Západočeská univerzita v Plzni
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

VYBRANÉ KAPITOLY Z ELEMENTÁRNÍ ALGEBRY
DIPLOMOVÁ PRÁCE

Bc. Jiří KRYČ
Učitelství pro 2. stupeň ZŠ, obor Mt - Fy
léta studia (2010 - 2013)

Vedoucí práce: Mgr. Lukáš HONZÍK

Plzeň, 25. březen 2013

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 25. březen 2013

……

vlastnoruční podpis

Poděkování:

Chtěl bych tímto poděkovat všem lidem, kteří mi pomáhali při vzniku této práce. Zejména bych chtěl vyzdvihnout vedoucího diplomové práce Mgr. Lukáše Honzíka, za odborné vedení práce, velkou trpělivost a cenné rady, které mi byly od něj uděleny. Dále ostatním, kteří mi zapůjčili potřebnou literaturu a těm, kteří mi pomohli kontrolovat práci.

OBSAH

0 ÚVOD

Toto téma diplomové práce jsem si vybral proto, že je velmi zajímavé a pohlíží na matematiku docela jiným způsobem. V předmětu elementární algebra, který jsem absolvoval ve 2. ročníku bakalářského studia, nám pan Doc. RNDr. Jaroslav Drábek CSc. podrobně popisoval problémy, postupy a řešení jednotlivých příkladů elementární algebry. Už v té době mi tato problematika velice zajímala. V první kapitole se zabývám hledáním největšího společného dělitele a nejmenšího společného násobku pomocí Euklidova algoritmu. Výpočty uvádím pro dvě přirozená, komplexní čísla a též pro dva polynomy. V druhé kapitole se zabývám hledání kongruencí podle zadaného modulu pomocí přičítání a odečítání modulu, Eulerovy věty, Bezoutovy věty a pomocí metody rozkladu modulu. A ve třetí, poslední kapitole, se zabývám diofantickými rovnicemi. Rovnicemi řeším reálné úkoly, které se dennodenně mohou využívat. Všechny tyto kapitoly mají společný jmenovatel – hledání největšího společného dělitele.

1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL A NEJMENŠÍ SPOLEČNÝ NÁSOBEK

1.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Jsou dána čísla a_1, a_2, d náležící množině celých čísel. Pro číslo d platí, že $d|a_1$ a $d|a_2$, pokud tyto podmínky číslo d splňuje, říkáme, že číslo d je společným dělitelem čísel a_1, a_2. Společný dělitel $d \geq 0$ čísel a_1, a_2, který je dělitelný libovolným společným dělitelem čísel a_1, a_2 se nazývá největším společným dělitelem D čísel a_1, a_2. Navíc ještě platí, že společný dělitel dělí největšího společného dělitele $d|D$.

Společného dělitele čísel a_1, a_2 budeme zapisovat ve tvaru

$$d(a_1, a_2).$$

Pro největšího společného dělitele čísel a_1, a_2 nutně musí platit

$$D(a_1, a_2) = \max d(a_1, a_2).$$

Největšího společného dělitele čísel a_1, a_2 budeme zapisovat ve tvaru

$$D(a_1, a_2).$$

Množinu všech společných dělitelů budeme zapisovat ve tvaru

$$d(a_1, a_2) = d(a_1) \cap d(a_2).$$

VĚTA O DĚLENÍ CELÝCH ČÍSEL SE ZBYTKEM – Pokud jsou zadána dvě čísla a_1, a_2 náležící množině přirozených čísel, existují jednoznačně zadaná čísla q náležící množině celých čísel a $a_3 \in \{0,1, \dots, a_2 - 1\}$ tak, že platí

$$a_1 = a_2 \cdot q + a_3,$$

potom platí následující rovnost

$$D(a_1, a_2) = D(a_2, a_3).$$

1.1.1 EUKLIDŮV ALGORITMUS

Nechť jsou dány dvě čísla a_1, a_2 náležící množině přirozených čísel. Každé číslo $n \geq 3$, pro které je výraz $a_{n-1} \neq 0$ si označíme a_n. a_n je zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Po konečném počtu kroků dostaneme zbytek $a_k = 0$. Tím pádem platí, že člen a_{k-1} je největším společným dělitelem D čísel a_1, a_2.

Následující větu si dokážeme pomocí věty o dělení celých čísel se zbytkem. Podle této věty platí, že $a_2 > a_3 > a_4$ …. Protože se však jedná o celá čísla nezáporná, je každé následující číslo alespoň o 1 menší než číslo předchozí. A proto se po určitém konečném počtu kroků musíme dostat k rovnosti $a_k = 0$. Zároveň platí rovnost, že $a_{k-1} \neq 0$. Z definice čísel a_n vyplývá, že existující čísla $q_1, q_2, \dots, q_{k-2}$ taková, že platí

$$\begin{aligned}
a_1 &= q_1 \cdot a_2 + a_3 \\
a_2 &= q_2 \cdot a_3 + a_4 \\
a_3 &= q_3 \cdot a_4 + a_5 \\
a_4 &= q_4 \cdot a_5 + a_6 \\
&\vdots \\
a_{k-5} &= q_{k-5} \cdot a_{k-4} + a_{k-3} \\
a_{k-4} &= q_{k-4} \cdot a_{k-3} + a_{k-2} \\
a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1} \\
a_{k-2} &= q_{k-2} \cdot a_{k-1} + 0.
\end{aligned}$$

Z poslední rovnosti vyplývá, že $a_{k-1} | a_{k-2}$. Z předposlední rovnosti $a_{k-1} | a_{k-3}$ z další předchozí $a_{k-1} | a_{k-4}$ a podobně. Analogicky se tímto procesem se dostaneme až k třetí rovnosti, kde platí $a_{k-1} | a_3$, u druhé rovnosti platí $a_{k-1} | a_2$ a konečně u první rovnosti platí $a_{k-1} | a_1$.

Člen a_{k-1} je tedy společným dělitelem d čísel a_1, a_2. Společný dělitel d ovšem dělí i čísla $a_3 = a_1 - q_1 \cdot a_2$, $a_4 = a_2 - q_2 \cdot a_3$ a $a_5 = a_3 - q_3 \cdot a_4, \dots$ tím pádem i číslo $a_{k-1} = a_{k-3} - q_{k-3} \cdot a_{k-2}$.

Tímto jsme dokázali, že člen a_{k-1} je největším společným dělitelem D čísel a_1, a_2.

VĚTA BEZOUTOVA – Pro libovolná celá čísla a_1, a_2 existuje jejich největší společný dělitel $D(a_1, a_2)$, přitom ovšem existují ještě čísla k_1, k_2 taková, že platí [6]

$$D(a_1, a_2) = k_1 \cdot a_1 + k_2 \cdot a_2.$$

Tento výraz budeme hledat pomocí Euklidova algoritmu. Výrazu budeme říkat celočíselná kombinace $D(a_1, a_2)$. Hledání oné kombinace bude probíhat tak, že budeme postupně vyjadřovat nalezené zbytky. Přičemž budeme postupovat od zbytku $D(a_1, a_2)$ směrem vzhůru.

DŮKAZ BEZOUTOVY VĚTY:

Větu stačí dokázat pro čísla a_1, a_2 náležící množině přirozených čísel. Jak je patrné, je možné čísla t, u náležící celým číslům vyjádřit ve tvaru $t = t_1a_1 + t_2a_2,\ u = u_1a_1 + u_2a_2$, kde čísla t_1, t_2, u_1, u_2 náleží množině celých čísel. Můžeme je vyjádřit i následovně

$$t + u = (t_1 + u_1)a_1 + (t_2 + u_2)a_2,$$

dále pro libovolné *e* náležící množině celých čísel platí

$$e \cdot t = (e \cdot t_1)a_1 + (e \cdot t_2)a_2.$$

Jelikož $a_1 = 1 \cdot a_1 + 0 \cdot a_2,\ a_2 = 0 \cdot a_1 + 1 \cdot a_2$ plyne z Euklidova algoritmu, že takto lze vyjádřit i členy $a_3 = a_1 + q_1 \cdot a_2,\ a_4 = a_2 + q_2 \cdot a_3, \dots, a_{k-1} = a_{k-3} - q_{k-3} \cdot a_{k-2}$, což je právě onen $D(a_1, a_2)$.

1.1.2 PŘÍKLADY NA VÝPOČET *D* DVOU PŘIROZENÝCH ČÍSEL POMOCÍ EUKLIDOVA ALGORITMU

PŘÍKLAD 1. Pomocí Euklidova algoritmu nalezněte $D(945, 729)$.

$$\begin{aligned} 945 &= 729 \cdot 1 + 216 \\ 729 &= 216 \cdot 3 + 81 \\ 216 &= 81 \cdot 2 + 54 \\ 81 &= 54 \cdot 1 + \mathbf{27} \\ 54 &= 27 \cdot 2 + 0. \end{aligned}$$

Největšího společného dělitele 27 vyjádříme jako celočíselnou kombinaci čísel 945 a 729. Budeme postupně vyjadřovat nalezené zbytky, přičemž budeme postupovat od zbytku 27 směrem vzhůru.

$$\begin{aligned} 27 &= 1 \cdot 81 - 1 \cdot 54 = \\ &= 1 \cdot (1 \cdot 729 - 3 \cdot 216) - 1 \cdot (1 \cdot 216 - 2 \cdot 81) = \\ &= 1 \cdot 729 - 4 \cdot 216 + 2 \cdot 81 = \\ &= 1 \cdot 729 - 4 \cdot (1 \cdot 945 - 1 \cdot 729) + 2 \cdot (1 \cdot 729 - 3 \cdot 216) = \\ &= 7 \cdot 729 - 4 \cdot 945 - 6 \cdot 216 = \\ &= 7 \cdot 729 - 4 \cdot 945 - 6 \cdot (1 \cdot 945 - 1 \cdot 729) = \\ &= 13 \cdot 729 - 10 \cdot 945. \end{aligned}$$

Hledaná celočíselná kombinace je ve tvaru

$$13 \cdot 729 + 945 \cdot (-10) = 27.$$

PŘÍKLAD 2. Pomocí Euklidova algoritmu nalezněte $D(843, 321)$.

$$\begin{aligned} 843 &= 2 \cdot 321 + 216 \\ 321 &= 1 \cdot 201 + 120 \\ 201 &= 1 \cdot 120 + 81 \\ 120 &= 1 \cdot 81 + 39 \\ 81 &= 2 \cdot 39 + \mathbf{3} \\ 39 &= 13 \cdot 3 + 0. \end{aligned}$$

Největšího společného dělitele 3 vyjádříme jako celočíselnou kombinaci čísel 843 a 321

$$\begin{aligned} 3 &= 1 \cdot 81 - 2 \cdot 39 = \\ &= 1 \cdot (1 \cdot 201 - 1 \cdot 120) - 2 \cdot (1 \cdot 120 - 1 \cdot 81) = \\ &= 1 \cdot 201 - 3 \cdot 120 + 2 \cdot 81 = \\ &= 1 \cdot (1 \cdot 843 - 2 \cdot 321) - 3 \cdot (1 \cdot 321 - 1 \cdot 201) + 2 \cdot (1 \cdot 201 - 1 \cdot 120) = \\ &= 1 \cdot 843 - 5 \cdot 321 + 5 \cdot 2012 \cdot 120 = \\ &= 1 \cdot 843 - 5 \cdot 321 + 5 \cdot (1 \cdot 843 - 2 \cdot 321) - 2 \cdot (1 \cdot 321 - 1 \cdot 201) = \\ &= 6 \cdot 843 - 17 \cdot 321 + 2 \cdot 201 = \\ &= 6 \cdot 843 - 17 \cdot 321 + 2 \cdot (1 \cdot 843 - 2 \cdot 321) = \\ &= 8 \cdot 843 - 21 \cdot 321 = \\ &= 8 \cdot 843 + 321 \cdot (-21). \end{aligned}$$

Hledaná celočíselná kombinace je ve tvaru

$$8 \cdot 843 + 321 \cdot (-21) = 3.$$

PŘÍKLAD 3. Pomocí Euklidova algoritmu nalezněte $D(2658, 1788)$.

$$2658 = 1 \cdot 1788 + 870$$
$$1788 = 2 \cdot 870 + 48$$
$$870 = 18 \cdot 48 + \mathbf{6}$$
$$48 = 8 \cdot 6 + 0.$$

Největšího společného dělitele 6 vyjádříme jako celočíselnou kombinaci čísel 2658 a 1788.

$$\begin{aligned} 6 &= 1 \cdot 870 - 18 \cdot 48 = \\ &= 1 \cdot (1 \cdot 2658 - 1 \cdot 1788) - 18 \cdot (1 \cdot 1788 - 2 \cdot 870) = \\ &= 1 \cdot 2658 - 19 \cdot 1788 + 36 \cdot 870 = \\ &= 1 \cdot 2658 - 19 \cdot 1788 + 36 \cdot (1 \cdot 2658 - 1 \cdot 1788) = \\ &= 37 \cdot 2658 - 55 \cdot 1788 = \\ &= 37 \cdot 2658 + 1788 \cdot (-55). \end{aligned}$$

Hledaná celočíselná kombinace je ve tvaru

$$37 \cdot 2658 + 1788 \cdot (-55) = 6.$$

PŘÍKLAD 4. Pomocí Euklidova algoritmu nalezněte $D(3578, 758)$.

$$3578 = 4 \cdot 758 + 546$$
$$758 = 1 \cdot 546 + 212$$
$$546 = 2 \cdot 212 + 122$$
$$212 = 1 \cdot 122 + 90$$
$$122 = 1 \cdot 90 + 32$$
$$90 = 2 \cdot 32 + 26$$
$$32 = 1 \cdot 26 + 6$$
$$26 = 4 \cdot 6 + \mathbf{2}$$
$$6 = 3 \cdot 2 + 0.$$

Největšího společného dělitele 2 vyjádříme jako celočíselnou kombinaci čísel 3578 a 758.

$$
\begin{aligned}
2 &= 1 \cdot 26 - 4 \cdot 6 = \\
&= 1 \cdot (1 \cdot 90 - 2 \cdot 32) - 4 \cdot (1 \cdot 32 - 1 \cdot 26) = \\
&= 1 \cdot 90 - 6 \cdot 32 + 4 \cdot 26 = \\
&= 1 \cdot (1 \cdot 212 - 1 \cdot 122) - 6 \cdot (1 \cdot 122 - 1 \cdot 90) + 4 \cdot (1 \cdot 90 - 2 \cdot 32) = \\
&= 1 \cdot 212 - 7 \cdot 122 + 10 \cdot 90 - 8 \cdot 32 = \\
&= 1 \cdot (1 \cdot 758 - 1 \cdot 576) - 7 \cdot (1 \cdot 546 - 2 \cdot 212) + 10 \cdot (1 \cdot 212 - 1 \cdot 122) - \\
&\quad -8 \cdot (1 \cdot 122 - 1 \cdot 90) = \\
&= 1 \cdot 758 - 8 \cdot 546 + 24 \cdot 212 - 18 \cdot 122 + 8 \cdot 90 = \\
&= 1 \cdot 758 - 8 \cdot (1 \cdot 3578 - 4758) + 24 \cdot (1 \cdot 758 - 1 \cdot 546) - \\
&\quad -18 \cdot (1 \cdot 546 - 2 \cdot 212) + 8 \cdot (1 \cdot 212 - 1 \cdot 122) = \\
&= 57 \cdot 758 - 8 \cdot 3578 - 42 \cdot 546 + 44 \cdot 212 - 8 \cdot 122 = \\
&= 57 \cdot 758 - 8 \cdot 3578 - 42 \cdot (1 \cdot 3578 - 4 \cdot 758) + 44 \cdot (1 \cdot 758 - 1 \cdot 546) - \\
&\quad -8 \cdot (1 \cdot 546 - 2 \cdot 212) = \\
&= 269 \cdot 758 - 50 \cdot 3578 - 52 \cdot 546 + 16 \cdot 212 = \\
&= 269 \cdot 758 - 50 \cdot 3578 - 52 \cdot (1 \cdot 3578 - 4 \cdot 758) + 16 \cdot (1 \cdot 758 - 1 \cdot 546) = \\
&= 493 \cdot 758 - 102 \cdot 3578 - 16 \cdot 546 = \\
&= 493 \cdot 758 - 102 \cdot 3578 - 16 \cdot (1 \cdot 3578 - 4 \cdot 758) = \\
&= 557 \cdot 758 - 118 \cdot 3578 = \\
&= 557 \cdot 758 + 3578 \cdot (-118).
\end{aligned}
$$

Hledaná celočíselná kombinace je ve tvaru

$$557 \cdot 758 + 3578 \cdot (-118) = 2.$$

Největšího společného dělitele dvou prvků a_1, a_2 nemůžeme definovat jako v množině přirozených čísel pomocí rovnosti. Do definice největšího společného dělitele musíme vložit charakteristickou vlastnost. Tato vlastnost zní – *společný dělitel dvou přirozených čísel dělí jejich největšího společného dělitele*.

1.1.3 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL VÍCE ČÍSEL

Největší společný dělitel D čísel $a_1, a_2, a_3, \dots, a_n$ náležící množině celých čísel bude definován úplně stejným způsobem, jako tomu bylo u dvou prvků a_1, a_2. Libovolnému číslu d, které splňuje podmínky, že $d|a_1, d|a_2, \dots, d|a_n$ budeme říkat společný dělitel prvků $a_1, a_2, a_3, \dots, a_n$. Společný dělitel $d \geq 0$ čísel $a_1, a_2, a_3, \dots, a_n$, který je dělitelný libovolným společným dělitelem těchto čísel, se nazývá největším společným dělitelem D čísel $a_1, a_2, a_3, \dots, a_n$. Navíc platí, že společný dělitel dělí největšího společného dělitele $d|D$.

Společného dělitele d prvků $a_1, a_2, a_3, \dots, a_n$ budeme značit

$$d(a_1, a_2, a_3, \dots, a_n).$$

Největšího společného dělitele D prvků $a_1, a_2, a_3, \dots, a_n$ budeme značit

$$D(a_1, a_2, a_3, \dots, a_n).$$

1.1.4 PŘÍKLADY NA VÝPOČET D DVOU KOMPLEXNÍCH ČÍSEL

Pojem Gaussovo celé číslo znamená v teorii čísel takové komplexní číslo, jehož reálnou i imaginární složku tvoří jen celá čísla.

Ke každým dvěma nenulovým Gaussovým číslům α, β existují Gaussova čísla η, ν taková, že platí

$$(1)\ \alpha = \beta \cdot \eta + \nu, \text{ kde } N(\nu) < N(\beta).$$

DŮKAZ:

1. Vypočítáme podíl čísel $\frac{\alpha}{\beta} = A + B \cdot i$. (A, B) mohou být i racionální čísla.

2. Vzniknou celá čísla x, y , pro která platí

$$(2)\ |A - x| \leq \frac{1}{2} \wedge |B - y| \leq \frac{1}{2}.$$

3. Sestrojíme Gaussova celá čísla

$$(3)\ \eta = x + y \cdot i \wedge \nu = \alpha - \beta \cdot \eta.$$

4. Stačí již dokázat, že platí $N(\nu) < N(\beta)$.

Platí vztah

$$(4)\ \nu = \alpha - \beta \cdot \eta = \beta \cdot \left(\frac{\alpha}{\beta} - \eta\right).$$

Přechodem k normám dostaneme z předešlého řádku

$$(5)\ N(\nu) = N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \eta\right).$$

Už jen dokážeme, že $N\left(\frac{\alpha}{\beta} - \eta\right) \leq \frac{1}{2}$. Následně bude platit

$$(6)\ \frac{\alpha}{\beta} - \eta = A + B \cdot i - (x + y \cdot i) = (A - x) + (B - y) \cdot i.$$

Pro normu platí $N\left(\frac{\alpha}{\beta} - \eta\right)$ [2]

$$N\left(\frac{\alpha}{\beta} - \eta\right) = (A - x)^2 + (B - y)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Tímto jsme větu bez problémů dokázali.

Pokud bude výraz $N(\nu)$ nenulový, proces zopakujeme pro dvojici Gaussových celých čísel β, ν. Jelikož se stávající normy Gaussových čísel postupně snižují, tak postup stále opakujeme, až se dostaneme k nulové hodnotě. Dále již z předchozí kapitoly víme, že poslední získaný **nenulový** zbytek představuje největšího společného dělitele.

PŘÍKLAD 5. Nalezněte $D(24 + 24i,\ 6 - 8i)$.

