + 8 = 3\,528.$$

7. 1 Sčítání soustav o základu vyšším než $z = 10$

Př. 7. 5:

Vyjádřete čísla $(2\ 972)_{10}$ a $(556)_{10}$ v $z = 12$, poté čísla sečtěte.

Řešení:

$$2\ 972 = (1\ 878)_{12};\ 556 = (3A4)_{12}.$$

$$(1\ 878)_{12}$$

$$+(3A4)_{12}$$

$$(2060)_{12}$$

$$8 + 4 = 12 = \underline{0} + \text{zvýšení řádu o } + 1,$$

$$7 + A + 1 = 18 = 12 + 6 = \underline{6} + \text{zvýšení řádu o } + 1,$$

$$8 + 3 + 1 = 12 = \underline{0} + \text{zvýšení řádu o } + 1,$$

$$1 + 1 = \underline{2}.$$

$$\text{Zk: } (2\ 060)_{12} = 2 \cdot 12^3 + 0 \cdot 12^2 + 6 \cdot 12^1 + 0 \cdot 12^0 = 3\ 456 + 72 = 3\ 528 = 2\ 972 + 556.$$

7. 2 Násobení soustav o základu různém od $z = 10$

Př. 7. 6:

Vyjádřete čísla $(56)_{10}$ a $(63)_{10}$ v $z = 4$, poté čísla vynásobte.

$$56 = (320)_4,\ 63 = (333)_4$$

$$(320)_4$$

$$(333)_4$$

$$2220$$

$$2220$$

$$\underline{2220}$$

$$313020$$

$$3 \cdot 0 = 0,$$

$$3 \cdot 2 = 6 = 4 + 2 = 2 + \text{zvýšení řádu o } + 1,$$

$$3 \cdot 3 + 1 = 10 = 2 \cdot 4 + 2 = 2 + \text{zvýšení řádu o } + 2,$$

$$\begin{aligned} \text{Zk: } (313020)_4 &= 3 \cdot 4^5 + 1 \cdot 4^4 + 3 \cdot 4^3 + 0 \cdot 4^2 + 2 \cdot 4^1 + 0 \cdot 4^0 = 3 \cdot 072 + 256 + 192 + 8 = \\ &= 3 \cdot 528 = 56 \cdot 63. \end{aligned}$$

Příklady k procvičení:

Př. 7. 7:

Vyjádřete číslo $a = (3 \ 528)_{10}$ v soustavě $z = 2$.

[110 111 001 000]

Př. 7. 8:

Vyjádřete číslo $a = (3 \ 528)_{10}$ v soustavě $z = 5$.

[103 103]

Př. 7. 9:

Vyjádřete číslo $a = (3 \ 528)_{10}$ v soustavě $z = 13$.

Správnost výpočtu ověřte zkouškou.

[17B5]

Př. 7. 10:

Vyjádřete čísla $(2 \ 972)_{10}$ a $(556)_{10}$ v $z = 13$, poté čísla sečtěte.

Správnost výpočtu ověřte zkouškou.

8. Užití dělitelnosti – kongruence

Definice 8. 1:

Nechť $m > 1 \in \mathbb{N}$, nechť a, b jsou celá čísla.

Řekneme, že a je kongruentní s b podle modulu m (nebo též modulo m), jestliže $m \mid (a - b)$.

Píšeme symbolicky: $a \equiv b \pmod{m}$.

Jestliže $m \nmid (a - b)$, říkáme, že a není kongruentní s b podle modulu m , respektive že a je inkongruentní s b podle modulu m ; píšeme $a \not\equiv b \pmod{m}$.

- Vztah $a \equiv b \pmod{m}$ se nazývá kongruence.
- Podle definice kongruence zápis $a \equiv 0 \pmod{m}$ znamená, že $m \mid a$.

Věta 8. 1:

Nechť a, b, c jsou celá čísla. Potom pro každé $(m > 1) \in \mathbb{N}$, platí:

- 1) $a \equiv a \pmod{m}$.
- 2) Je-li $a \equiv b \pmod{m}$, je i $b \equiv a \pmod{m}$.
- 3) Je-li $a \equiv b \pmod{m}$, a $b \equiv c \pmod{m}$, je i $a \equiv c \pmod{m}$.