Platí tedy

$$(7)\ \alpha = 24 + 24i \wedge \beta = 6 - 8i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{24 + 24i}{6 - 8i} = \frac{24 + 24i}{6 - 8i} \cdot \frac{6 + 8i}{6 + 8i} = \frac{144 + 192i + 144i + 192i^2}{36 - 64i^2} =$$
$$= \frac{-48 + 36i}{100} = \frac{-48}{100} + \frac{336i}{100} = -\mathbf{\frac{12}{25}} + \mathbf{\frac{84}{25}}\boldsymbol{i}.$$

Platí tedy

$$(8)\ A = -\frac{12}{25} \wedge B = \frac{84}{25}.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(9) x = 0 \ \wedge y = 3\ tj. \eta = 3i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(10)\ \nu &= \alpha - \beta \cdot \eta = (24 + 24i) - [3i \cdot (6 - 8i)] = \\ &= 24 + 24i - 18i + 24i^2 = \\ &= 24 + 24i - 18i - 24 = \\ &= \boldsymbol{6i}.\end{aligned}$$

Celkově dostáváme

$$(11)\ \ 24 + 24i = \left[\overbrace{(6 - 8i)}^{\beta} \cdot \overbrace{3i}^{\eta}\right] + \overbrace{6i}^{\nu}.$$

Celý postup zopakujeme pro

$$(12)\ \alpha = 6 - 8i \ \wedge \beta = 6i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{6 - 8i}{6i} = \frac{6 - 8i}{6i} \cdot \left(\frac{-6i}{-6i}\right) = \frac{-36i + 48i^2}{-36i^2} = \frac{-36i - 48}{36} = \frac{-36i}{36} - \frac{48}{36} =$$
$$= -i - \frac{4}{3} = -\frac{\boldsymbol{4}}{\boldsymbol{3}} - \boldsymbol{i}.$$

Platí tedy

$$(13)\ \alpha = -\frac{4}{3} \wedge \beta = -1.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(14)\ x = -1 \ \wedge y = -1\ \text{tj.}\ \eta = -1 - i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(15)\ \nu &= \alpha - \beta \cdot \eta = (6 - 8i) - [(1 - i) \cdot 6i] = \\ &= (6 - 8i) - (-6i - 6i^2) =\end{aligned}$$

$$= 6 - 8i + 6i - 6i^2 =$$
$$= \mathbf{-2i}.$$

Celkově dostáváme

$$(16)\ \overbrace{6-8i}^{\beta} = \left[\overbrace{6i}^{\nu} \cdot \overbrace{(-1-i)}^{\eta}\right] - \overbrace{2i}^{\nu}.$$

Celý postup zopakujeme pro

$$(17)\ \alpha = 6i \ \wedge\ \beta = -2i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{6i}{-2i} = \frac{6i}{-2i} \cdot \frac{2i}{2i} = \frac{12i^2}{-4i^2} = \frac{-12}{4} = \mathbf{-3}.$$

Celkově dostáváme

$$(18)\ \overbrace{6i}^{\nu} = \left[\overbrace{-2i}^{\nu} \cdot \left(\overbrace{-3}^{\frac{\alpha}{\beta}}\right)\right] + 0.$$

Řádky (11), (16) a (18) představují schéma odpovídajícího Euklidova algoritmu, v němž nenulový zbytek na (16) řádku představuje největšího společného dělitele. Platí tedy

$$(19)\ D(24 + 24i, 6 - 8i) = \mathbf{-2i}.$$

PŘÍKLAD 6. Nalezněte $D(12 - 16i,\ 10 + 2i)$.

Platí tedy

$$(20)\ \alpha = 12 - 16i \wedge \beta = 10 + 2i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{12 - 16i}{10 + 2i} = \frac{12 - 16i}{10 + 2i} \cdot \frac{10 - 2i}{10 - 2i} = \frac{120 - 24i - 160i + 32i^2}{100 - 4i^2} =$$
$$= \frac{88 - 184i}{104} = \frac{11}{13} - \frac{23i}{13} = \mathbf{\frac{11}{13} - \frac{23}{13}i}.$$

Platí tedy

$$(21)\ A = \frac{11}{13} \wedge B = -\frac{23}{13}.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(22) x = 1 \wedge y = -2i \text{ tj. } \eta = 1 - 2i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(23)\ \nu &= \alpha - \beta \cdot \eta = (12 - 16i) - [(10 + 2i) \cdot (1 - 2i)] = \\ &= (12 - 16i) - (14 - 18i) = \\ &= \mathbf{-2 + 2i}.\end{aligned}$$

Celkově dostáváme

$$(24)\ 12 - 16i = [(10 + 2i) \cdot (1 - 2i)] + (-2 + 2i).$$

Celý postup zopakujeme pro

$$(25)\ \alpha = 10 + 2i \wedge \beta = -2 + 2i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{10 + 2i}{-2 + 2i} = \frac{10 + 2i}{-2 + 2i} \cdot \left(\frac{-2 - 2i}{-2 - 2i}\right) = \frac{-20 - 20i - 4i - 4i^2}{4 - 4i^2} = \frac{-16 - 24i}{4 + 4} = \\ &= \frac{-16 - 24i}{8} = -\frac{16}{8} - \frac{24}{8}i = \mathbf{-2 - 3i}.\end{aligned}$$

Platí tedy

$$(26) \alpha = -2 \wedge \beta = -3i.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(27)\ x = -2 \wedge y = -3i \text{ tj. } \eta = -2 - 3i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(28)\ \nu &= \alpha - \beta \cdot \eta = (10 + 2i) - 2 + [2i \cdot (-2 - 3i)] = \\ &= (10 + 2i) - (4 + 6i - 4i - 6i^2) = \\ &= 10 + 2i - 4 - 6i + 4i + 6i^2 = \\ &= \mathbf{0}.\end{aligned}$$

Celkově dostáváme

$$(29)\ 10 + 2i = (-2 + 2i) \cdot (-2 - 3i) + 0.$$

Řádky (24) a (29) představují schéma odpovídajícího Euklidova algoritmu, v němž nenulový zbytek na (24) řádku představuje největšího společného dělitele. Platí tedy

$$(30)\ D(12 - 16,\ 10 + 2i) = \mathbf{-2 + 2i.}$$

PŘÍKLAD 7. Nalezněte $D(7 + i,\ i)$.

Platí tedy

$$(31)\ \alpha = 7 + i \wedge \beta = i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{7 + i}{i} = \frac{7 + i}{i} \cdot \left(\frac{-i}{-i}\right) = \frac{-7i - i^2}{-i^2} = \frac{-7i + 1}{1} = \mathbf{-7i + 1}.$$

Platí tedy

$$(32)\ A = 1\ \wedge B = -7.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(33) x = 1\ \wedge y = -7\ tj.\ \eta = 1 - 7i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(34)\ \nu &= \alpha - \beta \cdot \eta = (7 + i) - [i \cdot (1 - 7i)] = \\ &= 7 + i - i + 7i^2 = \\ &= \mathbf{0}.\end{aligned}$$

Celkově dostáváme

$$(35)\ 7 + i = [i \cdot (1 - 7i)] + 0.$$

Řádek (35) je schématem Euklidova algoritmu.

$$(36)\ D(7 + i,\ i) = \boldsymbol{i.}$$

PŘÍKLAD 8. Nalezněte $D(10-3i,\ 5-2i)$.

Platí tedy

$$(37)\ \alpha = 10-3i \wedge \beta = 5-2i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{10-3i}{5-2i} = \frac{10-3i}{5-2i}\cdot\frac{5+2i}{5+2i} = \frac{50+20i-15i-6i^2}{25-4i^2} = \frac{56+5i}{29} =$$
$$= \frac{56}{29} + \frac{5i}{29} = \mathbf{\frac{56}{29} + \frac{5}{29}i}.$$

Platí tedy

$$(38)\ A = \frac{56}{29} \wedge B = \frac{5}{29}.$$

2. Stanovíme číslo $\eta = x + y\cdot i$. Bude platit

$$(39)\ x = 2\ \wedge y = 0\ tj.\ \eta = 2.$$

3. Stanovíme číslo v. Bude platit

$$(40)\ v = \alpha - \beta\cdot\eta = (10-3i) - [2\cdot(5-2i)] =$$
$$= 10-3i-10+4i =$$
$$= \boldsymbol{i}.$$

Celkově dostáváme

$$(41)\ 10-3i = [(5-2i)\cdot 2] + i.$$

Celý postup zopakujeme pro

$$(42)\ \alpha = 5-2i\ \wedge \beta = i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{5-2i}{i} = \frac{5-2i}{i}\cdot\left(\frac{-i}{-i}\right) = \frac{-5i+2i^2}{-i^2} = \frac{-5i-2}{1} = -5i-2 =$$
$$= \mathbf{-2-5i}.$$

Platí tedy

$$(43)\ \alpha = -2\ \wedge \beta = -5.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(44)\ x = -2 \ \wedge y = -5 \text{ tj. } \eta = -2 - 5i.$$

3. Stanovíme číslo ν. Bude platit

$$\begin{aligned}(45)\ \nu = \alpha - \beta \cdot \eta &= (5 - 2i) - [(-2 - 5i) \cdot i] = \\ &= 5 - 2i + 2i + 5i^2 = \\ &= \mathbf{0}.\end{aligned}$$

Celkově dostáváme

$$(46)\ 5 - 2i = [i \cdot (-2 - 5i)] + 0.$$

Řádky $(41), (46)$ jsou schématem Euklidova algoritmu, v němž nenulový zbytek na (40) řádku představuje největšího společného dělitele. Platí tedy

$$(47)\ D(10 - 3i,\ 5 - 2i) = \boldsymbol{i}.$$

PŘÍKLAD 9. Nalezněte $D(16 + 16i,\ 7 - 9i)$.

Platí tedy

$$(48)\ \alpha = 16 + 16i \wedge \beta = 7 - 9i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\begin{aligned}\frac{\alpha}{\beta} = \frac{16 + 16i}{7 - 9i} = \frac{16 + 16i}{7 - 9i} \cdot \frac{7 + 9i}{7 + 9i} = \frac{112 + 144i + 112i + 144i^2}{49 - 81i^2} = \\ = \frac{-32 + 256i}{130} = \frac{-32}{130} + \frac{256i}{130} = -\frac{\mathbf{16}}{\mathbf{65}} + \frac{\mathbf{128}}{\mathbf{65}}\boldsymbol{i}.\end{aligned}$$

Platí tedy

$$(49)\ A = -\frac{16}{65} \wedge B = \frac{128}{65}.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(50) x = 0 \ \wedge y = 2 \text{ tj.} \eta = 2i.$$

3. Stanovíme číslo ν. Bude platit

$$(51)\ \nu = \alpha - \beta \cdot \eta = (16 + 16i) - [2i \cdot (7 - 9i)] =$$
$$= 16 + 16i - 14i + 18i^2 =$$
$$= 16 + 16i - 14i - 18 =$$
$$= \mathbf{-2 + 2i}.$$

Celkově dostáváme

$$(52)\ 16 + 16i = [(7 - 9i) \cdot 2i] + (-2 + 2i).$$

Celý postup zopakujeme pro

$$(53)\ \alpha = 7 - 9i\ \wedge \beta = -2 + 2i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{7 - 9i}{-2 + 2i} = \frac{7 - 9i}{-2 + 2i} \cdot \left(\frac{-2 - 2i}{-2 - 2i}\right) = \frac{-14 - 14i + 18i + 18i^2}{4 - 4i^2} = \frac{-32 + 2i}{8} =$$
$$= \frac{-32}{8} - \frac{2i}{8} = -4 - \frac{1i}{4} = \mathbf{-4 - \frac{i}{4}}.$$

Platí tedy

$$(54)\ \alpha = -4\ \wedge \beta = 0.$$

2. Stanovíme číslo $\eta = x + y \cdot i$. Bude platit

$$(55)\ x = -4\ \wedge y = 0 \text{ tj. } \eta = -4.$$

3. Stanovíme číslo ν. Bude platit

$$(56)\ \ \nu = \alpha - \beta \cdot \eta = [(7 - 9i) - (-4)] \cdot (-2 + 2i) =$$
$$= 7 - 9i - 8 + 8i =$$
$$= \mathbf{-1 - i}.$$

Celkově dostáváme

$$(57)\ 7 - 9i = [(-2 + 2i) \cdot (-4)] + (-1 - i).$$

Celý postup zopakujeme pro

$$(58)\ \alpha = -2 + 2i\ \wedge\ \beta = -1 - i.$$

1. Stanovíme podíl $\frac{\alpha}{\beta}$

$$\frac{\alpha}{\beta} = \frac{-2+2i}{-1-i} = \frac{-2+2i}{-1-i} \cdot \left(\frac{-1+i}{-1+i}\right) = \frac{2-2i-2i+2i^2}{1-i^2} = \frac{-4i}{2} = \mathbf{-2i}.$$

Celkově dostáváme

$$(59)\ -2+2i = [(-1-i)\cdot(-2i)] + 0.$$

Řádky $(52), (57)$ *a* (59) jsou schématem Euklidova algoritmu, v němž nenulový zbytek na (57) řádku představuje největšího společného dělitele. Platí tedy

$$(60)\ D(16+16i,\ 7-9i) = \mathbf{-1-i}.$$

1.2 NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Jsou dána čísla a_1, a_2, N náležící množině celých čísel. Pro číslo N platí, že $a_1|N$ a $a_2|N$, pokud tyto podmínky číslo N splňuje, říkáme, že číslo N je společným násobkem čísel a_1, a_2. Společný násobek $N \geq 0$ čísel a_1, a_2, který je libovolným společným násobkem čísel a_1, a_2 se nazývá nejmenším společným násobkem n čísel a_1, a_2. Samozřejmě platí, že nejmenší společný násobek musí vždy dělit společný násobek $n|N$.

Společný násobek čísel a_1, a_2 budeme zapisovat ve tvaru

$$N(a_1, a_2).$$

Pro nejmenší společný násobek čísel a_1, a_2 nutně musí platit

$$n(a_1, a_2) = \min N(a_1, a_2).$$

Nejmenší společný násobek čísel a_1, a_2 budeme zapisovat ve tvaru

$$n(a_1, a_2).$$

Množinu všech společných násobků budeme zapisovat ve tvaru

$$N(a_1, a_2) = N(a_1) \cap N(a_2).$$

Pro libovolná dvě čísla a_1, a_2 existuje nejmenší společný násobek $n(a_1, a_2)$ a platí

$$\boldsymbol{D(a_1, a_2)\cdot\ n(a_1, a_2) = a_1 \cdot a_2}.$$

DŮKAZ: Věta určitě platí, je-li jedno z čísel rovno nule. Pokud bude jedno číslo kladné a druhé záporné, pak se bude pravá strana rovnosti lišit právě o ono znaménko. Použijeme

tedy pro pravou stranu rovnosti absolutní hodnotu. Jelikož znaménko při hledání D nehraje roli, je možno důkaz omezit jen na kladná čísla. Čísla záporná jsou ošetřena právě onou absolutní hodnotou. Předpokládáme tedy, že obě čísla a_1, a_2 jsou nenulová a navíc kladná. Důkaz bude hotov tehdy, když dokážeme, že $n(a_1, a_2) = \left|\frac{a_1 \cdot a_2}{D(a_1,a_2)}\right|$ je nejmenším společným násobkem čísel a_1, a_2. Jelikož $D(a_1, a_2)$ je společným dělitelem čísel a_1, a_2, jsou také výrazy $\frac{a_1}{D(a_1,a_2)}$, $\frac{a_2}{D(a_1,a_2)}$ celá čísla, a proto výraz

$$n = \left|\frac{a_1 \cdot a_2}{D(a_1, a_2)}\right| = \left|\frac{a_1}{D(a_1, a_2)} \cdot a_2\right| = \left|\frac{a_2}{D(a_1, a_2)} \cdot a_1\right|$$

je společným násobkem čísel a_1, a_2.

DŮKAZ DĚLITELNOSTI $n|N$ POMOCÍ BEZOUTOVY VĚTY.

Bezoutova věta říká, že existují koeficienty k_1, k_2 náležící množině celých čísel pro která platí

$$D(a_1, a_2) = k_1 \cdot a_1 + k_2 \cdot a_2.$$

Budeme předpokládat, že N je libovolný společný násobek čísel a_1, a_2 a ukážeme si, že je dělitelný nejmenším společným násobkem n. Bude tedy platit, že $N|a_1$ a $N|a_2$ a proto lze napsat

$$\frac{N}{a_2} k_1 + \frac{N}{a_1} k_2 = \frac{N(k_1 \cdot a_1 + k_2 \cdot a_2)}{a_1 \cdot a_2} = \frac{N(a_1 \cdot a_2)}{a_1 \cdot a_2} = \frac{N}{n}.$$

Tímto jsme dokázali, že nejmenší společný násobek vždy dělí společný násobek $n|N$.

1.2.1 NEJMENŠÍ SPOLEČNÝ NÁSOBEK VÍCE PRVKŮ

Nejmenší společný násobek n čísel $a_1, a_2, a_3, \dots, a_n$ náležící množině celých čísel bude definován úplně stejným způsobem, jako tomu bylo u dvou prvků a_1, a_2. Libovolnému číslu N, které splňuje podmínky, že $a_1|N, a_2|N, \dots, a_n|N$ budeme říkat společný násobek prvků $a_1, a_2, a_3, \dots, a_n$. Společný násobek $N \geq 0$ čísel $a_1, a_2, a_3, \dots, a_n$, který je dělitelný libovolným společným násobkem těchto čísel, se nazývá nejmenším společným násobkem n čísel $a_1, a_2, a_3, \dots, a_n$.

Společný násobek N prvků $a_1, a_2, a_3, \dots, a_n$ budeme značit

$$N(a_1, a_2, a_3, \dots, a_n).$$

Nejmenší společný násobek n prvků $a_1, a_2, a_3, \dots, a_n$ budeme značit

$$n(a_1, a_2, a_3, \dots, a_n).$$

Samozřejmě i v tomto případě platí, že nejmenší společný násobek musí vždy dělit společný násobek $n|N$.

1.2.2 PŘÍKLADY NA VÝPOČET n DVOU PŘIROZENÝCH, KOMPLEXNÍCH ČÍSEL

PŘÍKLAD 10. Nalezněte nejmenší společný násobek čísel 945 a 729.

$$\begin{aligned} 945 &= 729 \cdot 1 + 216 \\ 729 &= 216 \cdot 3 + 81 \\ 216 &= 81 \cdot 2 + 54 \\ 81 &= 54 \cdot 1 + \mathbf{27} \\ 54 &= 27 \cdot 2 + 0. \end{aligned}$$

Z Euklidova algoritmu jsme zjistili, že

$$D(945, 729) = \mathbf{27}.$$

Největší společný násobek n$(945, 729)$ nalezneme pomocí vztahu

$$\begin{aligned} n(a_1, a_2) &= (a_1 \cdot a_2) : D(a_1, a_2)[1] = \\ &= (945 \cdot 729) : 27 = \\ &= 688\,905 : 27 = \\ &= \mathbf{25\,515}. \end{aligned}$$

Pro zadaná čísla platí $n(945, 729) = 25\,515$.

[1] Vzorec $n(a_1, a_2) = (a_1 \cdot a_2) : D(a_1, a_2)$ zjednodušíme (zpřehledníme) u dalších příkladů na tvar $n = (a_1 \cdot a_2) : D$.

PŘÍKLAD 11. Nalezněte nejmenší společný násobek čísel $n(24+24i,\ 6-8i)$.

Z příkladu 5 v této kapitole jsme pomocí Euklidova algoritmu zjistili, že $D(24+24i,\ 6-8i)$ je číslo $-2i$.

Naším úkolem je najít nejmenší společný násobek $n(24+24i,\ 6-8i)$.

Použijeme vztah

$$n=(a_1\cdot a_2):\ D=\frac{a_1\cdot a_2}{D},$$

dosadíme

$$n=\frac{a_1\cdot a_2}{D}=\frac{(24+24i)\cdot(6-8i)}{-2i}=\frac{144-192i+144i-192i^2}{-2i}=$$
$$=\frac{336-48i}{-2i}\cdot\frac{2i}{2i}=\frac{672i-96i^2}{-4i^2}=\frac{96+672i}{4}=\mathbf{24+168i}.$$

Nejmenší společný násobek je $n(24+24i,\ 6-8i)=\mathbf{24+168i}$.

PŘÍKLAD 12. Nalezněte nejmenší společný násobek čísel $n=(12-16i,\ 10+2i)$.

Z příkladu 6 v této kapitole jsme pomocí Euklidova algoritmu zjistili, že $D(12-16i,10+2i)$ je číslo $-2+2i$.

Naším úkolem je najít nejmenší společný násobek $n(12-16i,\ 10+2i)$.

Použijeme vztah

$$n=(a_1\cdot a_2):\ D=\frac{a_1\cdot a_2}{D},$$

dosadíme

$$n=\frac{a_1\cdot a_2}{D}=\frac{(12-16i)\cdot(10+2i)}{-2+2i}=\frac{120+24i-160i-32i^2}{-2+2i}=$$
$$=\frac{152-136i}{-2+2i}\cdot\frac{(-2-2i)}{(-2-2i)}=\frac{(-304-304i+272i+272i^2)}{4-4i^2}=$$
$$=\frac{(-576-32i)}{8}=\mathbf{-72-4i}.$$

Nejmenší společný násobek je $n(12-16i,\ 10+2i)=\mathbf{-72-4i}$.

PŘÍKLAD 13. Nalezněte nejmenší společný násobek čísel $n = (7 + i,\ i)$.

Z příkladu 7 v této kapitole jsme pomocí Euklidova algoritmu zjistili, že $D(7 + i,\ i)$ je číslo i.

Naším úkolem je najít nejmenší společný násobek $n(24 + 24i,\ 6 - 8i)$.

Použijeme vztah

$$n = (a_1 \cdot a_2) : D = \frac{a_1 \cdot a_2}{D},$$

dosadíme

$$n = \frac{a_1 \cdot a_2}{D} = \frac{(7 + i) \cdot i}{i} = \mathbf{7 + i}.$$

Nejmenší společný násobek je $n = (7 + i,\ i) = \mathbf{7 + i}$.

PŘÍKLAD 14. Nalezněte nejmenší společný násobek čísel $n = (10 - 3i,\ 5 - 2i)$.

Z příkladu 8 v této kapitole jsme pomocí Euklidova algoritmu zjistili, že $D(10 - 3i,\ 5 - 2i)$ je číslo i.

Naším úkolem je najít nejmenší společný násobek $n(24 + 24i,\ 6 - 8i)$.

Použijeme vztah

$$n = (a_1 \cdot a_2) : D = \frac{a_1 \cdot a_2}{D},$$

dosadíme

$$n = \frac{a_1 \cdot a_2}{D} = \frac{(10 - 3i) \cdot (5 - 2i)}{i} = \frac{50 - 20i - 15i + 6i^2}{i} =$$
$$= \frac{44 - 35i}{i} \cdot \frac{(-i)}{(-i)} = \frac{-44i + 35i^2}{-i^2} = \mathbf{-35 - 44i}.$$

Nejmenší společný násobek je $\boldsymbol{n}(24 + 24i,\ 6 - 8i) = \mathbf{-35 - 44i}$.

PŘÍKLAD 15. Nalezněte nejmenší společný násobek čísel $n = (16 + 16i,\ 7 - 9i)$.

Z příkladu 9 v této kapitole jsme pomocí Euklidova algoritmu zjistili, že $D(16 + 16i,\ 7 - 9i)$ je číslo $-1 - i$.

Naším úkolem je najít nejmenší společný násobek $n(24 + 24i,\ 6 - 8i)$.

Použijeme vztah

$$n = (a_1 \cdot a_2) : D = \frac{a_1 \cdot a_2}{D},$$

dosadíme

$$n = \frac{a_1 \cdot a_2}{D} = \frac{(16 + 16i) \cdot (7 - 9i)}{-1 - i} = \frac{112 - 144i + 112i - 144i^2}{-1 - i} =$$
$$= \frac{256 - 32i}{-1 - i} \cdot \frac{(-1 + i)}{(-1 + i)} = \frac{-256 + 256i + 32i - 32i^2}{1 - i^2} =$$
$$= \frac{(-224 + 288i)}{2} = \mathbf{-112 + 144i}.$$

Nejmenší společný násobek je $n(24 + 24i,\ 6 - 8i) = \mathbf{-112 + 144i}$.

1.3 DĚLITELNOST POLYNOMŮ

Polynom neboli mnohočlen je výraz sestávající jen z koeficientů, součtů, rozdílů, násobků a celočíselných mocnin proměnných. Obecný polynom může vypadat třeba takto

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0, \text{ kde } a_n \neq 0.$$

Polynom nazýváme polynomem n-tého stupně o jedné proměnné x.

Prvky $a_n, a_{n-1}, \ldots\ a_1, a_0$ nazýváme koeficienty polynomu.

Polynomem nultého stupně rozumíme polynom

$$f(x) = a_0, \text{ kde } a_0 \neq 0.$$

Nulový polynom $f(x) = 0$, který budeme značit $o(x)$, nemá stupeň.

Pokud se polynomy $f(x)$ a $g(x)$ se sobě rovnají, zapisujeme $f(x) = g(x)$ právě tehdy, když $(\forall a \in T)$: $f(a) = g(a)$. Můžeme říct, že dva polynomy se sobě rovnají právě tehdy, když se sobě rovnají odpovídající si koeficienty v těchto polynomech.

DŮKAZ: Budeme předpokládat, že máme dva polynomy, které se sobě rovnají. Současně existuje dvojice odpovídajících si koeficientů, které se sobě nerovnají. Potom by jejich rozdílem byl polynom alespoň nultého stupně, který by měl všechna čísla z příslušného číselného tělesa za své nulové body. T_0 znamená, že by existovala algebraická rovnice mající všechna čísla z číselného tělesa T za své kořeny, což není možné.

Důležitým důsledkem důkazu je, že nulový polynom je nulovým polynomem právě tehdy, když jsou všechny jeho koeficienty rovny nule. [1]

1.3.1 DĚLENÍ POLYNOMU POLYNOMEM

Jsou dány dva polynomy $f(x)$ a $g(x)$, kde polynom $g(x)$ je nenulový. Pak existují polynomy $r(x)$ a $z(x)$ takové, že pro ně platí

$$f(x) = r(x)g(x) + z(x),$$

pro stupně polynomů platí st $z <$ st g.

Polynomu $r(x)$ budeme říkat částečný podíl. Polynom $z(x)$ se nazývá zbytkem při dělení polynomu $f(x)$ polynomem $g(x)$.

1.3.2 POSTUP PŘI DĚLENÍ POLYNOMŮ

Polynomy $r(x)$ a $z(x)$ najdeme jednoduchým způsobem. Budeme postupovat, jako kdybychom dělili reálné polynomy, avšak nebudeme používat pojem dělení prvkem, ale budeme používat násobení inverzním prvkem.

Dělení vypadá následovně: jsou zadány dva polynomy $f(x)$ a $g(x)$

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ a

$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$, kde $b_m \neq 0$,

stupeň polynomu $f(x)$ je n a polynomu $g(x)$ je m. [1]

Pokud budeme předpokládat, že pro stupně polynomů platí nerovnost $n < m$, tak $f(x) = 0g(x) + f(x)$, st $f <$ st g. Polynomy $r(x)$ a $z(x)$ potom vypadají následovně $r(x) = 0$ a $z(x) = f(x)$.

Pokud budeme předpokládat, že pro stupně polynomů platí nerovnost st $n \geq$ st m, pak vezmeme členy polynomů s největší mocninou tj. $a_n x^n$ a $b_m x^m$. Výraz $a_n x^n$ vydělíme výrazem $b_m x^m$. Podíl bude roven výrazu $a_n b_m^{-1} x^{n-m}$. Polynom $a_n b_m^{-1} x^{n-m} \cdot g(x)$ bude polynomem stupně n. Koeficient bude u nejvyšší mocniny a_n.

Následně vznikne polynom

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x).$$

Pro polynom $h(x)$ nutně platí, že stupeň polynomu je ostře menší než stupeň n.

Nyní mohou nastat dva případy:

1. **st $\boldsymbol{h} <$ st $\boldsymbol{g}$** částečný podíl je $r(x) = a_n b_m^{-1} x^{n-m}$, zbytek při dělení je $z(x) = h(x)$.
2. **st $\boldsymbol{h} \geq$ st $\boldsymbol{g}$** a částečný podíl při dělení polynomu $f(x)$ polynomem $g(x)$ je roven součtu $a_n b_m^{-1} x^{n-m}$ a částečného podílu při dělení polynomu $h(x)$ polynomem $g(x)$. Zbytek při dělení obou polynomů je stejný jako zbytek při dělení $h(x)$ polynomem $g(x)$.

Jestliže je zbytek při dělení polynomu $f(x)$ polynomem $g(x)$ nulový. Potom říkáme, že polynom $g(x)$ dělí polynom $f(x)$ beze zbytku.

1.3.3 KOŘEN POLYNOMU

Nechť $f(x)$ je polynom, číslo $c \in N$ nazveme kořenem polynomu $f(x)$, jestliže platí $f(c) = 0$. Hodnotou polynomu $f(x)$ v bodě $b \in N$ rozumíme číslo $f(b)$.

Kořen c polynomu $f(x)$ je k-násobný, kde $k \in N$, jestliže je $f(x)$ dělitelný $(x - c)^k$, ale není dělitelný $(x - c)^{k+1}$.

1.3.4 IREDUCIBILNÍ POLYNOM

Polynom $f(x)$ se nazývá ireducibilním polynomem, jestliže se polynom $f(x)$ nedá napsat jakou součin dvou polynomů menšího stupně než je $f(x)$.

1.3.5 VLASTNOSTI DĚLITELNOSTI

- Jestliže polynom $g|f$ a polynom $f|h$, potom platí, že polynom $g|h$.
- Jestliže polynom $h|f$ a polynom $h|g$, potom platí, že polynom $h|(f \pm g)$.
- Jestliže polynom $h|f$ a polynom $g(x)$ je libovolný polynom, potom polynom $h|(f \cdot g)$.
- Každý polynom je dělitelný polynomem nultého stupně.
- Jestliže polynom $h|f$ a $c \in N$, potom $(c \cdot h)|h$.
- Děliteli polynomu $f(x)$ stejného stupně jako $f(x)$ jsou všechny polynomy tvaru $c \cdot f(x), c \in N$.
- Polynomy jsou vzájemně dělitelné, jestliže pro nějaké $c \in N$ je $g(x) = c \cdot f(x)$.
- Každý z dělitelů polynomů $f(x)$ a $c \cdot f(x)$ je dělitelem i druhého polynomu.

1.3.6 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL DVOU POLYNOMŮ

Jsou dány dva polynomy $f(x)$ a $g(x)$. Polynom $D(x)$ se nazývá největším společným dělitelem polynomů $f(x)$ a $g(x)$, jestliže splňuje následující podmínky

1. $D(x)$ dělí oba polynomy $f(x)$ a $g(x)$,
2. jestliže společný dělitel polynomů $f(x)$ a $g(x)$ polynom $d(x)$ dělí polynomy $f(x)$ a $g(x)$, pak polynom $d(x)$ dělí i $D(x)$.

Definice lze použít pro libovolný počet polynomů.

1.3.7 NEJMENŠÍ SPOLEČNÝ NÁSOBEK DVOU POLYNOMŮ

Jsou dány dva polynomy $f(x)$ a $g(x)$. Polynom $n(x)$ se nazývá nejmenším společným násobkem polynomů $f(x)$ a $g(x)$, jestliže splňuje následující podmínky

1. $n(x)$ dělí oba polynomy $f(x)$ a $g(x)$,

2. jestliže společný dělitel polynomů $f(x)$ a $g(x)$ polynom $N(x)$ dělí polynomy $f(x)$ a $g(x)$, pak polynom $n(x)$ dělí i $N(x)$.

Definice lze použít pro libovolný počet polynomů.

BEZOUTOVA VĚTA: Nechť $f(x), g(x)$ jsou polynomy a $h(x)$ jejich největším společným dělitelem. Potom existují polynomy $u(x), v(x)$ takové, že platí
$f(x) \cdot u(x) + g(x) \cdot v(x) = h(x)$.

Speciálně, jsou-li $f(x),\ g(x)$ nesoudělné, potom $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$. [6]

V další části se budeme zabývat příklady na hledání největšího společného dělitele a nejmenšího společného násobku dvou polynomů.

D a n budeme hledat úplně stejným způsobem, jako tomu bylo u dvou čísel přirozených i čísel komplexních.

1.3.8 PŘÍKLADY NA VÝPOČET D A n DVOU POLYNOMŮ

PŘÍKLAD 16. Najděte pomocí Euklidova algoritmu největší společný dělitel polynomů $f(x)$ a $g(x)$ a poté jejich nejmenší společný násobek.

$$f(x) = x^4 - 2x^2 + 1$$
$$g(x) = x^3 + 3x^2 - x - 3.$$

Naším prvním úkolem je najít $D\big(f(x),\ g(x)\big)$:

Provedeme dělení polynomu polynomem

$$(x^4 - 2x^2 + 1) : (x^3 + 3x^2 - x - 3) = x - 3 + \frac{\overbrace{8x^2 - 8}^{\text{Zbytek } R(x)}}{x^3 + 3x^2 - x - 3}.$$

$$\underline{-x^4 - 3x^3 + x^2 + 3x}$$
$$-3x^3 - x^2 + 3x + 1$$
$$\underline{3x^3 + 9x^2 - 3x - 9}$$
$$8x^2 - 8$$

Dostáváme

$$f(x) = g(x) \cdot \overbrace{(x-3)}^{Q(x)} + \overbrace{\Big(\underbrace{8x^2-8}_{\to x^2-1}\Big)}^{R(x)}.$$

Provedeme další dělení

$$\begin{array}{l} (x^3+3x^2-x-3) : (x^2-1) = x+3. \\ \underline{-x^3 \qquad +x} \\ \qquad 3x^2 \quad -3 \\ \quad \underline{-3x^2 \qquad +3} \\ \qquad\qquad\quad 0 \end{array}$$

Dostáváme

$$g(x) = (x^2-1) \cdot (x+3) + 0.$$

Největším společným dělitelem $D\big(f(x),\ g(x)\big) = R(x) = \boldsymbol{x^2-1}$.

Naším dalším úkolem je najít $n\big(f(x),\ g(x)\big)$:

Použijeme známý vzorec $n = (a_1 \cdot a_2) : D$, který přeznačíme na polynomy:

$$n = \big(f(x) \cdot g(x)\big) : D,$$

dosadíme:

$$\begin{aligned} n = \big(f(x) \cdot g(x)\big) : D &= f(x) \cdot [g(x) : (x^2-1)] = f(x) \cdot (x-3) = \\ &= (x^4-2x^2+1) \cdot (x+3) = x^5-2x^3+x+3x^4-6x^2+3 = \\ &= \boldsymbol{x^5+3x^4-2x^3-6x^2+x+3}. \end{aligned}$$

Nejmenší společný násobek polynomů

$$n = \big(f(x), g(x)\big) = \boldsymbol{x^5+3x^4-2x^3-6x^2+x+3}.$$

PŘÍKLAD 17. Najděte pomocí Euklidova algoritmu největší společný dělitel polynomů $f(x)$ a $g(x)$ a poté jejich nejmenší společný násobek.

$$f(x) = x^3 + 7x^2 + 16x + 12$$
$$g(x) = x^2 + x - 2.$$

Naším prvním úkolem je najít $D\big(f(x),\ g(x)\big)$:

Provedeme dělení polynomu polynomem

$$(x^3 + 7x^2 + 16x + 12) : (x^2 + x - 2) = x + 6 + \frac{12x + 24}{x^2 + x - 2}.$$

$$\begin{array}{r} \underline{-x^3 - x^2 + 2x} \\ 6x^2 + 18x + 12 \\ \underline{-6x^2 - 6x + 12} \\ 12x - 24 \end{array}$$

Dostáváme

$$f(x) = g(x) \cdot (x + 6) + \Big(\underbrace{12x + 24}_{\to x+2}\Big).$$

Provedeme další dělení

$$(x^2 + x - 2) : (x + 2) = x - 1.$$

$$\begin{array}{r} \underline{-x^2 - 2x} \\ -x - 2 \\ \underline{x + 2} \\ 0 \end{array}$$

Dostáváme

$$g(x) = (x + 2) \cdot (x - 1) + 0.$$

Největším společným dělitelem $D\big(f(x),\ g(x)\big) = R(x) = \boldsymbol{x + 2}$.

Naším dalším úkolem je najít $n\big(f(x), g(x)\big)$.

Použijeme známý vzorec $n = (a_1 \cdot a_2) : D$, který přeznačíme na polynomy:

$$n = \big(f(x) \cdot g(x)\big) : D,$$

dosadíme:

$$\begin{aligned} n = \big(f(x) \cdot g(x)\big) : D &= f(x) \cdot [g(x) : (x+2)] = f(x) \cdot (x-1) = \\ &= (x^3 + 7x^2 + 16x + 12) \cdot (x-1) = \\ &= x^4 - x^3 + 7x^3 - 7x^2 + 16x^2 - 16x + 12x - 12 = \\ &= \boldsymbol{x^4 + 6x^3 + 9x^2 - 4x - 12}. \end{aligned}$$

Nejmenší společný násobek polynomů $n = \big(f(x),\ g(x)\big) = \boldsymbol{x^4 + 6x^3 + 9x^2 - 4x - 12.}$

PŘÍKLAD 18. Najděte pomocí Euklidova algoritmu největší společný dělitel polynomů $f(x)$ a $g(x)$ a poté jejich nejmenší společný násobek.

$$\begin{aligned} f(x) &= 2x^3 + 3x^2 + 5x + 2 \\ g(x) &= x^2 + x + 1. \end{aligned}$$

Naším prvním úkolem je najít $D\big(f(x),\ g(x)\big)$:

Provedeme dělení polynomu polynomem

$$(2x^3 + 3x^2 + 5x + 2) : (x^2 + x + 1) = 2x + 1 + \frac{2x+1}{x^2 + x + 1}.$$

$$\begin{array}{r} \underline{-2x^3 - 2x^2 - 2x} \\ x^2 + 3x + 2 \\ \underline{-x^2 - x - 1} \\ 2x + 1 \end{array}$$

Dostáváme

$$f(x) = g(x) \cdot (2x+1) + (2x+1).$$

Provedeme další dělení

$$(x^2 + x + 1) : (2x + 1) = \frac{1}{2}x + \frac{1}{4} + \frac{\frac{3}{4}}{2x + 1}.$$

$$\begin{array}{l} -x^2 - \frac{1}{2}x \\ \qquad \frac{1}{2}x + 1 \\ \qquad -\frac{1}{2}x - \frac{1}{4} \\ \qquad\qquad \frac{3}{4} \end{array}$$

Dostáváme

$$g(x) = (2x + 1) \cdot \left(\frac{1}{2}x + \frac{1}{4}\right) + \frac{3}{4}.$$

Provedeme další dělení

$$(2x + 1) : \frac{3}{4} = \frac{8}{3}x + \frac{1}{\frac{3}{4}}.$$

$$\begin{array}{l} \underline{-2x} \\ \qquad 1 \end{array}$$

Dostáváme

$$(2x + 1) = \frac{3}{4} \cdot \frac{8}{3}x + 1.$$

Největším společným dělitelem $D\big(f(x),\ g(x)\big) = R(x) = \mathbf{1}$.

Naším dalším úkolem je najít $n\big(f(x),\ g(x)\big)$:

Použijeme známý vzorec $n = (a_1 \cdot a_2) : D$, který přeznačíme na polynomy:

$$n = \big(f(x) \cdot g(x)\big) : D,$$

dosadíme

$$n = \big(f(x)\cdot g(x)\big) : D = f(x)\cdot[g(x) :\ 1] = f(x)\cdot g(x) =$$
$$= (2x^3+3x^2+5x+2)\cdot(x^2+x+1) =$$
$$= 2x^5+2x^4+2x^3+3x^4+3x^3+3x^2+5x^3+5x^2+5x+2x^2+2x+2 =$$
$$= \boldsymbol{2x^5+5x^4+10x^3+10x^2+7x+2}.$$

Nejmenší společný násobek polynomů

$$n = \big(f(x), g(x)\big) = \boldsymbol{2x^5+5x^4+10x^3+10x^2+7x+2.}$$

PŘÍKLAD 19. Najděte pomocí Euklidova algoritmu největší společný dělitel polynomů $f(x)$ a $g(x)$ a poté jejich nejmenší společný násobek.

$$f(x) = 3x^5+7x^2-4$$
$$g(x) = x^3+2x^2+3x+6.$$

Naším prvním úkolem je najít $D\big(f(x),\ g(x)\big)$

Provedeme dělení polynomu polynomem

$$(3x^5+7x^2-4) :\ (x^3+2x^2+3x+6) = 3x^2-6x+3+\frac{x^2+27x-22}{x^3+2x^2+3x+6}.$$

$$\underline{-3x^5-6x^4-9x^3-18x^2}$$
$$-6x^4-9x^3\ +11x^2-4$$
$$\underline{6x^4-12x^3\ +18x^2-36x}$$
$$3x^3+7x^2+36x-4$$
$$\underline{-3x^3-6x^2+9x-18}$$
$$x^2+27x-22$$

Dostáváme

$$f(x) = g(x)\cdot(3x^2-6x+3)+(x^2+27x-22).$$

Provedeme další dělení

$$(x^3 + 2x^2 + 3x + 6) : (x^2 + 27x - 22) = x - 25.$$
$$\underline{-x^3 - 27x^2 + 22x}$$
$$-25x^2 + 25x + 6$$
$$\underline{-25\,x^2 + 675x - 550}$$
$$700x - 544$$

Dostáváme

$$g(x) = (x^2 + 27x - 22) \cdot (x - 25) + (700x - 544).$$

K polynomu $x^2 + 27x - 22$ vytvoříme tzv. asociovaný polynom. Ten vytvoříme tak, že polynom $x^2 + 27x - 22$ vynásobíme číslem 700 a potom jej budeme dělit zbytkem po dělení z předešlého kroku.

$$\overbrace{(x^2 + 27x - 22)}^{|\cdot 700} : (700x - 544) =$$
$$= (700x^2 + 18900x - 15400) : (700x - 544) =$$
$$= (175x^2 + 4725x - 3850) : (175x - 136).$$

$$(175x^2 + 4725x - 3850) : (175x - 136) = x + \frac{4861}{175}.$$
$$\underline{-175x^2 + 136x}$$
$$4861x - 3850$$
$$-4861x + 136 \cdot \tfrac{4861}{175}$$
$$\alpha \neq 0$$

Dostaneme

$$(x^2 + 27x - 22) = (700x - 544) \cdot \left(x + \frac{4861}{175} + \alpha\right).$$

POLYNOMY JSOU NESOUDĚLNÉ! NEJVĚTŠÍ SPOLEČNÝ DĚLITEL JE TEDY ROVEN 1.