Věta 8.1. říká, že kongruence podle libovolného přirozeného modulu je, podobně jako rovnost vztah:

- reflexivní,
- symetrická,
- tranzitivní.

Věta 8. 2:

Nechť a, b, c jsou celá čísla, $m \in \mathbb{N}$, $m > 1$.

Nechť dále $a \equiv b \pmod{m}$ a $c \equiv c \pmod{m}$.

Pak je také:

- 1) $(a + c) \equiv (b + c) \pmod{m}$.
- 2) $(a - c) \equiv (b - c) \pmod{m}$.
- 3) $ac \equiv bc \pmod{m}$.

Důkaz:

Je-li $a \equiv b \pmod{m}$ a $c \equiv c \pmod{m}$, tedy existuje takové číslo $t_1, t_2 \in \mathbb{Z}$ tak, aby $a = b + mt_1$ a $c = c + mt_2$, pak:

- 1) $a + c = (b + mt_1) + (c + mt_2) \Rightarrow a + c \equiv b + c \pmod{m}$.
- 2) $a - c = (b + mt_1) - (c + mt_2) \Rightarrow a - c \equiv b - c \pmod{m}$.
- 3) $a \cdot c = (b + mt_1) \cdot (c + mt_2) \Rightarrow a \cdot c \equiv b \cdot c \pmod{m}$.

Věta 8. 3:

Nechť $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$, $m > 1$. Dále necht' platí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$.

Potom je také:

- 1) $a + c \equiv b + d \pmod{m}$.
- 2) $a - c \equiv b - d \pmod{m}$.
- 3) $ac \equiv bd \pmod{m}$.

Důkaz:

Je-li $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, existuje takové číslo $t_1, t_2 \in \mathbb{Z}$ tak, že

$a = b + mt_1$ a $c = d + mt_2$, pak:

- 1) $a + c = b + d + m(t_1 + t_2) \Rightarrow a + c \equiv b + d \pmod{m}$.
- 2) $a - c = b - d + m(t_1 - t_2) \Rightarrow a - c \equiv b - d \pmod{m}$.
- 3) $a \cdot c = (b + mt_1) \cdot (d + mt_2) = b \cdot d + bmt_2 + dmt_1 + mt_1mt_2 =$
 $= b \cdot d + m(bt_2 + dt_1 + t_1mt_2) \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$.

Věta 8. 4:

Nechť $a, b \in \mathbb{Z}$ a $m, k \in \mathbb{N}$. Pokud $a \equiv b \pmod{m}$, pak také $a^k \equiv b^k \pmod{m}$.

Důkaz:

Je-li $a \equiv b \pmod{m}$, dokážeme indukcí vzhledem ke $k \in \mathbb{N}$, že $a^k \equiv b^k \pmod{m}$.

- Pro $k = 1$ není třeba dokazovat.
- Pro $k = k + 1$:

vynásobením kongruence $a^k \equiv b^k \pmod{m}$ a kongruence $a \equiv b \pmod{m}$ dostáváme $a^k \cdot a \equiv b^k \cdot b \pmod{m}$, tedy $a^{k+1} \equiv b^{k+1} \pmod{m}$, což je tvrzení pro $k + 1$.

Důkaz indukcí je hotov.

Věta 8. 5:

Relace kongruence podle daného modulu m vytvoří na množině celých čísel takzvaný **rozklad na zbytkové třídy**. Tyto třídy označíme:

- Z_0 (množina všech celých čísel, která jsou dělitelná m),
- Z_1 (množina všech celých čísel, která při dělení m dají zbytek 1),
- $\vdots$
- Z_{m-1} (množina všech celých čísel, která při dělení m dají zbytek $m - 1$).