Naším dalším úkolem je najít $n\big(f(x), g(x)\big)$.

Použijeme známý vzorec $n = (a_1 \cdot a_2) : D$, který přeznačíme na polynomy:

$$n = \big(f(x) \cdot g(x)\big) : D,$$

dosadíme:

$$\begin{aligned} n = \big(f(x) \cdot g(x)\big) : D &= f(x) \cdot [g(x) : 1] = f(x) \cdot g(x) = \\ &= (3x^5 + 7x^2 - 4) \cdot (x^3 + 2x^2 + 3x + 6) = \\ &= 3x^8 + 6x^7 + 9x^6 + 18x^5 + 7x^5 + 14x^4 + 21x^3 + 42x^2 - 4x^3 - 8x^2 - 12x - 24 = \\ &= \boldsymbol{3x^8 + 6x^7 + 9x^6 + 25x^5 + 14x^4 + 17x^3 + 34x^2 - 12x - 24}. \end{aligned}$$

Nejmenší společný násobek polynomů $n = \big(f(x),\ g(x)\big) =$

$$= \boldsymbol{3x^8 + 6x^7 + 9x^6 + 25x^5 + 14x^4 + 17x^3 + 34x^2 - 12x - 24.}$$

PŘÍKLAD 20. Najděte pomocí Euklidova algoritmu největší společný dělitel polynomů $f(x)$ a $g(x)$ a poté jejich nejmenší společný násobek.

$$\begin{aligned} f(x) &= x^5 + 2x^3 + x^2 + 2 \\ g(x) &= x^2 - 1. \end{aligned}$$

Naším prvním úkolem je najít $D\big(f(x),\ g(x)\big)$

Provedeme dělení polynomu polynomem

$$(x^5 + 2x^3 + x^2 + 2) : (x^2 - 1) = x^3 + 3x + 1 + \frac{3x + 3}{x^2 - 1}.$$

$$\begin{array}{l} \underline{-x^5 + x^3} \\ \quad 3x^3 + x^2 + 2 \\ \underline{-3x^3 + 3x} \\ \quad\quad x^2 + 3x + 2 \\ \underline{-x^2 + 1} \\ \quad\quad\quad 3x + 3 \end{array}$$

Dostáváme

$$f(x) = g(x) \cdot (x^3 + 3x + 1) + \Big(\underbrace{3x + 3}_{\to x+1}\Big).$$

Provedeme další dělení

$$(x^2 - 1) : (x + 1) = x - 1.$$
$$\underline{-x^2 - x}$$
$$-x - 1$$
$$\underline{x + 1}$$
$$0$$

Dostáváme

$$g(x) = (3x + 3) \cdot (x - 1) + 0.$$

Největším společným dělitelem $D\big(f(x),\ g(x)\big) = R(x) = x + 1.$

Naším dalším úkolem je najít $n\big(f(x),\ g(x)\big)$:

Použijeme známý vzorec $n = (a_1 \cdot a_2) : D$, který přeznačíme na polynomy:

$$n = \big(f(x) \cdot g(x)\big) : D,$$

dosadíme:

$$n = \big(f(x) \cdot g(x)\big) : D = f(x) \cdot [g(x) : (x + 1)] = f(x) \cdot (x - 1) =$$
$$= (x^5 + 2x^3 + x^2 + 2) \cdot (x - 1) =$$
$$= x^6 - x^5 + 2x^4 - 2x^3 + x^3 - x^2 + 2x - 2 =$$
$$= \boldsymbol{x^6 - x^5 + 2x^4 - x^3 - x^2 + 2x - 2}.$$

Nejmenší společný násobek polynomů

$$n = \big(f(x),\ g(x)\big) = \boldsymbol{x^6 - x^5 + 2x^4 - x^3 - x^2 + 2x - 2.}$$

2 KONGRUENCE

2.1 POPIS POJMU KONGRUENCE

Pojem kongruence byl zaveden už samotným Carlem Friedrichem Gaussem ($1777 - 1855$). I když je to pojem velice jednoduchý, je nesmírně důležitý v teorii čísel.

Říkáme, že celé číslo a je kongruentní s celým číslem b podle modulu m právě tehdy, když platí, že $m|(a-b)$. Modul m je libovolné přirozené číslo, které musí být větší než 1. [2]

Definici můžeme pomocí matematické symboliky napsat následovně

$$a \equiv b \Leftrightarrow m|(a-b) \bmod m.$$

Kongruenci čísel a a b podle modulu m budeme symbolicky zapisovat

$$a \equiv b \pmod{m}$$ čteme a je kongruentní s b podle modulu m.

Jinými slovy můžeme říct, že dvě čísla jsou spolu kongruentní podle modulu m, pokud mají stejný zbytek po dělení číslem m.

Pokud dvě čísla a a b podle modulu m nejsou kongruentní, budeme symbolicky zapisovat

$$a \not\equiv b \pmod{m}.$$

To znamená, že každé z čísel má jiný zbytek po dělení číslem m.

Kongruence je na množině celých čísel relací. V následující části si ukážeme, jaké vlastnosti má relace kongruence.

- Pro každé celé číslo m platí, že $m|0$. Z tohoto závěru je možné usoudit, že platí též $m|(a-a)$. Podle definice kongruence lze můžeme napsat, že $a \equiv a \pmod{m}$. Z tohoto vyplývá, že daná relace musí být na množině celých čísel **reflexivní** relací.
- Dále předpokládejme, že platí $a \equiv b \pmod{m}$. Podle definice platí, že $m|(a-b)$. Podle vlastností dělení celých čísel platí i následující vztah $m|(b-a)$. Zákonitě musí platit i kongruence $b \equiv a \pmod{m}$. Z toho vyplývá, že daná relace musí být na množině celých čísel **symetrickou** relací.
- Budeme předpokládat, že $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$. Podle definice platí, že $m|(a-b)$ a i $m|(b-c)$. Podle vlastností dělení celých čísel platí i následující

vztah $m|[(a-b)+(b-c)]$. Můžeme potom zapsat $m|(a-c)$. Tím pádem platí i následující kongruence $a \equiv c \pmod{m}$. Z toho vyplývá, že daná relace musí být na množině celých čísel **tranzitivní** relací.

Jelikož je tato relace reflexivní, tranzitivní i symetrická, říkáme, že je tato relace relací ekvivalence.

Relace kongruencí vytvářejí podle modulu m na množině celých čísel rozklad na zbytkové třídy. Tyto třídy označujeme $Z_0, Z_1 \dots Z_{m-1}$. Kde Z_0 je množina všech celých čísel, která jsou dělitelná modulem m. Z_1 je množina všech celých čísel, která při dělení modulem m dávají zbytek 1. Z_2 je množina všech celých čísel, která při dělení modulem m dávají zbytek 2 apod.

Například při kongruenci podle modulu 7 dostáváme následující zbytkové třídy

$$Z_0 = \{\dots -42; -35; -28; -21; -14; -7; 0; 7; 14; 21; 28; 35; 42 \dots\}$$
$$Z_1 = \{\dots -41; -34; -27; -20; -13; -6; 1; 8; 15; 22; 29; 36; 43 \dots\}$$
$$Z_2 = \{\dots -40; -33; -26; -19; -12; -5; 2; 9; 16; 23; 30; 37; 44 \dots\}$$
$$Z_3 = \{\dots -39; -32; -25; -18; -11; -4; 3; 10; 17; 24; 31; 38; 45 \dots\}$$
$$Z_4 = \{\dots -38; -31; -24; -17; -10; -3; 4; 11; 18; 25; 32; 39; 46 \dots\}$$
$$Z_5 = \{\dots -37; -30; -23; -16; -9; -2; 5; 12; 19; 26; 33; 40; 47 \dots\}$$
$$Z_6 = \{\dots -36; -29; -22; -15; -8; -1; 6; 13; 20; 27; 34; 41; 48 \dots\}$$

Kdybychom vybrali z každé zbytkové třídy jeden prvek, dostaneme úplnou soustavu zbytků podle modulu m. Pokud bychom si například vybrali množinu $\{-42; -27; -12; 3; 11; 40; 48\}$, tak tato množina je opravdu úplnou soustavou zbytků. Jelikož se v této množině vyskytuje právě jeden zbytek z každé zbytkové třídy $Z_0 - Z_6$.

Pokud bychom si například vybrali množinu $\{-42; -27; -12; 3; 11; 40\}$, tak tato množina není úplnou soustavou zbytků. Jelikož se v této množině se nevyskytuje právě jeden zbytek z každé zbytkové třídy $Z_0 - Z_6$. V této množině chybí prvek ze Z_6.

Množinu čísel $\{b_1; b_2 \dots b_m\}$ budeme nazývat úplnou soustavu zbytků podle modulu m právě tehdy, když platí

$$(\forall i, j) : i \neq j \Rightarrow b_i \not\equiv b_j.$$

Množinu všech čísel $\{0; 1; 2 \dots m-1\}$ budeme nazývat fundamentální úplnou soustavou zbytků podle modulu m.

Pro operace s konguencemi platí následující vztahy:

$$(\forall a, b, c \in Z)(\forall m \in N, m \geq 2)\ a \equiv b\ (\mathrm{mod}\ m) \Rightarrow \boldsymbol{a + c} \equiv \boldsymbol{b + c}\ (\mathrm{mod}\ m).$$
$$(\forall a, b, c \in Z)(\forall m \in N, m \geq 2)\ a \equiv b\ (\mathrm{mod}\ m) \Rightarrow \boldsymbol{a \cdot c} \equiv \boldsymbol{b \cdot c}\ (\mathrm{mod}\ m).$$

Věta o sčítání a násobení kongruencí:

sčítání $\quad a \equiv b\ (\mathrm{mod}\ m)\ \wedge c \equiv d\ (\mathrm{mod}\ m) \Rightarrow \boldsymbol{a + c} \equiv \boldsymbol{b + d}\ (\mathrm{mod}\ m)$

násobení $\quad a \equiv b\ (\mathrm{mod}\ m)\ \wedge c \equiv d\ (\mathrm{mod}\ m) \Rightarrow \boldsymbol{a \cdot c} \equiv \boldsymbol{b \cdot d}\ (\mathrm{mod}\ m)$

2.1.1 PŘÍKLADY NA VÝPOČET KONGRUENCÍ

PŘÍKLAD 1. pomocí kongruencí zjistěte, jaký zbytek dostaneme, pokud budeme dělit číslo 312^{15} číslem 77.

Nejprve si mocnitele převedeme do dvojkové soustavy

$$15 : 2 = 7 \text{ zb } 1$$
$$7 : 2 = 3 \text{ zb } 1$$
$$3 : 2 = 1 \text{ zb } 1$$
$$1 : 2 = 0 \text{ zb } 1$$

čísla v dvojkové soustavě se čtou proti směru dělení. Číslo 15 v dvojkové soustavě můžeme napsat následujícím způsobem

$$15 = (\mathbf{1\ 1\ 1\ 1})_2$$

tj.

$$15 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{8 + 4 + 2 + 1} = 15.$$

Začneme zjišťovat zbytek

1. $312 : 77 \doteq 4{,}052 \qquad 4 \cdot 77 = 308$
   $312 - 308 = 4 \quad \Longrightarrow \quad \mathbf{312 \equiv 4 \bmod 77}$
2. $\mathbf{312^2 \equiv 4^2 \equiv 16 \bmod 77}$
3. $312^4 \equiv 4^4 \equiv 16^2 \equiv 256 \qquad 256 : 77 \doteq 3{,}32 \qquad 3 \cdot 77 = 231$
   $256 - 231 = 25 \quad \Longrightarrow \quad \mathbf{312^4 \equiv 25 \bmod 77}$
4. $312^8 \equiv 25^2 \equiv 625 \qquad 625 : 77 \doteq 8{,}12 \qquad 8 \cdot 77 = 616$
   $626 - 616 = 9 \quad \Longrightarrow \quad \mathbf{312^8 \equiv 9 \bmod 77}$.

Jelikož číslo 15 ve dvojkové soustavě je $(1\,1\,1\,1)_2$, použijeme všechny výrazy s koeficientem jedna $1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$, aby byl výsledný součet 15.

$312^{15} \equiv 4 \cdot 16 \cdot 25 \cdot 9 = 14400 \qquad 14400 : 77 \doteq 187{,}01 \qquad 187 \cdot 77 = 14399$
$14400 - 14399 = 1 \qquad \Longrightarrow \quad \mathbf{312^{15} \equiv 1 \bmod 77}$

Abychom se vyvarovali vyšším číslům, můžeme též poslední krok rozdělit na více částí. Každou část přitom budeme redukovat modulem m. Oba výsledky jsou správné.

$312^{15} \equiv 4 \cdot 16 \cdot 25 = 1600 \qquad 1600 : 77 = 20{,}78 \qquad 20 \cdot 77 = 1540$
$1600 - 1540 = 60$
$312^{15} \equiv 60 \bmod 77$
$312^{15} \equiv 60 \cdot 9 = 540 \qquad 540 : 77 = 7{,}013 \qquad 7 \cdot 77 = 539$
$540 - 539 = \mathbf{1}$
$\mathbf{312^{15} \equiv 1 \bmod 77}$.

Zbytek po dělení čísla 312^{15} číslem 77 je roven 1.

Celkový výsledek jsme našli tak, že při rozepisování mocnitele do dvojkové soustavy byly koeficienty buď 0, nebo 1. Tam kde byly koeficienty rovny jedné, jsme zjistili, s jakým zbytkem je číslo 312 kongruentní. Následně jsme jen jednotlivé zbytky vynásobili a zjistili s jakým zbytkem je 312^{15} kongruentní.

PŘÍKLAD 2. pomocí kongruencí zjistěte, jaký zbytek dostaneme, pokud budeme dělit číslo 1985^{37} číslem 87.

Nejprve si mocnitele převedeme do dvojkové soustavy

$$37 : 2 = 18 \text{ zb } 1$$
$$18 : 2 = 9 \text{ zb } 0$$
$$9 : 2 = 4 \text{ zb } 1$$
$$4 : 2 = 2 \text{ zb } 0$$
$$2 : 2 = 1 \text{ zb } 0$$
$$1 : 2 = 0 \text{ zb } 1$$

čísla v dvojkové soustavě se čtou proti směru dělení. Číslo 37 v dvojkové soustavě můžeme napsat následujícím způsobem

$$37 = (\mathbf{1\,0\,0\,1\,0\,1})_2$$

tj.

$$37 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{32 + 4 + 1 = 37}.$$

Začneme zjišťovat zbytek

1. $1985 : 87 \doteq 22{,}82 \qquad 22 \cdot 87 = 1914$
   $1985 - 1914 = 71 \quad \Longrightarrow \quad \mathbf{1985 \equiv 71 \bmod 87}.$

   Pro zjednodušení výpočtu, odečteme od čísla 71 modul 87.

   $$\mathbf{1985 \equiv -16 \bmod 87}$$

2. $1985^2 \equiv (-16)^2 \equiv 256 \qquad 256 : 87 = 2{,}94 \qquad 2 \cdot 87 = 174$
   $256 - 174 = 82 \quad \Longrightarrow \quad 1985^2 \equiv 82 \bmod 87.$

   Pro zjednodušení výpočtu, opět odečteme od čísla 82 modul 87.

   $$\mathbf{1985 \equiv -5 \bmod 87}$$

3. $1985^4 \equiv (-5)^2 \equiv 25 \qquad \mathbf{1985^4 \equiv 25 \bmod 87}$

4. $1985^8 \equiv 25^2 \equiv 625 \qquad 625 : 87 \doteq 7{,}18 \qquad 7 \cdot 87 = 609$
   $625 - 609 = 16 \quad \Longrightarrow \quad 1985^8 \equiv 16 \bmod 87$

5. $1985^{16} \equiv 16^2 \equiv 256 \qquad 256 : 87 \doteq 2{,}94 \qquad 2 \cdot 87 = 174$
   $256 - 174 = 82 \quad \Longrightarrow \quad 1985^{16} \equiv 82 \bmod 87.$

Pro zjednodušení výpočtu, opět odečteme od čísla 82 modul 87.

$$\mathbf{1985 \equiv -5 \bmod 87}$$

6. $1985^4 \equiv (-5)^2 \equiv 25$ $\mathbf{1985^4 \equiv 25 \bmod 87}$.

Jelikož číslo 37 ve dvojkové soustavě je $(1\,0\,0\,1\,0\,1)_2$, použijeme všechny výrazy s koeficientem jedna $1 \cdot 2^5 + 1 \cdot 2^2 + 1 \cdot 2^0$, aby byl výsledný součet 37.

$1985^{37} \equiv 71 \cdot 25 = 1775$ $1775 : 87 = 20{,}4$ $20 \cdot 87 = 1740$

$1775 - 1740 = 35$

$1985^{37} \equiv 35 \cdot 25 = 875$ $875 : 87 = 10{,}05$ $10 \cdot 87 = 870$

$875 - 870 = \mathbf{5}$

$\mathbf{1985^{37} \equiv 5 \bmod 87.}$

Zbytek po dělení čísla 1985^{37} číslem 87 je roven 5.

PŘÍKLAD 3. pomocí kongruencí zjistěte, jaký zbytek dostaneme, pokud budeme dělit číslo 459^{57} číslem 93.

Nejprve si mocnitele převedeme do dvojkové soustavy

$57 : 2 = 28$ zb 1

$28 : 2 = 14$ zb 0

$14 : 2 = 7$ zb 0

$7 : 2 = 3$ zb 1

$3 : 2 = 1$ zb 1

$1 : 2 = 0$ zb 1

čísla v dvojkové soustavě se čtou proti směru dělení. Číslo 57 v dvojkové soustavě můžeme napsat následujícím způsobem

$$57 = (\mathbf{1\,1\,1\,0\,0\,1})_2$$

tj.

$$57 = 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{32 + 16 + 8 + 1 = 57}.$$

Začneme zjišťovat zbytek

1. $459 : 93 \doteq 4{,}94 \qquad 4 \cdot 93 = 372$
   $459 - 372 = 87 \qquad \Longrightarrow \qquad \mathbf{459 \equiv 87 \bmod 93}$.

   Pro zjednodušení výpočtu, odečteme od čísla 87 modul 93.

   $$\mathbf{459 \equiv -6 \bmod 93}$$

2. $459^2 \equiv (-6)^2 \equiv 36 \qquad 459^2 \equiv 36 \bmod 93$

3. $459^4 \equiv 36^2 \equiv 1296 \qquad 1296 : 93 = 13{,}94 \qquad 13 \cdot 93 = 1209$
   $1296 - 1209 = 87 \qquad \Longrightarrow \qquad \mathbf{459^4 \equiv 87 \bmod 93}$
   dále se již postup a výsledky budou opakovat

4. $459^8 \equiv \mathbf{36 \bmod 93}$

5. $459^{16} \equiv \mathbf{87 \bmod 93}$

6. $459^{32} \equiv \mathbf{36 \bmod 93}$.

Jelikož číslo 57 ve dvojkové soustavě je $(1\,1\,1\,0\,0\,1)_2$, použijeme všechny výrazy s koeficientem jedna $1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^0$, aby byl výsledný součet 57.

$459^{57} \equiv 87 \cdot 36 = 3132 \qquad 3132 : 93 = 33{,}67 \qquad 33 \cdot 93 = 3069$
$3132 - 3069 = 63$
$459^{57} \equiv 63 \bmod 93$
$459^{57} \equiv 63 \cdot 87 = 5481 \qquad 5481 : 93 = 58{,}93 \qquad 58 \cdot 93 = 5394$
$5481 - 5394 = 87$
$459^{57} \equiv 87 \bmod 93$
$459^{57} \equiv 87 \cdot 36 = 3132 \qquad 3132 : 93 = 33{,}67 \qquad 33 \cdot 93 = 3069$
$3132 - 3069 = \mathbf{63}$
$\mathbf{459^{57} \equiv 63 \bmod 93}$.

Zbytek po dělení čísla 459^{57} číslem 93 je roven 63.

PŘÍKLAD 4. Nalezněte zbytek, který dostaneme, když číslo $(1235^{12} + 201^4 \cdot 343^5)$ budeme dělit číslem 43.

Nejprve si zjistíme zbytek u každého z čísel:

$$1235^{12} \bmod 43.$$

Nejprve si mocnitele převedeme do dvojkové soustavy

$$12 = (\mathbf{1\ 1\ 0\ 0})_2$$

tj.

$$12 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = \mathbf{8 + 4 = 12}$$

1. $1235 \equiv 31 \bmod 43$
2. $1235^2 \equiv 15 \bmod 43$
3. $1235^4 \equiv \mathbf{10 \bmod 43}$
4. $1235^8 \equiv \mathbf{14 \bmod 43}$.

Jelikož číslo 12 ve dvojkové soustavě je $(1\ 1\ 0\ 0)_2$, použijeme všechny výrazy s koeficientem jedna $1 \cdot 2^3 + 1 \cdot 2^2$, aby byl výsledný součet 12.

$\mathbf{1235^{12} \equiv 11 \bmod 43}$.

Zbytek po dělení čísla 1235^{12} číslem 43 je 11.

Dále zjistíme zbytek u čísla 201^4 děleným též číslem 43

$$201^4 \bmod 43.$$

Nejprve si mocnitele převedeme do dvojkové soustavy

$$4 = (\mathbf{1\ 0\ 0})_2$$

tj.

$$4 = 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = \mathbf{4}$$

1. $201 \equiv 29 \bmod 43$
2. $201^2 \equiv 24 \bmod 43$

3. $201^4 \equiv \mathbf{17 \bmod 43}$

$\mathbf{201^{12} \equiv 17 \bmod 43}$.

Zbytek po dělení čísla 201^4 číslem 43 je 17.

Dále zjistíme zbytek u čísla 343^5 děleným též číslem 43

$$343^4 \bmod 43.$$

Nejprve si mocnitele převedeme do dvojkové soustavy

$$5 = (\mathbf{1\ 0\ 1})_2$$

tj.

$$4 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{4 + 1 = 5}$$

1. $343 \equiv 42 \bmod 43$
2. $343^2 \equiv 1 \bmod 43$
3. $343^4 \equiv \mathbf{1 \bmod 43}$

$\mathbf{343^5 \equiv 42 \bmod 43}$.

Zbytek po dělení čísla 343^5 číslem 43 je 42.

Máme najít zbytek celého výrazu, jenž byl dělen 43

$$(1235^{12} + 201^4 \cdot 343^5)$$

do výrazu pouze dosadíme jednotlivé zbytky po dělení 43

$$(1235^{12} + 201^4 \cdot 343^5) = 11 + 17 \cdot 42 = 725 \equiv \mathbf{37 \bmod 43}.$$

Zbytek po dělení výrazu $(1235^{12} + 201^4 \cdot 343^5)$ číslem 43 je 37.

2.2 LINEÁRNÍ KONGRUENCE O JEDNÉ NEZNÁMÉ

Lineární kongruenci o jedné neznámé x budeme nazývat následující rovnici ve tvaru $ax + b \equiv 0 \pmod{m}$, kde $m \nmid a$ (modul m nedělí a), $a \wedge b \in Z, m \in N, m \geq 2$. [2]

Pokud řešíme lineární kongruence s jednou neznámou, mohou při řešení nastat tyto tři případy:

1. Pokud platí, že u lineární kongruence $ax + b \equiv 0 \pmod{m}$ je $D(a,m) > 1$ a $D \nmid b$. Tak tato rovnice nemá v úplné soustavě zbytků žádné řešení.

   Zadejme si například rovnici $\boldsymbol{6x + 1 \equiv 0 \bmod 8}$. Pomocí tabulky zjistíme, že tato rovnice opravdu nemá žádné řešení.

   Do tabulky vpisujeme čísla následovně. Do prvního řádku píšeme zbytek z úplné soustavy zbytků. Do druhého řádku píšeme výsledek po dosazení zbytku do zadání. Do třetího řádku píšeme číslo patřící do fundamentální úplné soustavy zbytků kongruentní podle modulu m s číslem ve druhém řádku.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Hodnota výrazu	1	7	13	19	25	31	37	43
Redukce modulem	1	7	5	3	1	7	5	3

   Příklad výpočtu pro $x = 6$.

   Hodnota výrazu: $6x + 1 = 6 \cdot 6 + 1 = 36 + 1 = \mathbf{37}$.

   Redukce modulem 8: $37 : 8 = 4{,}625$ $4 \cdot 8 = 32$ $37 - 32 = \mathbf{5}$.

2. Pokud platí, že u lineární kongruence $ax + b \equiv 0 \pmod{m}$ je $D(a,m) = 1$. Tak tato kongruence má v úplné soustavě zbytků právě jedno řešení.

   Zadejme si například rovnici $\boldsymbol{3x + 1 \equiv 0 \bmod 8}$. Pomocí tabulky zjistíme, že tato rovnice má právě jedno řešení.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Hodnota výrazu	1	4	7	10	13	16	19	22
Redukce modulem	1	4	7	2	5	0	3	6

   Řešení této rovnice je jedno a to $\boldsymbol{x = 5}$.

3. Pokud platí, že u lineární kongruence $ax + b \equiv 0 \pmod{m}$ je $D(a,m) = d, d > 1$ a $d|b$. Tak tato kongruence má v úplné soustavě zbytků právě d řešení.

   Zadejme si například rovnici $\mathbf{6x + 4 \equiv 0 \bmod 8}$. Pomocí tabulky zjistíme, že tato rovnice má právě d řešení.

   Pomocí Euklidova algoritmu zjistíme $D(8,6)$

   $$8 = 1 \cdot 6 + \mathbf{2}$$
   $$6 = 3 \cdot 2 + 0$$

   $D(8,6) = 2$, tudíž tato rovnice musí mít 2 řešení.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Hodnota výrazu	4	10	16	22	28	34	40	46
Redukce modulem	4	2	0	6	4	2	0	6

   Řešením této rovnice je $\boldsymbol{x_1 = 2, x_2 = 6}$.

V příkladech $5, 6$ a 7 budeme využívat poznatky, které již o kongruencích známe. Příklady budeme řešit tak, že budeme postupně přičítat nebo odečítat modul m, k levé, či pravé straně kongruence. Pokud budeme kongruenci dělit číslem q, které dělí zároveň modul m, tak nesmíme zapomenout vydělit i modul číslem q. Pokud číslo q nedělí modul m, vydělíme pouze levou a pravou stranu kongruence a modul m necháme beze změny. Řešení zadané kongruence může být obecně nekonečně mnoho, přičemž všechna jsou navzájem kongruentní podle modulu m.

2.2.1 PŘÍKLADY NA VÝPOČET LINEÁRNÍCH KONGRUENCÍ

PŘÍKLAD 5. Vyřešte lineární kongruenci $3x \equiv -2 \bmod 7$.

Podle Euklidova algoritmu[2] zjistíme $D(3,7)$

$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + \mathbf{1}$$
$$2 = 2 \cdot 1 + 0.$$

[2] Euklidovým algoritmem jsme se podrobně zabývali v 1. kapitole s názvem: Největší společný dělitel a nejmenší společný násobek.

Daná kongruence má právě jedno řešení

$$\begin{aligned} 3x &\equiv -2 \mod 7 && \text{|pravá strana } +7 \\ 3x &\equiv 5 \mod 7 && \text{|PS } +7 \\ 3x &\equiv 12 \mod 7 && \text{| : } 3 \\ \boldsymbol{x} &\equiv \mathbf{4} \mod 7. \end{aligned}$$

Řešení zadané kongruence lze zapsat též v parametrickém tvaru. Parametrický tvar v tomto případě je $x = 4 + 7t,\ \ t \in Z$.

PŘÍKLAD 6. Vyřešte lineární kongruenci $21x \equiv 6 \mod 9$.

Podle Euklidova algoritmu zjistíme $D(21,9)$

$$\begin{aligned} 21 &= 2 \cdot 9 + \mathbf{3} \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Daná kongruence má právě tři řešení

$$\begin{aligned} 21x &\equiv 6 \mod 9 && \text{|levá strana } -9 \\ 12x &\equiv 6 \mod 9 && \text{|LS } -9 \\ 3x &\equiv 6 \mod 9 && \text{| : } 3 \\ \boldsymbol{x} &\equiv \mathbf{2} \mod 3. \end{aligned}$$ [3]

Našli jsme prozatím jedno řešení. Ostatní najdeme velice jednoduše a to tak, že přičteme k ostatním dvěma řešení modul 3 a vyjdou ostatní řešení podle modulu 9.

$$\begin{aligned} x_1 &\equiv 2 \mod 9 \\ x_2 &\equiv 5 \mod 9 \\ x_3 &\equiv 8 \mod 9. \end{aligned}$$

Toto jsou všechna řešení kongruence $21x \equiv 6 \mod 9$.

[3] Jelikož jsme v předešlém kroku rovnici vydělili číslem 3, které zároveň dělí modul 9. Museli jsme i modul dělit číslem 3.

PŘÍKLAD 7. Vyřešte lineární kongruenci $9x \equiv 12 \bmod 11$.

Podle Euklidova algoritmu zjistíme $D(11,9)$

$$11 = 1 \cdot 9 + 2$$
$$9 = 4 \cdot 2 + \mathbf{1}$$
$$2 = 2 \cdot 1 + 0.$$

Daná kongruence má právě jedno řešení

$$\begin{aligned} 9x &\equiv 12 \bmod 11 && |\text{LS } -11 \\ -2x &\equiv 12 \bmod 11 && |:2 \\ -x &\equiv 6 \bmod 11 && |\text{LS a PS } +11 \\ 10x &\equiv 17 \bmod 11 && |\text{PS } +11 \\ 10x &\equiv 28 \bmod 11 && |\text{PS} + 11 \\ 10x &\equiv 39 \bmod 11 && |\text{PS} + 11 \\ 10x &\equiv 40 \bmod 11 && |:10 \\ \boldsymbol{x} &\equiv \mathbf{4 \bmod 11}. \end{aligned}$$

Řešení kongruence $9x \equiv 12 \bmod 11$ je $x \equiv 4 \bmod 11$.

2.2.2 ŘEŠENÍ LINEÁRNÍCH KONGRUENCÍ POMOCÍ EULEROVY VĚTY

FERMATOVA VĚTA (MALÁ FERMATOVA VĚTA): Pro libovolné prvočíslo p a každé celé číslo a platí $a^p \equiv a \bmod p$. Pokud je ještě navíc splněno $D(a,p) = 1$, tak platí $a^{p-1} \equiv 1 \bmod p$. [6]

DŮKAZ: Budeme uvažovat čísla $a; 2a; 3a \ldots (p-1)a$. Čísla $b_1; b_2; b_3 \ldots b_{p-1}$ budou jejich zbytky po dělení modulem p. Zákonitě bude platit:

$$ja = b_j \bmod p \text{ pro čísla } j = 1 \ldots p-1.$$

Čísla b_j jsou z úplné fundamentální soustavy zbytků po dělení modulem p. Můžeme napsat

$$\{b_1; b_2 \ldots b_{p-1}\} = \{1; 2 \ldots p-1\}.$$

Tato rovnost ovšem není prozatím úplně zřejmá. Abychom rovnost mohli využít, musíme ověřit, zda platí

$$b_i = b_j \text{ a dále ještě pro } i = j.$$

Rovnost $b_i = b_j$ je stejná jako zápis $ia \equiv ja \bmod p$.

Jelikož platí věta

$$(\forall a, b, c \in Z)(\forall m \in N, m \geq 2)\ a \equiv b\ (\mathrm{mod}\ m) \Rightarrow \boldsymbol{a \cdot c \equiv b \cdot c}\ (\mathrm{mod}\ m),$$

tak můžeme napsat, že $i \equiv j \bmod p$. A protože uvažujeme $i, j \in \{1; 2 \dots p-1\}$, tak musí platit i vztah $i = j$.

Čísla $b_1; b_2 \dots b_{p-1} \in \{1; 2 \dots p-1\}$ jsou navzájem různá a je jich počet je $p-1$, musí tedy vztah $\{b_1; b_2 \dots b_{p-1}\} = \{1; 2 \dots p-1\}$ platit.

Následně mezi sebou vynásobíme všechny kongruence

$$a \cdot 2a \cdot 3a \dots (p-1)a \equiv b_1 b_2 b_3 \dots b_{p-1} = 1 \cdot 2 \cdot 3 \dots (p-1) \bmod p,$$

platí $a^{p-1} \cdot (p-1)! \equiv (p-1)! \bmod p$. A právě odsud vyplývá řešení. Pokud si uvědomíme, že čísla $2; 3 \dots (p-1)$ jsou nesoudělná s p a tím je možné jimi kongruenci zkrátit. [6]

EULEROVA FUNKCE: Nechť $n \in N$, pak můžeme definovat Eulerovu funkci, kterou můžeme popsat následujícím vztahem

$$\varphi(n) = \{a \in N, 0 < a \leq n;\ (a, n) = 1\},$$

neboli slovně řečeno: Eulerovu funkci můžeme nadefinovat jako počet přirozených čísel menších než n, která jsou navíc nesoudělná s n.

Pokud platí, že $n \in N$ a jeho rozklad je v následujícím tvaru $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Pak platí $\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \dots \left(p_k^{k_1} - p_k^{\alpha_{k-1}}\right)$.

Po úpravě můžeme napsat $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$. Je dobře vidět, že pro prvočíslo p je Eulerova funkce dána vztahem $\varphi(p) = p - 1$.

Pokud budeme mít Eulerovu funkci zadanou ve tvaru $\varphi(m_1 \cdot m_2)$ bude platit $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$.

2.2.3 PŘÍKLAD NA VÝPOČET EULEROVY FUNKCE

PŘÍKLAD 8. Vypočítejte hodnotu Eulerovy funkce pro číslo 756.

Nejdříve si číslo 756 rozložíme na součin prvočísel

$$756 = 3 \cdot 252 = 3 \cdot 7 \cdot 36 = 3 \cdot 2 \cdot 3 \cdot 2 \cdot 3 \cdot 7 = \mathbf{7 \cdot 3^3 \cdot 2^2}.$$

Dále už jen dosadíme do vzorce

$$\begin{aligned}
\varphi(756) &= \varphi(7) \cdot \varphi(3^3) \cdot \varphi 2^2 \\
\varphi(756) &= 6 \cdot (3^3 - 3^2) \cdot (2^2 - 2^1) \\
\varphi(756) &= 6 \cdot 18 \cdot 2 \\
\varphi(756) &= \mathbf{216}.
\end{aligned}$$

Eulerova funkce má pro číslo 756 hodnotu 216.

EULEROVA VĚTA: Jestliže číslo je nesoudělné s modulem m, potom platí následující kongruence

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

kde $\varphi(m)$ je Eulerova funkce.

Pokud je kongruence ve tvaru $ax - b \equiv 0 \bmod m$, neboli $ax \equiv b \bmod m$ a navíc platí, že $D(a, m) = 1$. Tohoto ovšem můžeme dosáhnout většinou vydělením. Poté lze psát

$$ax \equiv b \bmod m,$$

vynásobení kongruenci číslem $a^{\varphi(m)-1}$ a dostaneme tvar

$$\begin{aligned}
ax &\equiv b \bmod m \quad | \cdot a^{\varphi(m)-1} \\
a^{\varphi(m)-1} \cdot a \cdot x &\equiv b \cdot a^{\varphi(m)-1} \mod m,
\end{aligned}$$

dále pak tuto rovnici upravíme a dostaneme

$$\begin{aligned}
a^{\varphi(m)-1+1} \cdot x &\equiv b \cdot a^{\varphi(m)-1} \mod m \\
a^{\varphi(m)} \cdot x &\equiv a^{\varphi(m)-1} \cdot b \mod m,
\end{aligned}$$

protože $a^{\varphi(m)} \equiv 1 \bmod m$, platí

$$x \equiv a^{\varphi(m)-1} \cdot b \mod m.$$

Zavedeme novou neznámou y do kongruence

$$x \equiv (b + m \cdot y) \cdot a^{\varphi(m)-1} \bmod m,$$

pro kterou platí kongruence

$$b + m \cdot y \equiv 0 \bmod a$$

a dopočteme hodnotu y.

Konečné řešení najdeme tak, že do vztahu $x \equiv \underbrace{\underbrace{(b + m \cdot y)}_{a} \cdot a^{\varphi(m)-1}}_{a^{\varphi(m)}} \bmod m$ dosadíme vypočítanou hodnotu y za neznámou y. Dále využijeme, že platí $a^{\varphi(m)} \equiv 1 \bmod m$. Pak již jen dosadíme za b, m, y a a a vypočítáme hodnotu ξ

$$(b + m \cdot y) = a \cdot \xi$$
$$\frac{(b + m \cdot y)}{a} = \xi.$$

Vypočítaná hodnota ξ se rovná hodnotě x. A tudíž známe výsledek kongruence s neznámou x podle modulu m.

2.2.4 PŘÍKLADY NA VÝPOČET LINEÁRNÍCH KONGRUENCÍ POMOCÍ EULEROVY VĚTY

PŘÍKLAD 9. Řešte kongruenci $26x \equiv 4 \bmod 15$ pomocí Eulerovy věty:

Podle Euklidova algoritmu zjistíme $D(26,15)$

$$26 = 1 \cdot 15 + 11$$
$$15 = 1 \cdot 11 + 4$$
$$11 = 2 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + \mathbf{1}$$
$$3 = 3 \cdot 1 + 0.$$

Podle Euklidova algoritmu jsme zjistili, že $D(26,15) = 1$. Kongruence má právě jedno řešení.

Jelikož je splněna podmínka, že $D(a,m)=1$, můžeme kongruenci řešit pomocí Eulerovy metody.

Nejdříve spočítáme Eulerovu funkci pro číslo 15. Využijeme pro výpočet vzorec

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

$$\varphi(15)=3\cdot 5$$

$$\varphi(15)=15\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)=15\cdot\frac{2}{3}\cdot\frac{4}{5}=15\cdot\frac{8}{15}=\mathbf{8}.$$

Eulerova funkce má pro číslo 15 hodnotu 8.

V následujícím kroku vynásobíme kongruenci číslem $a^{\varphi(m)-1}=26^{8-1}=26^7$

$$26x\equiv 4 \bmod 15 \qquad |\cdot 26^7$$

$$26x\cdot 26^7\equiv 4\cdot 26^7 \bmod 15$$

$$26^8x\equiv 4\cdot 26^7 \bmod 15.$$

Protože podle Eulerovy věty platí $a^{\varphi(m)}\equiv 1 \bmod m$, neboli pro tento případ $26^8\equiv 1 \bmod 15$. Můžeme dále napsat

$$x\equiv 4\cdot 26^7 \bmod 15.$$

Dále upravíme, abychom získali výsledek. Tj. číslo 26^7 nahradíme zbytkem po dělení[4] modulem 15

$$x\equiv 4\cdot 26^7 \bmod 15$$

$$x\equiv 4\cdot 11 \bmod 15$$

$$x\equiv 44 \bmod 15$$

$$\boldsymbol{x\equiv 14 \bmod 15}.$$

Řešením je $x\equiv 14 \bmod 15$.

[4] Budeme postupovat jako u příkladů $1-3$ na počátku této kapitoly. V tomto případě se dá velice snadno snížit číslo 26^7 podle modulu 15. U ostatních příkladů tomu tak již není.

PŘÍKLAD 10. Řešte kongruenci $86x \equiv 75 \bmod 91$ pomocí Eulerovy věty:

Podle Euklidova algoritmu zjistíme $D(91,86)$

$$91 = 1 \cdot 86 + 5$$
$$86 = 17 \cdot 5 + \mathbf{1}$$
$$5 = 5 \cdot 1 + 0.$$

Jelikož je splněna podmínka, že $D(a,m) = 1$, můžeme kongruenci řešit pomocí Eulerovy metody.

Nejdříve si číslo 91 rozložíme na součin prvočísel

$$91 = 7 \cdot 13.$$

Dále už jen dosadíme do vzorce

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$
$$\varphi(91) = 7 \cdot 13$$
$$\varphi(91) = 91 \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{13}\right) = 91 \cdot \frac{6}{7} \cdot \frac{12}{13} = 91 \cdot \frac{72}{91} = \mathbf{72}.$$

Eulerova funkce má pro číslo 91 hodnotu 72.

V následujícím kroku vynásobíme kongruenci číslem $a^{\varphi(m)-1} = 86^{72-1} = 86^{71}$

$$86x \equiv 75 \bmod 91 \qquad | \cdot 86^{71}$$
$$86x \cdot 86^{71} \equiv 75 \cdot 86^{71} \bmod 91$$
$$86^{72}x \equiv 75 \cdot 86^{71} \bmod 91.$$

Protože podle Eulerovy věty platí $a^{\varphi(m)} \equiv 1 \bmod m$, neboli pro tento případ $86^{72} \equiv 1 \bmod 91$. Můžeme dále napsat

$$x \equiv 75 \cdot 86^{71} \bmod 91.$$

Zavedeme novou neznámou y do kongruence

$$x \equiv \underbrace{(75 + 91y)}_{\text{dělitelné 86}} \cdot 86^{71} \bmod 86.$$

Vyřešíme kongruenci

$$\begin{aligned} 75 + 91y &\equiv 0 \bmod 86 \\ 91y &\equiv -75 \bmod 86 \qquad |\text{LS } -86 \\ 5y &\equiv -75 \bmod 86 \qquad |:5 \\ y &\equiv -15 \bmod 86 \qquad |\text{PS } +86 \\ \boldsymbol{y} &\equiv \mathbf{71 \bmod 86}. \end{aligned}$$

Konečné řešení najdeme tak, že do vztahu $x \equiv (b + m \cdot y) \cdot a^{\varphi(m)-1} \bmod m$ dosadíme vypočítanou hodnotu y za neznámou y. Dále využijeme, že platí $a^{\varphi(m)} \equiv 1 \bmod m$. Dále již jen dosadíme za b, m, y a a a vypočítáme hodnotu ξ

$$\begin{aligned} (b + m \cdot y) &= a \cdot \xi \\ \frac{(b + m \cdot y)}{a} &= \xi \\ \frac{(75 + 91 \cdot 71)}{86} &= \xi \\ \boldsymbol{\xi} &= \mathbf{76}. \end{aligned}$$

Vypočítaná hodnota ξ se rovná hodnotě x. Tudíž výsledek kongruence s neznámou x podle modulu m je $\boldsymbol{x \equiv 76 \bmod 91}$.