Například při kongruenci podle modulu 5 dostaneme zbytkové třídy:

$$Z_0 = \{ \dots, -15, -10, -5, 0, 5, 10, 15, \dots \},$$

$$Z_1 = \{ \dots, -14, -9, -4, 1, 6, 11, 16, \dots \},$$

$$Z_2 = \{ \dots, -13, -8, -3, 2, 7, 12, 17, \dots \},$$

$$Z_3 = \{ \dots, -12, -7, -2, 3, 8, 13, 18, \dots \},$$

$$Z_4 = \{ \dots, -11, -6, -1, 4, 9, 14, 19, \dots \}.$$

Vybereme-li z každé zbytkové třídy jedno číslo dostaneme tzv. *úplnou soustavu zbytků podle modulu m* . Například množina $\{-15, -4, 2, 13, 19\}$ je úplnou soustavou zbytků podle modulu 5.

Věta 8. 6:

Úplná soustava zbytků modulo m je libovolná m -tice čísel po dvou nekongruentních modulo m (nejčastěji $0, 1, \dots, m-1$).

Redukovaná soustava zbytků R_i modulo m je libovolná $\varphi(m)$ -tice čísel nesoudělných s m a po dvou nekongruentních modulo m .

Věta 8. 7:

Redukovaný zbytkový systém modulo m tvoří $\varphi(m)$ -tice čísel $(x_1, x_2, \dots, x_{\varphi(m)})$ právě tehdy, když $x_i \in R_i$, $i = 1, \dots, \varphi(m)$. Všechny prvky redukovaného systému jsou nesoudělné s m .

Věta 8. 8:

Pokud $(x_1, x_2, \dots, x_{\varphi(m)})$ je redukovaný zbytkový systém modulo m a $D(m, c) = 1$, pak i $(cx_1, cx_2, \dots, cx_{\varphi(m)})$ je redukovaný zbytkový systém modulo m .

Věta 8. 9:

Nechť $(x_1, x_2, \dots, x_{\varphi(m)})$ a $(y_1, y_2, \dots, y_{\varphi(m)})$ jsou libovolné redukované zbytkové systémy modulo m , pak platí $x_1 \cdot x_2 \cdot \dots \cdot x_{\varphi(m)} \equiv y_1 \cdot y_2 \cdot \dots \cdot y_{\varphi(m)} \pmod{m}$.

Př. 8. 1:

Dokažte, že číslo $101^{103} + 103^{101}$ je dělitelné číslem 51.

Řešení:

Máme dokázat, že zbytek součtu $101^{103} + 103^{101}$ po dělení číslem 51 je 0, proto použijeme kongruence podle modulu 51.

$$101^1 \equiv -1 \pmod{51},$$

$$103^1 \equiv 1 \pmod{51},$$

$$101^{103} \equiv -1^{103} \pmod{51}.$$

$$103^{101} \equiv 1^{101} \pmod{51}.$$

$$101^{103} + 103^{101} \equiv -1 + 1 = 0 \pmod{51}.$$

Tím je důkaz ukončen.

Př. 8. 2:

Určete zbytek po dělení čísla $1\,428^{29} - 312^{15} \cdot 627^{16}$ číslem 77.

Řešení:

Tentokrát se pokusíme nalézt řešení pomocí systematického algoritmu mocnin čísel. Stanovíme, jaké mocniny čísel je třeba realizovat a jaké kongruence je potom třeba vynásobit.

$1\,428^{29} \Rightarrow$ vyjádříme exponent 29 ve dvojkové soustavě:

$$29 = (11101)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \underline{16 + 8 + 4 + 1}.$$

Stačí tedy stanovit, s jakými čísly jsou kongruentní mocniny 16, 8, 4, a 1 čísla 1 428 a ty mezi sebou vynásobit:

$$1\,428^1 \equiv 42 \pmod{77},$$

$$1\,428^4 \equiv 49 \pmod{77},$$

$$1\,428^8 \equiv 14 \pmod{77},$$

$$1\,428^{16} \equiv 42 \pmod{77},$$

$$42 \cdot 49 \cdot 14 \cdot 42 = 1\,210\,104 \equiv \underline{49} \pmod{77}.$$

$312^{15} \Rightarrow$ vyjádříme exponent 15 ve dvojkové soustavě:

$$15 = (1111)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \underline{8 + 4 + 2 + 1}.$$

$$312^1 \equiv 4 \pmod{77},$$

$$312^2 \equiv 16 \pmod{77},$$

$$312^4 \equiv 25 \pmod{77},$$

$$312^8 \equiv 9 \pmod{77},$$

$$4 \cdot 16 \cdot 25 \cdot 9 = 14\,400 \equiv 1 \pmod{77}.$$

$627^{16} \Rightarrow$ vyjádříme exponent 16 ve dvojkové soustavě:

$$16 = (1000)_2 = 1 \cdot 2^4 = 16.$$

$$627^1 \equiv 11 \pmod{77},$$

$$627^{16} \equiv 11^{16} \pmod{77},$$

$$11^2 \equiv 44 \pmod{77},$$

$$11^{16} = (11^2)^8 \equiv 44^8 \pmod{77},$$

$$44^2 \equiv 11 \pmod{77},$$

$$44^8 \equiv 11 \pmod{77}.$$

$$1\,428^{29} - 312^{15} \cdot 627^{16} \equiv 49 - 1 \cdot 11 = 38 \pmod{77}.$$

Zbytek dělení čísla $1\,428^{29} - 312^{15} \cdot 627^{16}$ číslem 77 je 38.

Př. 8. 3:

Najděte všechna řešení soustavy kongruencí

$$x \equiv 1 \pmod{2}, \quad x \equiv -1 \pmod{3}, \quad x \equiv 2 \pmod{5}.$$

Řešení:

Hledáme $0 \leq x < 30$.

Třetí kongruenci splňují čísla 2, 7, 12, 17, 22 a 27. Z první kongruence plyne, že hledané číslo je liché, zbývají tedy 7, 17 a 27, z nichž jedině 17 řeší druhou kongruenci.

Všechna řešení soustavy jsou tedy tvaru $x = 30k + 17$, $k \in \mathbb{Z}$.

Příklady k procvičení:

Př. 8. 4:

Určete zbytek po dělení čísla 5^{20} číslem 26.

[1]

Př. 8. 5:

Určete zbytek po dělení čísla $77^{2006} + 12^{2006}$ číslem 6.

[1]

Př. 8. 6:

Určete zbytek po dělení čísla $13^{742} - 10 \cdot 14^{521} + 22^{102}$ číslem 15.

[3]

Př. 8. 7:

Určete zbytek po dělení čísla $1717^{12} + 769^{13}$ číslem 35.

[0]

Př. 8. 8:

Dokažte, že číslo $12^{136} + 47^2$ je dělitelné číslem 65.

Př. 8. 9:

Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné 7.

Př. 8. 10:

Dokažte, že číslo $(835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

Př. 8. 11:

Najděte všechna celá kladná čísla a taková, pro která je výraz $a^{10} + 1$ dělitelný číslem 10.

Př. 8. 12:

Nalezněte všechna celočíselná řešení soustavy

$$5x \equiv 3 \pmod{6}, \quad 2x \equiv 1 \pmod{5}.$$

[30k + 3]

Př. 8. 13:

Nalezněte všechna celočíselná řešení soustavy

$$x \equiv 1 \pmod{3}, \quad x \equiv -1 \pmod{5}, \quad x \equiv 2 \pmod{8}.$$

[120k + 34]

Př. 8. 14:

Šest loupežníků si chtělo rozdělit zlatáky. Když je rozdělovali na šest stejných hromádek, tři zlatáky zbyly. Když je zkusili rozdělit na pět stejných hromádek, jeden zlaták zbyl. Nakonec se nepoprali, protože se vrátil sedmý loupežník, který z kapsy přidal tři zlatáky na stůl a všechny zlatáky pak rozdělil na sedm stejných hromádek. Kolik zlatáků měli původně, víte-li, že jich nebylo více než 400 a méně než 100.

[291]

9. Eulerova funkce

Věta 9. 1:

Eulerova funkce určuje počet čísel v posloupnosti $(1, 2, \dots, n - 1)$ nesoudělných s n . Například $\varphi(10) = 4$, neboť čísla nesoudělná s číslem 10 jsou právě čísla 1, 3, 7, 9.