PŘÍKLAD 11. Řešte kongruenci $239x \equiv 191 \bmod 311$ pomocí Eulerovy věty:

Podle Euklidova algoritmu zjistíme $D(311{,}239)$

$$\begin{aligned} 311 &= 1 \cdot 239 + 72 \\ 239 &= 3 \cdot 72 + 23 \\ 72 &= 3 \cdot 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Jelikož je splněna podmínka, že $D(a, m) = 1$, můžeme kongruenci řešit pomocí Eulerovy metody.

Nejdříve spočítáme Eulerovu funkci pro číslo 311. Jelikož číslo 311 je prvočíslo, využijeme vztahu $\varphi(p) = p - 1 = 311 - 1 = \mathbf{310}$.

Eulerova funkce má pro číslo 311 hodnotu 310.

V následujícím kroku vynásobíme kongruenci číslem $a^{\varphi(m)-1} = 239^{310-1} = 239^{309}$

$$239x \equiv 191 \bmod 311 \qquad | \cdot 239^{309}$$
$$239x \cdot 239^{309} \equiv 191 \cdot 239^{309} \bmod 311$$
$$239^{310}x \equiv 191 \cdot 239^{309} \bmod 311.$$

Protože podle Eulerovy věty platí $a^{\varphi(m)} \equiv 1 \bmod m$, neboli pro tento případ $239^{310} \equiv 1 \bmod 311$. Můžeme dále napsat

$$x \equiv 191 \cdot 239^{309} \bmod 311.$$

Zavedeme novou neznámou y do kongruence

$$x \equiv (191 + 311y) \cdot 239^{309} \bmod 239.$$

Vyřešíme kongruenci

$$191 + 311y \equiv 0 \bmod 239$$
$$311y \equiv -181 \bmod 239 \qquad |\text{LS } -239;\ \text{PS } +239$$
$$72y \equiv 48 \bmod 239 \qquad | : 24$$
$$3y \equiv 2 \bmod 239 \qquad | \text{ PS } + 239$$
$$3y \equiv 480 \bmod 239 \qquad | : 3$$
$$\boldsymbol{y \equiv 160 \bmod 239}.$$

Konečné řešení najdeme tak, že do vztahu $x \equiv (b + m \cdot y) \cdot a^{\varphi(m)-1} \bmod m$ dosadíme vypočítanou hodnotu y za neznámou y. Dále využijeme, že platí $a^{\varphi(m)} \equiv 1 \bmod m$. Dále již jen dosadíme za b, m, y a a a vypočítáme hodnotu ξ

$$(b + m \cdot y) = a \cdot \xi$$
$$\frac{(b + m \cdot y)}{a} = \xi$$
$$\frac{(191 + 311 \cdot 160)}{239} = \xi$$
$$\boldsymbol{\xi = 209}.$$

Vypočítaná hodnota ξ se rovná hodnotě x. Tudíž výsledek kongruence s neznámou x podle modulu m je $\boldsymbol{x \equiv 209 \bmod 311}$.

2.2.5 ŘEŠENÍ LINEÁRNÍCH KONGRUENCÍ POMOCÍ BEZOUTOVY VĚTY

BEZOUTOVA VĚTA říká, že v kongruenci ve tvaru $ax - b \equiv 0 \bmod m$, neboli $ax \equiv b \bmod m$ existují koeficienty $k_1, k_2 \in Z$. Pro které platí, že $D(a,m) = k_1 \cdot a + k_2 \cdot m$. Kde čísla k_1, k_2 se dají vypočítat pomocí Euklidova algoritmu. [6]

Z rovnosti výrazu $D = k_1 \cdot a + k_2 \cdot m$ plyne kongruence ve tvaru $k_1 \cdot a + k_2 \cdot m \equiv D \bmod m$. Člen $k_2 \cdot m$ můžeme vyloučit, neboť je jasné, že je kongruentní s 0 podle modulu m. Po vynásobení zbylého členu číslem $\frac{b}{D}$ pak dostaneme výraz

$$k_1 \cdot a \cdot \frac{b}{D} \equiv b \bmod m.$$

Pokud porovnáme zápis $ax \equiv b \bmod m$ s výrazem $k_1 \cdot a \cdot \frac{b}{D} \equiv b \bmod m$, dostaneme vždy výsledek ve tvaru

$$x \equiv k_1 \cdot \frac{b}{D} \bmod m.$$

2.2.6 PŘÍKLADY NA VÝPOČET LINEÁRNÍCH KONGRUENCÍ POMOCÍ BEZOUTOVY VĚTY

PŘÍKLAD 12. Řešte kongruenci $7x \equiv 13 \bmod 19$ pomocí Bezoutovy věty:

Pomocí Euklidova algoritmu zjistíme $D(19,7)$ a poté koeficienty k_1, k_2

$$\begin{aligned} 19 &= 2 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + \mathbf{1} \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

$D(19,7) = 1$ kongruence má jedno řešení.

$$\begin{aligned} 1 &= 1 \cdot 5 - 2 \cdot 2 = \\ &= 1 \cdot (1 \cdot 19 - 2 \cdot 7) - 2 \cdot (1 \cdot 7 - 1 \cdot 5) = \\ &= 1 \cdot 19 - 4 \cdot 7 + 2 \cdot 5 = \\ &= 1 \cdot 19 - 4 \cdot 7 + 2 \cdot (1 \cdot 19 - 2 \cdot 7) = \\ &= \mathbf{3 \cdot 19 - 8 \cdot 7}. \end{aligned}$$

Pomocí Euklidova algoritmu jsme zjistili koeficienty, které potřebujeme do Bezoutovy rovnosti

$$1 = \mathbf{3} \cdot 19 + 7 \cdot (-\mathbf{8}).$$

Dále můžeme napsat

$$1 \equiv\ 3 \cdot 19 + 7 \cdot (-8) \bmod 19.$$

Sčítanec obsahující stejnou hodnotu jako modul, je kongruentní s 0, můžeme jej vynechat

$$7 \cdot (-8) \equiv 1 \bmod 19.$$

Nyní celou kongruenci vynásobíme číslem 13 (člen b v zadání)

$$\begin{aligned} 7 \cdot (-8) &\equiv 1 \bmod 19 \quad \mid \cdot 13 \\ 13 \cdot 7 \cdot (-8) &\equiv 1 \cdot 13 \bmod 19 \\ 13 \cdot 7 \cdot (-8) &\equiv 13 \bmod 19. \end{aligned}$$

Jelikož jsme získali kongruenci, která se rovná stejné hodnotě jako hodnotě v zadání, obě kongruence porovnáme a vyjde nám výsledek

$$\begin{aligned} 13 \cdot 7 \cdot (-8) &\equiv 7x \bmod 19 \quad \mid : 7 \\ 13 \cdot (-8) &\equiv x \bmod 19 \\ -104 &\equiv x \bmod 19 \\ \mathbf{10} &\equiv \boldsymbol{x} \textbf{ mod } \mathbf{19}. \end{aligned}$$

Řešením rovnice $7x \equiv 13 \bmod 19$ je $x \equiv 10 \bmod 19$.

PŘÍKLAD 13. Řešte kongruenci $16x \equiv 5 \bmod 7$ pomocí Bezoutovy věty:

Pomocí Euklidova algoritmu zjistíme $D(16,7)$ a poté koeficienty k_1, k_2

$$\begin{aligned} 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

$D(16,7) = 1$ kongruence má jedno řešení

$$\begin{aligned} 1 &= 1 \cdot 7 - 3 \cdot 2 = \\ &= 1 \cdot 7 - 3 \cdot (1 \cdot 16 - 2 \cdot 7) = \\ &= 7 \cdot 7 - 3 \cdot 16. \end{aligned}$$

Pomocí Euklidova algoritmu jsme zjistili koeficienty, které potřebujeme do Bezoutovy rovnosti

$$1 = \mathbf{7} \cdot 7 + 16 \cdot (-\mathbf{3}).$$

Dále můžeme napsat

$$1 \equiv 7 \cdot 7 + 16 \cdot (-3) \bmod 7.$$

Sčítanec obsahující stejnou hodnotu jako modul, je kongruentní s 0, můžeme jej vynechat

$$16 \cdot (-3) \equiv 1 \bmod 7.$$

Nyní celou kongruenci vynásobíme číslem 5 (člen b v zadání)

$$\begin{aligned} 16 \cdot (-3) &\equiv 1 \bmod 7 \quad | \cdot 5 \\ 5 \cdot 16 \cdot (-3) &\equiv 1 \cdot 5 \bmod 7 \\ 5 \cdot 16 \cdot (-3) &\equiv 5 \bmod 7. \end{aligned}$$

Jelikož jsme získali kongruenci, která se rovná stejné hodnotě jako hodnotě v zadání, obě kongruence porovnáme a vyjde nám výsledek

$$\begin{aligned} 16 \cdot 5 \cdot (-3) &\equiv 16x \bmod 7 \quad | : 16 \\ 5 \cdot (-3) &\equiv x \bmod 7 \\ -15 &\equiv x \bmod 7 \\ \mathbf{6} &\equiv \boldsymbol{x} \textbf{ mod } \mathbf{7}. \end{aligned}$$

Řešením rovnice $16x \equiv 5 \bmod 7$ je $x \equiv 6 \bmod 7$.

PŘÍKLAD 14. Řešte kongruenci $37x \equiv 21 \bmod 32$ pomocí Bezoutovy věty:

Pomocí Euklidova algoritmu zjistíme $D(37,32)$ a poté koeficienty k_1, k_2

$$\begin{aligned} 37 &= 1 \cdot 32 + 5 \\ 32 &= 6 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

$D(37{,}32) = 1$ kongruence má jedno řešení.

$$\begin{aligned} 1 &= 1 \cdot 5 - 2 \cdot 2 = \\ &= 1 \cdot (1 \cdot 37 - 1 \cdot 32) - 2 \cdot (1 \cdot 32 - 6 \cdot 5) = \\ &= 1 \cdot 37 - 3 \cdot 32 + 12 \cdot 5 = \\ &= 1 \cdot 37 - 3 \cdot 32 + 12 \cdot (1 \cdot 37 - 1 \cdot 32) = \\ &= \mathbf{13 \cdot 37 - 15 \cdot 32}. \end{aligned}$$

Pomocí Euklidova algoritmu jsme zjistili koeficienty, které potřebujeme do Bezoutovy rovnosti

$$1 = \mathbf{13} \cdot 37 + 32 \cdot (-\mathbf{15}).$$

Dále můžeme napsat

$$1 \equiv\ 13 \cdot 37 + 32 \cdot (-15) \bmod 32.$$

Sčítanec obsahující stejnou hodnotu jako modul, je kongruentní s 0, můžeme jej vynechat

$$13 \cdot 37 \equiv 1 \bmod 32.$$

Nyní celou kongruenci vynásobíme číslem 21 (člen b v zadání)

$$\begin{aligned} 13 \cdot 37 &\equiv 1 \bmod 32 \quad \mid \cdot 21 \\ 21 \cdot 13 \cdot 37 &\equiv 1 \cdot 21 \bmod 32 \\ 21 \cdot 13 \cdot 37 &\equiv 21 \bmod 32. \end{aligned}$$

Jelikož jsme získali kongruenci, která se rovná stejné hodnotě jako hodnotě v zadání, obě kongruence porovnáme a vyjde nám výsledek

$$\begin{aligned} 21 \cdot 13 \cdot 37 &\equiv 37x \bmod 32 \quad \mid : 37 \\ 273 &\equiv x \bmod 32 \\ \mathbf{17} &\equiv \boldsymbol{x} \textbf{ mod } \mathbf{32}. \end{aligned}$$

Řešením rovnice $37x \equiv 21 \bmod 32$ je $x \equiv 17 \bmod 32$.

2.2.7 ŘEŠENÍ LINEÁRNÍCH KONGRUENCÍ POMOCÍ METODY ROZKLADU MODULU

Je zadána kongruence ve tvaru $a \cdot x \equiv b \bmod m$. Modul m se pokusíme rozložit na součin čísel $m_1 \cdot m_2$. Čísla m_1, m_2 jsou nesoudělná. [2]

V dalším kroku budeme řešit dvě pomocné kongruence podle modulů m_1 a m_2. První kongruence bude vypadat:

$$a \cdot x \equiv b \bmod m_1$$

a druhá

$$a \cdot x \equiv b \bmod m_2.$$

Jelikož jsme řešili dvě kongruence, musí nám zákonitě vyjít i dvě řešení, která si označíme x_1 a x_2. Tato dvě řešení nutně patří do úplné fundamentální soustavy zbytků.

Poté již vyřešíme neurčitou rovnici o neznámých y a z ve tvaru $m_2 y - m_1 z = 1$. Výsledné řešení bude ve tvaru

$$x \equiv m_2 \cdot x_1 \cdot y - m_1 \cdot x_2 \cdot z \bmod m.$$

2.2.8 PŘÍKLAD NA VÝPOČET LINEÁRNÍ KONGRUENCE POMOCÍ METODY ROZKLADU MODULU

PŘÍKLAD 15. Řešte kongruenci $89x \equiv 14 \bmod 240$ pomocí rozkladu modulu.

Provedeme rozklad modulu na dvě nesoudělná čísla. V tomto případě se pro modul 240 hodí čísla 3 a 80.

$$240 = \overset{m_1}{\overbrace{3}} \cdot \overset{m_2}{\overbrace{80}}.$$

Budeme řešit dvě kongruence:

$$\begin{aligned}
89x_1 &\equiv 14 \bmod 3 && |\text{LS} + 3\\
92x_1 &\equiv 14 \bmod 3 && |\text{LS} + 3\\
95x_1 &\equiv 14 \bmod 3 && |\text{LS} + 3\\
98x_1 &\equiv 14 \bmod 3 && |:14\\
7x_1 &\equiv 1 \bmod 3 && |\text{PS} + 3\\
7x_1 &\equiv 4 \bmod 3 && |\text{PS} + 3\\
7x_1 &\equiv 7 \bmod 3 && |:3\\
\boldsymbol{x_1} &\boldsymbol{\equiv 1 \bmod 3},
\end{aligned}$$

$$\begin{aligned} 89x_2 &\equiv 14 \bmod 80 && |\ \text{LS } -80 \\ 9x_2 &\equiv 14 \bmod 80 && |\text{PS } +80 \\ 9x_2 &\equiv 94 \bmod 80 && |\text{PS } +80 \\ 9x_2 &\equiv 174 \bmod 80 && |\text{PS } +80 \\ 9x_2 &\equiv 254 \bmod 80 && |\text{PS } +80 \\ 9x_2 &\equiv 334 \bmod 80 && |\text{PS } +80 \\ 9x_2 &\equiv 414 \bmod 80 && |\ :9 \\ \boldsymbol{x_2} &\equiv \boldsymbol{46 \bmod 8.} \end{aligned}$$

Výsledky si ve fundamentální úplné soustavě označíme $x_1 = 1$ a $x_2 = 46$.

Dále si vyřešíme jednoduchou neurčitou diofantickou rovnici[5] ve tvaru

$$80y - 3z = 1.$$

Diofantickou rovnici si převedeme na kongruenci ve tvaru $m_2 \equiv 1 \bmod m_1$ a vyřešíme

$$\begin{aligned} 80y &\equiv 1 \bmod 3 && |\text{PS } +3 \\ 80y &\equiv 4 \bmod 3 && |\ :4 \\ 20y &\equiv 1 \bmod 3 && |\text{PS} + 3 \\ 20y &\equiv 4 \bmod 3 && |\ : 4 \\ 5y &\equiv 1 \bmod 3 && |\text{PS +3} \\ 5y &\equiv 4 \bmod 3 && |\text{PS +3} \\ 5y &\equiv 7 \bmod 3 && |\text{PS +3} \\ 5y &\equiv 10 \bmod 3 && |\ : 5 \\ \boldsymbol{y} &\equiv \textbf{2mod 3}. \end{aligned}$$

Výsledek $y = 2$ dosadíme do diofantické rovnice a dostaneme výsledek pro neznámou z

$$\begin{aligned} 80y - 3z &= 1 \\ 80 \cdot 2 - 3z &= 1 \\ 160 - 3z &= 1 \\ 159 &= 3z \\ \boldsymbol{z} &= \textbf{53}. \end{aligned}$$

[5] Neurčitými a diofantickými rovnicemi se budeme podrobně zabývat ve 3. kapitole s názvem: Neurčité diofantické rovnice

Před dalším pokračování ve výpočtech si shrneme všechny výsledky

$$m_1 = 3;\ m_2 = 80;\ x_1 = 1;\ x_2 = 46; y = 2; z = 53.$$

V posledním kroku dosadíme vztahu

$$\begin{aligned} x &\equiv m_2 \cdot x_1 \cdot y - m_1 \cdot x_2 \cdot z \bmod m \\ x &\equiv 80 \cdot 1 \cdot 2 - 3 \cdot 46 \cdot 53 \bmod 240 \\ x &\equiv 160 - \overbrace{114}^{\text{redukce modulem 240}} \bmod 240 \\ \boldsymbol{x} &\equiv \mathbf{46} \bmod \mathbf{240}. \end{aligned}$$

Řešením kongruence ve tvaru $89x \equiv 14 \bmod 240$ je číslo $x \equiv 46 \bmod 240$.

Jelikož je tato metoda poměrně náročná na výpočet, čas a je poměrně složitá, je zde uveden jen jeden příklad.

Ukázali jsme si tři metody pro řešení kongruencí. Mezi jednodušší metody k výpočtu kongruencí patří metoda Eulerova a řešení kongruencí pomocí Bezoutovy věty. Výpočet kongruencí pomocí těchto vět není moc náročné, avšak najdou se místa, kde se člověk může velice potrápit.

U Eulerovy metody se využívá faktu, že $a^{\varphi(m)} \equiv 1 \bmod m$. Tímto způsobem pak jednoduše dopočteme kongruence a dostaneme se k výsledku. Metoda je vhodná tehdy, pokud je hodnota Eulerovy funkce vysoká. Metodu lze využít i tehdy, pokud je modul prvočíslem.

Metoda pomocí Bezoutovy věty je též poměrně jednoduchá, hledají se zde prvky k_1, k_2, které se dají vypočítat pomocí Euklidova algoritmu a následně dosadit do Bezoutovy rovnosti. Metoda je vhodná pro příklady, které mají spíše méně kroků Euklidova algoritmu. Pokud je u Euklidova algoritmu moc kroků, obtížně se hledá celočíselná kombinace a tím i koeficienty k_1, k_2, bez kterých by metoda nevedla k dosažení výsledku. Metodu lze využít i tehdy, pokud je modul prvočíslem.

Další možností je Metoda rozkladu modulu, tato metoda se velice dobře hodí, pokud je modul rozložitelný na nesoudělná čísla m_1, m_2. Zvláště výhodná je tehdy, pokud má modul velkou číselnou hodnotu. Pokud nastane případ, že modul m je prvočíslo, tato

metoda nelze použít. Prvočíslo totiž nelze rozložit na součin nesoudělných čísel. Metoda je jak jsem psal výše poměrně složitá a zdlouhavá.

3 NEURČITÉ DIOFANTICKÉ ROVNICE

3.1 LINEÁRNÍ NEURČITÉ ROVNICE

Lineární neurčité rovnice jsou rovnice, které mají více neznámých avšak jen v první mocnině. Obecný tvar lineární neurčité rovnice je

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

kde koeficienty $a_1, a_2 \ldots a_n$ a číslo b náleží celým číslům. $x_1, x_2 \ldots x_n$ jsou neznámé a též náleží celým číslům.

Řešení těchto rovnic si ukážeme na příkladech.

PŘÍKLAD 1. Eliška má v kasičce dvoukoruny a pětikoruny. Celkem má v kasičce mince v hodnotě 30 korun. Kolik má v kasičce dvoukorun a pětikorun?

Tato úloha se dá řešit velice jednoduše pomocí úsudku – nejprve budeme uvažovat nad pětikorunami a poté budeme dopočítávat jednotlivé dvoukoruny.