- Je-li p je prvočíslo, pak:

$$\varphi(p) = p - 1.$$

- Je-li p prvočíslo a $k, k > 1$ přirozené číslo, pak:

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

Důkaz:

Číslo menší než p^k je soudělné s p^k právě když je násobkem čísla p . Násobků čísla p menších než p^k je zřejmě právě $p^{k-1} - 1$. To znamená, že naopak čísel nesoudělných s p^k máme $\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^{k-1} \cdot (p - 1)$.

- Je-li $n > 1$ přirozené číslo a $n = p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$ jeho rozklad, pak:

$$\varphi(n) = p_1^{m_1-1} \cdot (p_1 - 1) \cdot p_2^{m_2-1} \cdot (p_2 - 1) \cdot \dots \cdot p_k^{m_k-1} \cdot (p_k - 1).$$

Př. 9. 1:

$$\varphi(270) = \varphi(2 \cdot 3^3 \cdot 5) = (2 - 1) \cdot 3^2 \cdot (3 - 1) \cdot (5 - 1) = 72.$$

Př. 9. 2:

$$\varphi(45\,375) = \varphi(3 \cdot 5^3 \cdot 11^2) = (3 - 1) \cdot 5^2 \cdot (5 - 1) \cdot 11 \cdot (11 - 1) = 22\,000.$$

9.1. Eulerova věta

Věta 9. 2:

Pro libovolné celé číslo a a libovolné přirozené číslo n takové, že $D(a, m) = 1$ platí:

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

Důkaz:

Je-li m prvočíslo, pak $\varphi(m) = m - 1$ a Eulerova věta přechází na tvar malé Fermatovy věty (důkaz viz věta 10.1).

Větu zbývá dokázat pro případ, kdy m je číslo složené.

Uvažujme libovolné složené číslo $m \in \mathbb{Z}$. Redukovaný zbytkový systém modulo m tvoří $n = \varphi(m)$ redukovaných zbytkových tříd $R_{i_1}, \dots, R_{i_n}$, $i_1 < i_2 < \dots < i_n$.

Nechť redukovaný zbytkový systém tvoří libovolná n -tice $(x_{i_1}, x_{i_2}, \dots, x_{i_n})$, kde $x_{i_k} \in R_{i_k}$, pro $k = 1, \dots, n$. Jelikož požadujeme, aby $D(a, m) = 1$, tvoří redukovaný zbytkový systém n -tice $(ax_{i_1}, ax_{i_2}, \dots, ax_{i_n})$. Pak ovšem platí, že:

$$ax_{i_1} \cdot ax_{i_2} \cdot \dots \cdot ax_{i_n} \equiv x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_n} \pmod{m},$$

po úpravě dostaneme

$$a^n (x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_n}) \equiv x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_n} \pmod{m},$$

po vykrácení dostaneme tvar

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

a jelikož $n = \varphi(m)$, pak

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

Tím je důkaz ukončen.

Př. 9. 3:

Zjistěte poslední cifru čísla 77^{2006} .

Řešení:

Protože $D(77, 10) = 1$ a $\varphi(10) = 4$, platí:

$$77^4 \equiv 1 \pmod{10},$$

$$77^{2006} = (77^4)^{501} \cdot 77^2 \equiv 1^{501} \cdot 77^2 \pmod{10},$$

$$77 \equiv 7 \pmod{10},$$

$$77^2 \equiv 7^2 \pmod{10},$$

$$49 \equiv 9 \pmod{10},$$

$$77^{2006} \equiv 9 \pmod{10} \Rightarrow \text{zbytek po dělení je } 9.$$

Příklady k procvičení:

Př. 9. 4:

Spočtěte $\varphi(1\,968)$.

[640]

Př. 9. 5:

Spočtěte $\varphi(3\,528)$.

[1 008]

Př. 9. 6:

Dokažte, že $\forall n \in \mathbb{N} : \varphi(4n + 2) = \varphi(2n + 1)$.

Př. 9. 7:

Spočtěte $121^{121} \pmod{18}$.

[13]

Př. 9. 8:

Spočtěte $12^{144} \pmod{65}$.

[1]

Př. 9. 9:

Nalezněte zbytek po dělení čísla 171^{2147} číslem 52.

[7]

Př. 9. 10:

Nalezněte zbytek po dělení čísla 793^{792} číslem 24.

[1]

Př. 9. 11:

Nalezněte zbytek po dělení čísla $3\,528^{2007} - 3^{2007}$ číslem 25.

[0]

10. Malá Fermatova věta

Věta 10. 1:

Je-li p prvočíslo a $p \nmid a$, pak

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

Důkaz:

Uvažujme prvočíslo p a redukovaný zbytkový systém mod p . Takový systém obsahuje právě $p - 1$ redukovaných zbytkových tříd $R_1, R_2, \dots, R_{p-1}$. Necht' uvažovaný redukovaný zbytkový systém tvoří libovolná n -tice $(x_1, x_2, \dots, x_{p-1})$,

kde $x_i \in R_i, i = 1, \dots, p - 1$.

Jelikož z předpokladu platí, že $D(a, p) = 1$, tvoří redukovaný zbytkový systém také n -tice $(ax_1, ax_2, \dots, ax_{p-1})$. Platí tedy rovnost:

$$ax_1 \cdot ax_2 \cdot \dots \cdot ax_{p-1} \equiv x_1 \cdot x_2 \cdot \dots \cdot x_{p-1} \pmod{p},$$

jednoduchou úpravou dostaneme:

$$a^{p-1} (x_1 \cdot x_2 \cdot \dots \cdot x_{p-1}) \equiv x_1 \cdot x_2 \cdot \dots \cdot x_{p-1} \pmod{p}.$$

Vidíme, že obě strany kongruence můžeme vydělit součinem prvků redukovaného zbytkového systému, čímž dostaneme požadovanou rovnost

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

Tím je důkaz ukončen.

Př. 10. 1:

Určete zbytek po dělení čísla $2\,007^{2001}$ číslem 401.

Řešení:

Jelikož 401 je prvočíslo a $401 \nmid 2\,007$, podle Fermatovy věty platí:

$$2\,007^{401-1} \equiv 1 \pmod{401},$$

$$2\,007^{2001} = (2\,007^{400})^5 \cdot 2\,007^1 \equiv 1^5 \cdot 2\,007^1 \pmod{401},$$

$$2\,007 \equiv 2 \pmod{401}.$$

Zbytek po dělení je číslo 2.

Př. 10. 2:

Najděte $a, b \in \mathbb{Z}$ tak, aby platilo $4a + 5b = 1$.

Řešení:

Hledáme a tak, aby $5 \mid (1 - 4a) \Rightarrow b = (1 - 4a) \mid 5$ bude řešením. Tedy chceme, aby:

$$1 - 4a \equiv 0 \pmod{5}, \text{ tj. } 4a \equiv 1 \pmod{5}.$$

Víme, že $D(5, 4) = 1$, tudíž:

$$4^4 \equiv 1 \pmod{5} \Rightarrow a = 4^3 = 64.$$

Nyní snadno dopočítáme $b = (1 - 4 \cdot 64) \mid 5 = -51$.

Příklady k procvičení:**Př. 10. 3:**

Určete zbytek při dělení čísla 8^{105} číslem 13.

[8]

Př. 10. 4:

Určete zbytek při dělení čísla $22\,182^{7021}$ číslem 541.

[1]

Př. 10. 5:

Určete zbytek při dělení čísla $6\,112\,007^{127}$ číslem 127.

[5]

Př. 10. 6:

Určete zbytek při dělení čísla $44\,144^{565}$ číslem 283.

[-4]

Př. 10.7:

Dokažte, že $11 \mid 3^{2000} + 4^{2002} + 5^{2001}$.

Př. 10. 8:

Dokažte, že $181 \mid 12\,321^{2\,882} - 321^{2\,882} + 2^6$.

Př. 10. 9:

Dokažte, že $89 \mid 1\,512^{1\,998} - 268^{1\,998}$.

11. Wilsonova věta

Věta 11. 1:

Je-li $p > 1$ prvočíslo, pak:

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Př. 11. 1:

Určete zbytek při dělení čísla 18^{18} číslem 19.