1. Uvážíme, že má v kasičce 1 pětikorunu a zbytek dvoukorun. Mohou mít jednotlivé mince dohromady hodnotu 30? **Ne**, pokud by měla jednu pětikorunu a zbytek dvoukorun, hodnota 30 korun nemůže nastat. Neboť $1 \cdot 5 = 5$ a $30 - 5 = 25$. Hodnotu čísla 25 nemůžeme nikdy složit beze zbytku pomocí dvoukorun, protože $2 \nmid 25$.
2. Uvážíme, že má v kasičce 2 pětikoruny a zbytek dvoukorun. Mohou mít jednotlivé mince dohromady hodnotu 30? **Ano**, hodnota pětikorun je v tomto případě 10 a zbylých 20 korun pomocí dvoukorun můžeme jednoduše složit. Neboť $2 \cdot 5 = 10$ a $30 - 10 = 20$. Hodnotu čísla 20 můžeme vždy složit beze zbytku pomocí dvoukorun, protože $2 \mid 20$. U ostatních případů budeme postupovat analogicky.
3. Uvážíme, že má v kasičce 3 pětikoruny a zbytek dvoukorun. Mohou mít jednotlivé mince dohromady hodnotu 30? **Ne**, pokud by měla tři pětikoruny a zbytek dvoukorun, hodnota 30 korun nemůže nastat.

4. Uvážíme, že má v kasičce 4 pětikoruny a zbytek dvoukorun. Mohou mít jednotlivé mince dohromady hodnotu 30? **Ano**, hodnota pětikorun je v tomto případě 20 a zbylých 10 korun pomocí dvoukorun můžeme jednoduše složit.
5. Uvážíme, že má v kasičce 5 pětikorun a zbytek dvoukorun. Mohou mít jednotlivé mince dohromady hodnotu 30? **Ne**, pokud by měla pět pětikorun a zbytek dvoukorun, hodnota 30 korun nemůže nastat.
6. Ještě by mohla přicházet v úvahu další dvě řešení.
    a. Eliška má v kasičce 6 pětikorun. Hodnota mincí je opravdu 30 korun. Ovšem v zadání je výslovně napsáno, že má mince hodnoty dvoukorun a pětikorun. Tudíž toto řešení nemůžeme pokládat za správné.
    b. Eliška má v kasičce 15 dvoukorun. Hodnota mincí je též 30 korun. Ovšem v zadání je výslovně napsáno, že má mince hodnoty dvoukorun a pětikorun. Tudíž toto řešení nemůžeme též pokládat jako správné.

Řešení jsou dvě: buď měla Eliška 2 pětikoruny a 10 dvoukorun nebo 4 pětikoruny a 5 dvoukorun.

Tuto slovní úlohu můžeme řešit i pomocí rovnice. V rovnici si označíme hodnotu pětikorunové mince neznámou x a dvoukorunové mince neznámou y. Rovnici pak jednoduše sestavíme a vznikne

$$5x + 2y = 30.$$

Těmto rovnicím se říká neurčité lineární rovnice. Jsou to soustavy rovnic, které mají více neznámých než počet rovnic.

3.2 DIOFANTICKÉ[6] ROVNICE

Neurčitou rovnici nazýváme diofantickou, jestliže neurčitá rovnice má dvě neznámé. Tato rovnice má obecně tvar:

$$ax + by = c, \qquad a \wedge b \neq 0$$

kde koeficienty a, b, c náleží celým číslům a neznámé x, y také celým číslům. [3]

Aby byla diofantická rovnice řešitelná, musíme najít nutnou podmínku pro řešitelnost těchto rovnic. Nutnou podmínkou pro řešitelnost těchto rovnic je, aby největší společný dělitel D koeficientů a, b dělil celé číslo c [4]. Nalezneme jej pomocí Euklidova algoritmu[7]. Dále budeme předpokládat, že rovnice $ax + by = c$ má řešení x_0, y_0. Koeficienty x_0 a y_0 najdeme pomocí Euklidova algoritmu. Potom bude platit $D|a \cdot x_0 + b \cdot y_0$, protože $D|a \wedge D|b$, tak zároveň platí, že $D|c$. Všechna řešení rovnice jsou dána lineárními parametrickými rovnicemi ve tvaru:

$$x = x_0 + \left(\frac{b}{D}\right) \cdot t$$
$$y = y_0 - \left(\frac{a}{D}\right) \cdot t,$$

kde parametr t náleží množině celých čísel.

Často se ovšem setkáváme s tím, že u řešení slovních úloh pomocí diofantických rovnic musíme parametr t omezit určitými podmínkami, které slovní úloha ukládá. Tyto podmínky můžeme zadat např. následovně $x \geq 0$ a $y \geq 0$. Poté již jen vypočítáme lineární nerovnice s parametrem t

$$x_0 + \left(\frac{b}{D}\right) \cdot t \geq 0$$
$$y_0 - \left(\frac{a}{D}\right) \cdot t \geq 0,$$

a vyjdou nám množiny čísel. Pomocí průniku množin čísel zjistíme všechna možná správná řešení dané rovnice.

[6] V literatuře a na internetu se často setkáváme též s pojmem neurčité rovnice.
[7] Euklidovým algoritmem jsme se podrobně zabývali v 1. kapitole s názvem: Největší společný dělitel a nejmenší společný násobek.

3.2.1 SLOVNÍ ÚLOHY ŘEŠENÉ POMOCÍ DIOFANTICKÝCH ROVNIC

PŘÍKLAD 2. Vypočteme si **PŘÍKLAD** 1 z předešlé strany pomocí rovnice. Rovnice je ve tvaru

$$5x + 2y = 30.$$

Pomocí Euklidova algoritmu zjistíme největšího společného dělitele $D(5,2)$

$$5 = 2 \cdot 2 + \mathbf{1}$$
$$2 = 2 \cdot 1 + 0.$$

Největším společným dělitelem čísel $D(5,2) = 1$. Jelikož $1|5, 1|2$ a i v tomto případě $1|30$, má tato rovnice nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 5}$, $\boldsymbol{b = 2.}$

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

Hledaná celočíselná kombinace je ve tvaru

$$1 \cdot 5 + 2 \cdot (-2) = 1$$
$$\mathbf{5x + 2y = 30}$$
$$5 \cdot 1 + 2 \cdot (-2) = 1 \qquad | \cdot 30$$
$$5 \cdot 30 + 2 \cdot (-60) = 30,$$

našli jsme řešení $\boldsymbol{x_0 = 30}$ a $\boldsymbol{y_0 = -60.}$

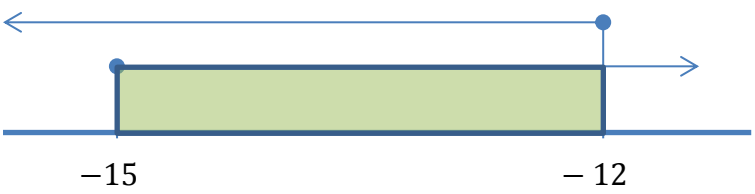
Následně si vypočítáme x a y podle vzorců:

$$x = x_0 + \left(\frac{b}{D}\right)t = 30 + \frac{2}{1}t = \mathbf{30 + 2t}$$
$$y = y_0 - \left(\frac{a}{D}\right)t = -60 - \frac{5}{1}t = \mathbf{-60 - 5t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$$x = 30 + 2t \qquad 30 + 2t \geq 0 \qquad \boldsymbol{t \geq -15}$$
$$y = -60 - 5t \qquad -60 - 5t \geq 0 \qquad \boldsymbol{t \leq -12}.$$

Průnikem zjistíme jednotlivé výsledky



Řešením je množina celočíselných hodnot: $\{-15; -14; -13; -12\}$.

Nyní budeme hledat všechna zbylá řešení:

Všechna řešení	**-15**	**-14**	**-13**	**-12**
x	0	2	4	6
y	15	10	5	0
Výsledek	30	30	30	30

Možná řešení této rovnice jsou dvě. Podle zadání má v kasičce dvoje mince. Eliška mohla mít v kasičce 2 pětikoruny a 10 dvoukorun nebo 4 pětikoruny a 5 dvoukorun. Opět se nabízejí i ona dvě okrajová řešení. Eliška měla dva typy mincí (pětikorunové, dvoukorunové)! Tudíž případy, kdy měla buď 6 pětikorunových mincí anebo 15 dvoukorunových mincí, nejsou správnými řešeními.

PŘÍKLAD 3. Kolika způsoby lze rozlít 92 litrů vody do 24 nádob o objemu $3, 4$ a 5 litrů?

Proměnné jsou v tomto případě počty nádob o objemech $3, 4$ a 5 litrů. [5]

$$3x + 4y + 5z = 92 \qquad x, y, z \geq 0$$
$$x + y + z = 24 \quad \Rightarrow \quad z = 24 - x - y$$

dosadím do 1. rovnice: $3x + 4y + 5 \cdot (24 - x - y) = 92$

$$3x + 4y + 120 - 5x - 5y = 92$$
$$\boldsymbol{2x + y = 28}.$$

Největší společný dělitel čísel $2, 1$ je číslo $\boldsymbol{D(2, 1) = 1}$, protože $1|2$, $1|1$ a $1|28$. Rovnice $2x + y = 28$ má nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 2}$, $\boldsymbol{b = 1.}$

Můžeme zvolit číslo $x_0 = \mathbf{12}$, dosadíme ho do rovnice $2x + y = 28$ a výsledek je $y_0 = \mathbf{4}$.

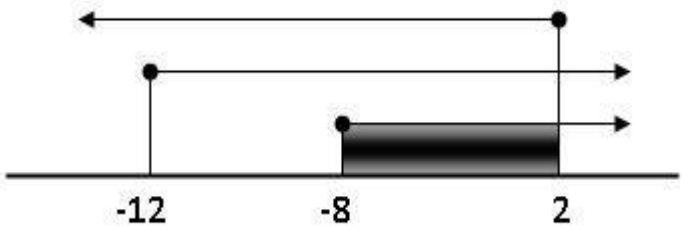
Následně si vypočítáme x a y podle následujících vzorců: [5]

$$x = x_0 + \left(\frac{b}{D}\right)t = 12 + \frac{1}{1}t = \mathbf{12 + t}$$
$$y = y_0 - \left(\frac{a}{D}\right)t = 4 - \frac{2}{1}t = \mathbf{4 - 2t}$$
$$z = 24 - 12 - t - 4 + 2t = \mathbf{8 + t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$$\begin{aligned} x &= 12 + t & 12 + t &\geq 0 & \boldsymbol{t} &\geq \boldsymbol{-12} \\ y &= 4 - 2t & 4 - 2t &\geq 0 & \boldsymbol{t} &\leq \boldsymbol{2} \\ z &= 8 + t & 8 + t &\geq 0 & \boldsymbol{t} &\geq \boldsymbol{-8}. \end{aligned}$$

Průnikem řešení získáme hledané výsledky



Řešením je množina celočíselných hodnot:

$$\{-12; -11; -10; -9; -8; -7; -6; -5; -4; -3; -2; -1; 0; 1; 2\}.$$

Tabulka všech možných řešení:

Všechna řešení	**-8**	**-7**	**-6**	**-5**	**-4**	**-3**	**-2**	**-1**	**0**	**1**	**2**
x	4	5	6	7	8	9	10	11	12	13	14
y	20	18	16	14	12	10	8	6	4	2	0
z	0	1	2	3	4	5	6	7	8	9	10
Výsledek	**92**	**92**	**92**	**92**	**92**	**92**	**92**	**92**	**92**	**92**	**92**

Výpočet $t = -7$ byl řešen: $(5 \cdot 3) + (18 \cdot 4) + (1 \cdot 5) = \boldsymbol{92}$.

Řešení dané rovnice je 11. Jedno z řešení je takové, že můžeme 92 litrů vody rozlít následovně: do pěti třílitrových nádob, osmnácti čtyřlitrových nádob a jedné pětilitrové nádoby.

PŘÍKLAD 4. Existuje terč o třech kruzích. V každém kruhu je jiné bodové skóre. Ve vnějším kruhu je skóre 8, v prostředním kruhu 12 a uvnitř kruhu je 20. Dosažený počet bodů po hře byl 168. Kolik zásahů bylo v jednotlivých kruzích, když v prostředním kruhu (mezi vnitřním a vnějším kruhem) byl stejný počet zásahů jako ve zbývajících dvou?

Jednotlivé kruhy si popíšeme pomocí proměnných. Hodnotu vnitřního kruhu si označíme x, prostředního y a vnějšího z.

(Na konci tohoto příkladu si ukážeme, co by se stalo, kdybychom rovnici už v počátku nedělili číslem 4*).*

Dále sestavíme rovnice

$$\text{I. } 20x + 12y + 8z = 168 \quad |:4$$
$$\underline{\text{II. } y = x + z}$$
$$\text{I. } 5x + 3y + 2z = 42$$
$$\underline{\text{II. } y = x + z.}$$

Pomocí substituční metody dosadíme za y v I. rovnici rovnici II. a dostaneme:

$$5x + 3 \cdot (x + z) + 2z = 42$$
$$5x + 3x + 3z + 2z = 42$$
$$\mathbf{8x + 5z = 42}.$$

Pomocí Euklidova algoritmu zjistíme $D(8,5)$

$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + \mathbf{1}$$
$$2 = 2 \cdot 1 + 0.$$

Největší společný dělitel čísel $D(8,5) = 1$. Jelikož $1|8$, $1|5$ a $1|42$, má rovnice $8x + 5z = 42$ nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 8}$, $\boldsymbol{b = 5}$.

$$1 = 1 \cdot 3 - 1 \cdot 2 =$$
$$= 1 \cdot (1 \cdot 8 - 1 \cdot 5) - 1 \cdot (1 \cdot 5 - 1 \cdot 3) =$$
$$= 1 \cdot 8 - 2 \cdot 5 + 1 \cdot 3 =$$
$$= 1 \cdot 8 - 2 \cdot 5 + 1 \cdot (1 \cdot 8 - 1 \cdot 5) =$$
$$= 2 \cdot 8 - 3 \cdot 5.$$

Hledaná celočíselná kombinace je ve tvaru

$$2 \cdot 8 + 5 \cdot (-3) = 1$$
$$\boldsymbol{8x + 5z = 42}$$
$$8 \cdot 2 + 5 \cdot (-3) = 1 \quad | \cdot 42$$
$$8 \cdot 84 + 5 \cdot (-126) = 42,$$

našli jsme řešení $\boldsymbol{x_0 = 84}$ a $\boldsymbol{z_0 = -126.}$

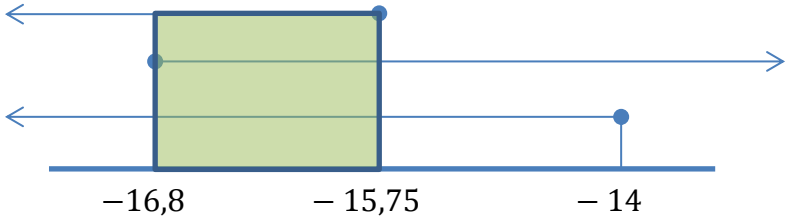
Následně si vypočítáme x a z podle vzorců:

$$x = x_0 + \left(\frac{b}{D}\right) t = 84 + \frac{5}{1} t = \boldsymbol{84 + 5t}$$
$$z = z_0 - \left(\frac{a}{D}\right) t = -126 - \frac{8}{1} t = \boldsymbol{-126 - 8t}$$
$$y = x + z = 84 + 5t + (-126 - 8t) = \boldsymbol{-42 - 3t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$x = 84 + 5t$	$84 + 5t \geq 0$	$\boldsymbol{t \geq -16,8}$
$z = -126 - 8t$	$-126 - 8t \geq 0$	$\boldsymbol{t \leq -15,75}$
$y = -42 - 3t$	$-42 - 3t \geq 0$	$\boldsymbol{t \leq -14}$.

Průnikem zjistíme jednotlivé výsledky



Řešením je pouze jednoprvková množina $\{-16\}$.

Pro $t = -16$ platí:

$x = 84 + 5t = 84 + 5 \cdot (-16) = \mathbf{4}$

$z = -126 - 8t = -126 - 8 \cdot (-16) = \mathbf{2}$

$y = -42 - 3t = -42 - 3 \cdot (-16) = \mathbf{6}$.

Pro kontrolu: Výsledky byly počítány tak: pro $t = -16$

$$(20 \cdot 4) + (12 \cdot 6) + (8 \cdot 2) = \mathbf{168}.$$

Ve vnějším kruhu byly 2 zásahy, v prostředním 6 zásahů a ve vnitřním 4 zásahy.

Zde následuje ukázka postupu, pokud bychom v počátku nedělili rovnici číslem 4.

$$\text{I. } 20x + 12y + 8z = 168$$
$$\underline{\text{II. } y = x + z.}$$

Pomocí substituční metody dosadíme za y v I. rovnici rovnici II. a dostaneme:

$$20x + 12 \cdot (x + z) + 8z = 168$$
$$20x + 12x + 12z + 8z = 168$$
$$\mathbf{32x + 20z = 168}.$$

Pomocí Euklidova algoritmu zjistíme $D(32{,}20)$

$$32 = 1 \cdot 20 + 12$$
$$20 = 1 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + \mathbf{4}$$
$$8 = 2 \cdot 4 + 0.$$

Největší společný dělitel čísel $D(32{,}20) = 4$. Jelikož $4|32$, $4|20$ a $4|168$, má rovnice $32x + 20z = 168$ nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 32}$, $\boldsymbol{b = 20}$.

$4 = 1 \cdot 12 - 1 \cdot 8 =$

$= 1 \cdot (1 \cdot 32 - 1 \cdot 20) - 1 \cdot (1 \cdot 20 - 1 \cdot 12) =$

$= 1 \cdot 32 - 2 \cdot 20 + 1 \cdot 12 =$

$= 1 \cdot 32 - 2 \cdot 20 + 1 \cdot (1 \cdot 32 - 1 \cdot 20) =$

$= 2 \cdot 32 - 3 \cdot 20.$

Hledaná celočíselná kombinace je ve tvaru

$$2 \cdot 32 + 5 \cdot (-20) = 4$$
$$\boldsymbol{32x + 20z = 168}$$
$$32 \cdot 2 + 20 \cdot (-3) = 4 \qquad | \cdot 42$$
$$32 \cdot 84 + 20 \cdot (-126) = 42,$$

našli jsme řešení $\boldsymbol{x_0 = 84}$ a $\boldsymbol{z_0 = -126}$.

Následně si vypočítáme x a z podle vzorců:

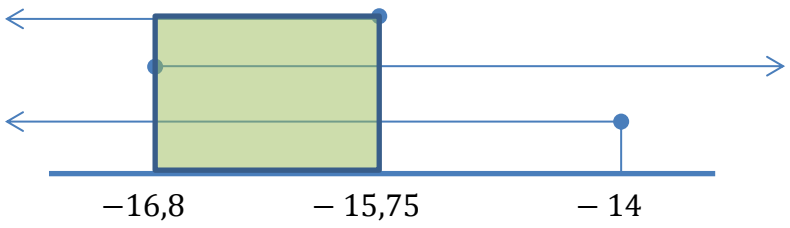
$$x = x_0 + \left(\frac{b}{D}\right) t = 84 + \frac{20}{4} t = \boldsymbol{84 + 5t}$$
$$z = z_0 - \left(\frac{a}{D}\right) t = -126 - \frac{32}{4} t = \boldsymbol{-126 - 8t}$$
$$y = x + z = 84 + 5t + (-126 - 8t) = \boldsymbol{-42 - 3t}.$$

Další postup je již totožný s předchozím, ale přesto si jej uvedeme.

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$x = 84 + 5t$	$84 + 5t \geq 0$	$\boldsymbol{t \geq -16,8}$
$z = -126 - 8t$	$-126 - 8t \geq 0$	$\boldsymbol{t \leq -15,75}$
$y = -42 - 3t$	$-42 - 3t \geq 0$	$\boldsymbol{t \leq -14}$.

Průnikem zjistíme jednotlivé výsledky



Řešením je pouze jednoprvková množina $\{-16\}$.

Pro $t = -16$ platí:

$x = 84 + 5t = 84 + 5 \cdot (-16) = \boldsymbol{4}$

$z = -126 - 8t = -126 - 8 \cdot (-16) = \boldsymbol{2}$

$y = -42 - 3t = -42 - 3 \cdot (-16) = \boldsymbol{6}$.

Pro kontrolu: Výsledky byly počítány tak: pro $t = -16$

$$(20 \cdot 4) + (12 \cdot 6) + (8 \cdot 2) = \mathbf{168}.$$

Ve vnějším kruhu byly 2 zásahy, v prostředním 6 zásahů a ve vnitřním 4 zásahy.

Jak je patrné, pokud bychom rovnici na počátku nevydělili číslem 4, řešení by vyšlo stejné, avšak postup je složitější, protože se počítá s většími čísly. V prvním případě jsme vydělením docílili toho, že $D(8,5) = 1$, pak jsme pokračovali vyjádřením celočíselné kombinace D. V druhém případě byl $D(32,20) = 4$, poté jsme též dopočítávali celočíselnou kombinaci D. Je vidět, že řešení jsou stejná, avšak při výpočtu x, z jsme dosazovali v obou případech za a, b a D jiná čísla. Další postup již byl shodný.