Řešení:

Jelikož 19 je prvočíslo a $19 - 1 = 18$, pak:

$$(18)! + 1 \equiv 0 \pmod{19},$$

$$(18^{18})! \equiv -1 \pmod{19}.$$

Zbytek po dělení je -1 .

Příklady k procvičení:

Př. 11. 2:

Určete zbytek při dělení čísla 484 číslem 23.

[1]

Př. 11. 3:

Určete zbytek při dělení čísla 27 000 číslem 31.

[-1]

12. Lineární neurčité (Diofantské) rovnice

Definice 12. 1:

Lineární neurčitou (Diofantskou) rovnici o dvou neznámých rozumíme rovnici o tvaru:

$$ax + by = c, \quad a \neq 0, b \neq 0; \quad a, b, c \in \mathbb{Z} \text{ jsou neznámé.}$$

Věta 12. 1:

Nutnou a postačující podmínkou pro to, aby neurčitá rovnice $ax + by = c$ měla alespoň jednu dvojici řešení je, aby $D(a, b) \mid c$.

Řešení neurčitých rovnic:

- 1) Nalezneme $D(a, b)$.
- 2) Vydělíme rovnici $ax + by = c$ číslem $D(a, b)$.
- 3) Nalezneme čísla $x', y' \in \mathbb{Z}$ tak, že:
$$a \mid D(a, b) \cdot x' + b \mid D(a, b) \cdot y' = 1.$$
- 4) Vynásobíme rovnici číslem c a dostaneme:
$$ax' \cdot c \mid D(a, b) + by' \cdot c \mid D(a, b) = c.$$
- 5) Čísla x_0 a y_0 jsou řešením rovnice, a to ve tvaru:
$$x_0 = x' \cdot c \mid D(a, b), \quad y_0 = y' \cdot c \mid D(a, b).$$
- 6) Všechna řešení rovnice nalezneme dosazením do rovnic ve tvaru:
$$x = x_0 + (b \mid D(a, b)) \cdot t, \quad y = y_0 - (a \mid D(a, b)) \cdot t,$$

kde t je parametr.

Př. 12. 1:

Nalezněte všechny dvojice přirozených čísel x, y , které splňují rovnici:

$$21x - 15y = 3.$$

Řešení:

- 1) $D(21, 15) = 3.$
- 2) $21 \mid 3 \cdot x - 15 \mid 3 \cdot y = 3 \mid 3 \Rightarrow 7x - 5y = 1.$
- 3) $x' = 3, y' = 4.$
- 4) $21 \cdot 3 - 15 \cdot 4 = 3.$
- 5) $x_0 = 3, y_0 = 4.$
- 6) $x = 3 - 5t, y = 4 - 7t.$

Řešením je tedy rovnice $21(3 - 5t) - 15(4 - 7t) = 3.$

Př. 12. 2:

Zájezdu se má účastnit 195 osob. Je možno objednat dva typy autobusů, které mají 42 a 36 míst k sezení. Denní poplatek za větší autobus je 6 000,- Kč a za menší 5 000,- Kč. Kolik je třeba objednat větších a kolik menších autobusů, aby všichni účastníci zájezdu měli místo k sezení a celkové náklady na autobus byly minimální?

Řešení:

Označíme-li počet větších autobusů x a menších y , pak počet míst v těchto autobusech je $42x + 36y \geq 195$. Celková cena za 1 den zájezdu je pak $6\,000x + 5\,000y$.

Sestavíme tabulku:

x	0	1	2	3	3	4	5
y	6	5	4	3	2	1	0
počet sedadel	216	222	228	234	198	204	210
celková cena	30 000	31 000	32 000	33 000	28 000	29 000	30 000

Z tabulky vyplývá, že nejmenší náklady s dostatečným počtem sedadel jsou v případě, kdy objednáme 3 větší a 2 menší autobusy.