PŘÍKLAD 5. Z fabriky se vyváží denně $10\,000$ výrobků stejného druhu ve třech různých kontejnerech. Do nejmenšího kontejneru se vejde 60 výrobků, do středního kontejneru 80 výrobků a do největšího kontejneru 150 výrobků. Největších kontejnerů lze ovšem použít jen maximálně 10. Středních co nejméně, protože je jich kritický nedostatek. Kolika způsoby lze pomocí úplně naplněných kontejnerů vyvést $10\,000$ výrobků?

Počet nejmenších kontejnerů si označíme neznámou x, středních y a největších z.

Sestavíme rovnici:

$$60x + 80y + 150z = 10000 \qquad |:10$$
$$6x + 8y + 15z = 1000.$$

1. Vyžijeme podmínky, že středních kontejnerů má být co nejméně. Dosadíme za $y = 0$ a dostaneme rovnici:

$$6x + 15z = 1000.$$

Podle Euklidova algoritmu zjistíme $D(6,15)$

$$15 = 2 \cdot 6 + \mathbf{3}$$
$$6 = 2 \cdot 3 + 0.$$

Největší společný dělitel čísel $D(15,6) = 3$. Jelikož $3|15$, $3|6$, ale $3 \nmid 1000$, rovnice $6x + 15z = 1000$ nemá žádné řešení.

2. Pro $y = 0$ rovnice neměla řešení. Dosadíme tedy za $y = 1$ a dostaneme rovnici:

$$6x + 15z + 8 = 1000$$
$$6x + 15z = 992.$$

Největší společný dělitel čísel $D(15,6) = 3$. Protože $3|15$, $3|6$, ale $3 \nmid 992$, rovnice $6x + 15z = 992$ nemá žádné řešení.

3. Pro $y = 0$ a $y = 1$ rovnice neměla řešení. Dosadíme tedy za $y = 2$ a dostaneme rovnici:

$$6x + 15z + 16 = 1000$$
$$6x + 15z = 984 \qquad |:3$$
$$\boldsymbol{2x + 5z = 328}.$$

Podle Euklidova algoritmu zjistíme $D(5,2)$

$$5 = 2 \cdot 2 + \mathbf{1}$$
$$2 = 2 \cdot 1 + 0.$$

Největší společný dělitel čísel $D(5,2) = 1$. Protože $1|5$, $1|2$ a i v tomto případě $1|328$, má rovnice $2x + 5z = 328$ nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 2}, \boldsymbol{b = 5}$.

$$1 = 1 \cdot 5 - 2 \cdot 2.$$

Hledaná celočíselná kombinace je ve tvaru

$$1 \cdot 5 + (-2) \cdot 2 = 1$$
$$-2 \cdot 2 + 1 \cdot 5 = 1.$$

Najdeme řešení x_0, z_0

$$2x + 5z = 328$$
$$2 \cdot (-2) + 5 \cdot 1 = 1 \qquad |\cdot 328$$
$$2 \cdot (-656) + 5 \cdot 328 = 328$$
$$x_0 = -656$$
$$z_0 = 328.$$

Následně si vypočítáme x a y podle vzorců:

$$x = x_0 + \left(\frac{b}{D}\right)t = -656 + \frac{5}{1}t = \mathbf{-656 + 5t}$$

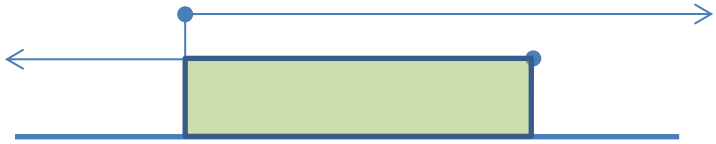
$$z = z_0 - \left(\frac{a}{D}\right)t = 328 - \frac{2}{1}t = \mathbf{328 - 2t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$x = -656 + 5t$	$-656 + 5t \geq 0$	$\boldsymbol{t \geq -131,2}$
$z = 328 - 2t$	$328 - 2t \geq 0$	$\boldsymbol{t \leq 164}$.

(Pokud bychom při výpočtu neznámé $\boldsymbol{z}$ zadali podmínku ze zadání, že největších kontejnerů může být maximálně 10*, postup řešení by nám to velice zjednodušilo. Výpočet s podmínkou pro největší kontejnery si uvedeme na konci příkladu).*

Průnikem řešení získáme hledané výsledky



131,2 164

Řešením je množina celočíselných hodnot: $\{132; 133; 134; \ldots; 162; 163; 164\}$.

$x = -656 + 5t = -656 + 5 \cdot 132 = \mathbf{4}$

$z = 328 - 2t = 328 - 2 \cdot 132 = \mathbf{64}$

$y = \mathbf{2}$.

Tabulka možných řešení:

Všechna řešení	*x*	*y*	*z*	Výsledek
132	4	2	64	10000
133	9	2	62	10000
134	14	2	60	10000
135	19	2	58	10000
136	24	2	56	10000
137	29	2	54	10000
138	34	2	52	10000
139	39	2	50	10000
140	44	2	48	10000
141	49	2	46	10000
142	54	2	44	10000
143	59	2	42	10000
144	64	2	40	10000
145	69	2	38	10000
146	74	2	36	10000
147	79	2	34	10000
148	84	2	32	10000
149	89	2	30	10000
150	94	2	28	10000
151	99	2	26	10000
152	104	2	24	10000
153	109	2	22	10000
154	114	2	20	10000
155	119	2	18	10000
156	124	2	16	10000
157	129	2	14	10000
158	134	2	12	10000
159	139	2	10	10000
160	144	2	8	10000
161	149	2	6	10000
162	154	2	4	10000
163	159	2	2	10000
164	164	2	0	10000

Jelikož podmínka ze zadání říká, že největších kontejnerů může být maximálně 10, přicházejí v úvahu jen následujících šest řešeních:

Správná řešení	*x*	*y*	*z*	Výsledek
159	139	2	10	10000
160	144	2	8	10000
161	149	2	6	10000
162	154	2	4	10000
163	159	2	2	10000
164	164	2	0	10000

Výpočet $t = 159$ byl řešen: $(139 \cdot 60) + (2 \cdot 80) + (10 \cdot 150) = \mathbf{10\,000}$.

V tomto případě budou výrobky odvezeny v následujících počtech kontejnerů: nejmenších bude 139, střední 2 a největších 10.

Odvést $10\,000$ výrobků úplně plnými kontejnery lze šesti způsoby.

Pokud bychom zadali při výpočtu neznámé z podmínku, že maximální počet největších kontejnerů může být 10*. Postup by vypadal následovně:*

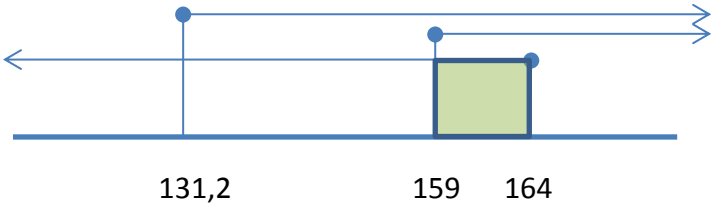
$$x = -656 + 5t \qquad -656 + 5t \geq 0 \qquad \boldsymbol{t \geq -131,2}$$
$$z = 328 - 2t \qquad 328 - 2t \geq 0 \qquad \boldsymbol{t \leq 164}$$

A podmínka pro největší kontejnery: $z = 328 - 2t \leq \mathbf{10}$.

Dále vyřešíme nerovnici

$$z = 328 - 2t \leq \mathbf{10}$$
$$328 - 2t \leq \mathbf{10}$$
$$-2t \leq 10 - 328$$
$$-2t \leq -318 \quad | : (-2)$$
$$\boldsymbol{t \geq 159}.$$

Průnikem řešení získáme hledané výsledky



Řešením je množina celočíselných hodnot: $\{159; 160; 161; 162; 163; 164\}$.

Kontrolní výpočet pro hodnotu parametru $t = 159$.

$x = -656 + 5t = -656 + 5 \cdot 159 = \mathbf{139}$

$z = 328 - 2t = 328 - 2 \cdot 159 = \mathbf{10}$

$y = \mathbf{2}$.

Řešení dle podmínky $z \leq 10$.

Správná řešení	*x*	*y*	*z*	Výsledek
159	139	2	10	10000
160	144	2	8	10000
161	149	2	6	10000
162	154	2	4	10000
163	159	2	2	10000
164	164	2	0	10000

Je dobře vidět, že po zadání podmínky $z \leq 10$ nám vyšla hned všechna správná řešení. Těchto řešení je jako v předešlém postupu opět 6.

PŘÍKLAD 6. Úloha z historie: Pokud dostaneš 100 drachem a je ti řečeno: „Kup za 100 drachem tři druhy ptáků (holuby, kachny a kuřata). Jedna kachna stojí 2 drachmy, tři holubi stojí 1 drachmu a dvě kuřata jsou též po 1 drachmě.“ Kolik ptáků každého druhu můžeš koupit?

Označíme si kachny k, holuby h, kuřata r.

Dostaneme soustavu rovnic

$$\text{I. } k + h + r = 100 \qquad \Rightarrow \quad k = 100 - h - r$$

$$\text{II. } 2k + \frac{h}{3} + \frac{r}{2} = 100.$$

Metodou substituce dosadíme k z I. rovnice za k do II. rovnice

$$2 \cdot (100 - h - r) + \frac{h}{3} + \frac{r}{2} = 100$$

$$200 - 2h - 2r + \frac{h}{3} + \frac{r}{2} = 100$$

$$-2h + \frac{h}{3} - 2r + \frac{r}{2} = 100 - 200$$

$$-\frac{5}{3}h-\frac{3}{2}r=-100 \qquad |\cdot(-6)$$
$$\boldsymbol{10h+9r=600}.$$

Podle Euklidova algoritmu zjistíme $D(10,9)$

$$10=1\cdot 9+\mathbf{1}$$
$$9=9\cdot 1+0.$$

Největší společný dělitel čísel $D(10,9)=1$. Jelikož $1|10,\ 1|9$ a i v tomto případě $1|600$, má rovnice $10h+9r=600$ nekonečně mnoho řešení. Označíme si $\boldsymbol{a=10, b=9}$.

$$1=1\cdot 10-1\cdot 9$$
$$1=1\cdot 10+(-1)\cdot 9.$$

Hledaná celočíselná kombinace je ve tvaru

$$1\cdot 10+(-1)\cdot 9=1.$$

Najdeme řešení h_0, r_0

$$10h+9r=600$$
$$1\cdot 10+(-1)\cdot 9=1 \qquad |\cdot 600$$
$$600\cdot 10+(-600)\cdot 9=600$$
$$h_0=600$$
$$r_0=-600.$$

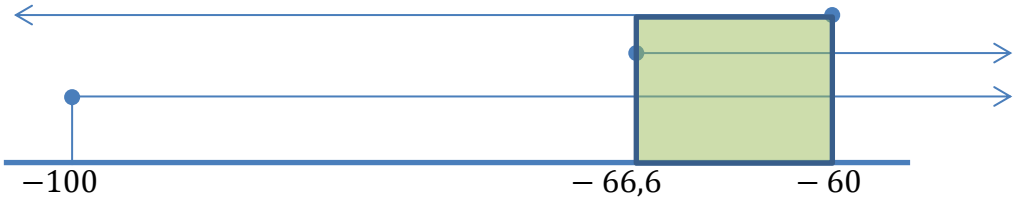
Následně si vypočítáme h, r a k podle vzorců:

$$h=h_0+\left(\frac{b}{D}\right)t=600+\frac{9}{1}t=\boldsymbol{600+9t}$$
$$r=r_0-\left(\frac{a}{D}\right)t=-600-\frac{10}{1}t=\ \boldsymbol{-600-10t}$$
$$k=100-h-r=100-(600+9t)-(-600-10t)=\boldsymbol{100+t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$$h=600+9t \qquad 600+9t\geq 0 \qquad \boldsymbol{t\geq -66,6}$$
$$r=-600-10t \qquad -600-10t\geq 0 \qquad \boldsymbol{t\leq -60}$$
$$k=100+t \qquad 100+t\geq 0 \qquad \boldsymbol{t\geq -100}.$$

Průnikem řešení získáme hledané výsledky



Řešením je množina celočíselných hodnot: $\{-66; -65; -64; -63; -62; -61; -60\}$.

$h = 600 + 9t = 600 + 9 \cdot (-66) = 6$

$r = -600 - 10t = -600 - 10 \cdot (-66) = 60$

$k = 100 + t = 100 + (-66) = 34.$

Tabulka všech možných řešení:

Všechna řešení	**-66**	**-65**	**-64**	**-63**	**-62**	**-61**	**-60**
$\boldsymbol{h}$	6	15	24	33	42	51	60
$\boldsymbol{r}$	60	50	40	30	20	10	0
$\boldsymbol{k}$	34	35	36	37	38	39	40
Výsledek	100	100	100	100	100	100	100

Výpočet $t = -66$ byl řešen: $\left(6 \cdot \frac{1}{3}\right) + \left(60 \cdot \frac{1}{2}\right) + (34 \cdot 2) = 2 + 30 + 68 = \mathbf{100}$ **drachem.**

V tomto případě koupí šest holubů, šedesát kuřat a třicet čtyři holubů.

PŘÍKLAD 7. Partička lidí šla na film do kina. Byly zakoupeny dva druhy vstupenek. Jeden druh po 60 korunách a druhý po 75 korunách. Kolik vstupenek mohlo být od každé zakoupeno, jestliže kupující za ně zaplatil 1875 korun.

Označíme si počet lístků za 60 korun x a za 75 korun y.

Dostaneme rovnici

$$60x + 75y = 1875 \quad |:5$$
$$12x + 15y = 375 \quad |:3$$
$$\boldsymbol{4x + 5y = 125}.$$

Podle Euklidova algoritmu zjistíme $D(5,4)$

$$5 = 1 \cdot 4 + \mathbf{1}$$
$$4 = 2 \cdot 2 + 0.$$

Největší společný dělitel čísel $D(5,4) = 1$. Jelikož $1|5,\ 1|4$ a i v tomto případě $1|125$, má rovnice $4x + 5y = 125$ nekonečně mnoho řešení. Označíme si $\boldsymbol{a = 4, b = 5}$.

$1 = 1 \cdot 5 - 1 \cdot 4.$

Hledaná celočíselná kombinace je ve tvaru

$$1 \cdot 5 + (-1) \cdot 4 = 1$$
$$-1 \cdot 4 + 1 \cdot 5 = 1.$$

Najdeme řešení x_0, y_0

$$4x + 5y = 125$$
$$-1 \cdot 4 + 1 \cdot 5 = 1 \qquad | \cdot 125$$
$$-125 \cdot 4 + 125 \cdot 5 = 125$$
$$x_0 = -125$$
$$y_0 = 125.$$

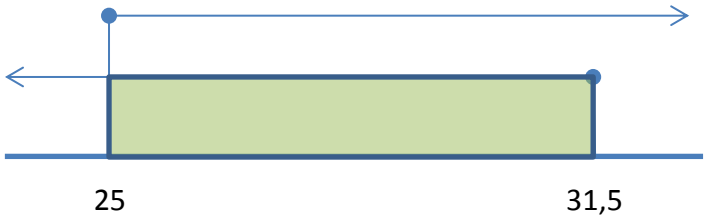
Následně si vypočítáme x a y podle vzorců:

$$x = x_0 + \left(\frac{b}{D}\right)t = -125 + \frac{5}{1}t = \mathbf{-125 + 5t}$$
$$y = y_0 - \left(\frac{a}{D}\right)t = 125 - \frac{4}{1}t = \mathbf{125 - 4t}.$$

Vzhledem k tomu, že řešením mohou být jen celá nezáporná čísla, určíme podmínky pro parametr $\boldsymbol{t}$:

$x = -125 + 5t$	$-125 + 5t \geq 0$	$\boldsymbol{t \geq 25}$
$y = 125 - 4t$	$125 - 4t \geq 0$	$\boldsymbol{t \leq 31,5}$.

Průnikem řešení získáme hledané výsledky



Řešením je množina celočíselných hodnot: $\{25; 26; 27; 28; 29; 30; 31\}$.

Pro $t = 25$ platí,

$x = -125 + 5t = -125 + 5 \cdot 25 = \mathbf{0}$

$y = 125 - 4t = 125 - 4 \cdot 25 = \mathbf{25}$.

Tabulka všech možných řešení:

Všechna řešení	**25**	**26**	**27**	**28**	**29**	**30**	**31**
x	0	5	10	15	20	25	30
y	25	21	17	13	9	5	1
Výsledek	1875	1875	1875	1875	1875	1875	1875

Výpočet $t = 26$ byl řešen: $(5 \cdot 60) + (21 \cdot 75) = 1875$ korun.

V tomto případě bylo nakoupeno pět vstupenek za šedesát korun a dvacet jedna za sedmdesát pět korun.

4 ZÁVĚR

Je velmi zajímavé proniknout do skoro základů matematiky a uvědomit si, jak bylo těžké správně vymyslet postup při řešení výpočtů. Ať již to bylo hledání největšího společného dělitele před dobou, než Euklides vymyslel svůj algoritmus, který byl po něm pojmenován. Hledání největšího společného dělitele bez Euklidova algoritmu probíhalo mnohem složitěji, než s ním. Objevení algoritmu zjednodušilo výpočet neurčitých (diofantických) rovnic a hledání kongruencí, které bylo velmi obtížné i pro velké matematiky té doby.

Matematika za dobu od svého počátku zvládla projít nepřebernými proměnami. Dříve lidé používali jakési „recepty“ – návody, jak který příklad vypočítat (Egypt). Ve starověkém Řecku začali lidé používat zákonitosti a matematické texty si dokazovali. Jak doba plynula, tak se i matematika vyvíjela. Začaly vznikat algoritmy, v 19. století byla dokázána neřešitelnost starověkých řeckých problémů – kvadratura kruhu, trisekce úhlu a duplikace krychle.

Dnes se matematika ubírá úplně jiným směrem, než tomu bylo dříve. Matematiku ovládly kalkulačky, počítače a pouhý člověk již k ní a jejím počátkům (prapočátkům) nemá takový přístup, jako tomu bylo dříve.

Sám ale můžu říci, že matematika je moc pěkný obor, který přináší spoustu poznatků, příležitostí, ale i problémů. Jelikož matematika není mrtvá věda, ale i v dnešní době se neustále rozvíjí a dennodenně nás provází životem. Tak mohu s klidným vědomím říci, že bez matematiky bychom se v minulosti, dnes a ani v budoucnosti nikdy neobešli.

5 SEZNAM LITERATURY

[1] DRÁBEK, Jaroslav a Jaroslav HORA. Algebra. 1. vyd. Plzeň: Západočeská univerzita v Plzni, 2001, 125 s. ISBN 80-708-2787-4.

[2] DRÁBEK, Jaroslav. Texty přednášek předmětu KMT/ELA.

[3] DAŇKOVÁ, Magdaléna. O řešitelnosti některých typů diofantovských rovnic. Plzeň, 2007. Diplomová práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

[4] KOVÁČOVÁ, Jana. Diofantické rovnice. Plzeň, 2010. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Drábek, CSc.

[5] KRYČ, Jiří. Významné matematické úlohy. Plzeň, 2010. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

[6] BULANT, Michal. Algebra 2 - Teorie čísel [online]. Brno, 2008 [cit. 2013-02-25]. Dostupné z: http://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-screen.pdf. Skripta. Masarykova univerzita, Brno.

6 RESUMÉ

Tato práce se zabývá hledáním největšího společného dělitele a nejmenšího společného násobku. V této práci bylo jedním z hlavních cílů aplikovat tyto pojmy do praktických úkolů a reálných úloh. Bez největšího společného dělitele bychom nebyli schopni najít řešení diofantických rovnic a hledání kongruencí podle modulu by též nebylo možné.

Práce by mohla být využita při výuce matematiky na vysoké škole (střední škole, gymnáziu). Obzvlášť se hodí do předmětu Elementární algebra (KMT/ELA) nebo jako materiál pro výuku klasické matematiky, kde by mohla být použita pro představu, jak matematika pracuje.

7 ABSTRACT

This work deals with finding the greatest common divisor and least common multiple. In this work, one of the main target was, to apply these concepts to practical tasks and real exercises. Without the greatest common divisor we have not been able to find a solution of Diophantine equations and a search of Congruence according to the module wouldn´t also be possible.

The work could be used in teaching mathematics at the university (secondary school, high school). Particularly it suits to the subject elementary algebra or as a material for the teaching of classical mathematics, where it could be used for an idea how mathematics works.

8 EVIDENČNÍ LIST

Souhlasím s tím, aby moje bakalářská práce byla půjčována k prezenčnímu studiu v Univerzitní knihovně ZČU v Plzni.

Datum: 25. březen 2013 Podpis:

Uživatel stvrzuje svým čitelným podpisem, že tuto bakalářskou práci použil ke studijním účelům a prohlašuje, že ji uvede mezi použitými prameny.

Jméno	Fakulta/katedra	Datum	Podpis