Příklady k procvičení:

Př. 12. 3:

Nalezněte všechny dvojice přirozených čísel x, y , které splňují rovnici:

$$14x + 5y = 6.$$

$$[14 \cdot (-6 + 5t) + 5 \cdot (18 - 4t) = 6]$$

Př. 12. 4:

Existují takové dva druhy konzerv, že hmotnost každého z obou druhů je celým násobkem 100g. Menší konzerva má hmotnost menší než 1kg a je známo, že 11 menších konzerv se dá vyvážit na rovnoramenných vahách 6-ti většími konzervami a závažím o hmotnosti 1kg. Určete hmotnost větší a menší konzervy.

$$[800\text{g a } 1\,300\text{g}]$$

Př. 12. 5:

Devatenáct bodů v rovině tvoří vrcholy trojúhelníků a čtyřúhelníků. Kolik takových trojúhelníků a čtyřúhelníků existuje, jestliže každý bod je vrcholem jediného obrazce.

$$[1 \text{ a } 4 \text{ nebo } 5 \text{ a } 1]$$

Př. 12. 6:

Je dán terč o kruzích s 20, 12, a 8 body. Dosažený počet bodů byl roven 168. Kolik zásahů bylo v jednotlivých kruzích, když ve středním kruhu byl stejný počet zásahů jako ve zbývajících dvou.

$$[80, 72, 16]$$

Př. 12. 7:

Na přehradě se uskutečnila projížďka motorovými čluny, které se zúčastnilo 288 rekreatů. Čluny byly 17-ti a 19-ti místné. Kolik člunů z každého druhu bylo použito, byla-li obsazena všechna sedadla.

$$[8, 8]$$

Př. 12. 8:

Rodiče studentů gymnázia zorganizovali zájezd na hory. Je známo, že: cena jízdenky pro dospělého byla o 20% vyšší, než cena jízdenky studenta, že cena každé jízdenky byla vyjádřena dvojčífným přirozeným číslem a že hodnota jízdenky pro dospělého byla zapsána stejnými číslicemi jako pro studenta, avšak v opačném

pořadí. Celkové jízdné bylo menší než 2000 Kč. Kolik korun stály všechny jízdenky, jestliže se zájezdu zúčastnilo 25 studentů a 8 dospělých?

[1557]

Př. 12. 9:

Obchodník chtěl zakoupit menší množství látky (nejvýše 30m). Nakonec si vybral dva druhy. Za jeden metr látky prvního druhu zaplatil 80 Kč, jeden metr látky druhého druhu byl o 10 Kč dražší. Celkem za oba druhy zaplatil 2 530 Kč. Kolik které látky koupil?

[8p a 21d nebo 17p a 13d]

Př. 12. 10:

Pouťový obchodník začal prodávat „turecký“ med. Kousek medu stál buď 5 Kč nebo dvojnásobně velký 8 Kč. Za chvíli měl v pokladniče 400 Kč.

Pro jaký parametr t má úloha řešení?

[150, 151, ... , 160]

Př. 12. 11:

Porovná-li věk mých dětí, mohu říci, že čtrnáctinásobek věku staršího syna je o 1 rok větší než sedmnáctinásobek věku mladšího syna. Zjistěte věk obou chlapců.

[9 a 11]

Závěr

Doufám, že tato práce bude přínosem pro studenty studující předmět algebra II. a pomůže k lepšímu pochopení a porozumění probírané látky.

Celou práci jsem se snažila koncipovat systematicky. Postupně nás seznamuje se základními pravidly, které se v algebře vyskytují. Dále jsou uvedeny některé důležité matematické věty, s jejichž pomocí je svět čísel a výpočtů snazší a podle mého také zajímavější. V neposlední řadě snad tato práce zaujme a poskytne dostatek zajímavých a neobvyklých příkladů k procvičení.

Cílem této bakalářské práce je především ukázat správnou cestu a dopřát potencionálnímu studentovi dobrý pocit z pochopení a uchopení nově nabytých znalostí.

Použitá literatura:

- [1] Hruša, Dlouhý, Rohlíček: Úvod do studia matematiky, Praha: SPN 1977
- [2] Katriňák T. : Algebra a teoretická aritmetika 2, Bratislava: Alfa 1986
- [3] Tlustý P.: Algebra 2 – skripta, České Budějovice 1995
- [4] WIKIPEDIA – The free Encyclopedia – <http://www.wikipedia.org>