1 Základní pojmy z teorie čísel

V této přednášce bude $\mathbb{N}$ vždy značit množinu všech přirozených čísel *bez nuly*. Nezáporná celá čísla jsou tedy prvky množiny $\mathbb{N} \cup \{0\}$. Množinu všech celých čísel budeme značit $\mathbb{Z}$.

1.A Dělitelnost v přirozených číslech

Vedle bežného uspořádání $\leq$ přirozených čísel podle velikosti můžeme na $\mathbb{N}$ zavést uspořádání *dělitelností*. Řekneme, že $m \in \mathbb{N}$ *dělí* $n \in \mathbb{N}$, pokud existuje $k \in \mathbb{N}$ takové, že $n = km$, značíme $m|n$. V následujícím lemmatu shrneme několik jednoduchých vlastností dělitelnosti.

Lemma 1.1 (vlastnosti dělitelnosti) (1) $1|n$ *a* $n|n$ *pro všechna* $n \in \mathbb{N}$.
(2) *Pokud* $k|m$ *a zároveň* $m|n$, *pak* $k|n$.
(3) *Pokud* s *dělí dvě z čísel v rovnosti* $n = m + k$, *pak dělí i třetí z těchto čísel.*

Důkaz lemmatu je snadný. Uvědomme si pouze, že v bodě (3) počítáme chvíli s celými (i zápornými) čísly: pokud $s|n$ a $s|m$, pak $n' \cdot s = m' \cdot s + k$ a $(n' - m')s = k$. Ovšem $s, k \in \mathbb{N}$, tudíž $n' - m' \in \mathbb{N}$ a proto $s|k$ v $\mathbb{N}$.

Relace dělitelnosti je tedy reflexivní a tranzitivní a lehko se ověří, že je na $\mathbb{N}$ i slabě antisymetrická. Je to tudíž uspořádání $\mathbb{N}$.

Máme dána dvě uspořádání $\mathbb{N}$, běžné $\leq$ a dělitelnost $|$. Pokud $m|n$, pak $m \leq n$ a v obou uspořádáních je nejmenším prvkem 1. Druhým nejmenším prvkem podle $\leq$ je 2, zatímco v uspořádání $|$ je "druhých nejmenších prvků" více, snadno najdeme několik příkladů: 2, 3, 5, 7, 11, ... Tato čísla p, $p \neq 1$, s vlastností $m|p$ pouze je-li $m = 1$ nebo $m = p$, nazýváme *prvočísla* (pro obecné uspořádání s nejmenším prvkem se takové prvky nazývají atomy, prvočísla jsou tedy atomy dělitelnosti).

Rozklad na součin prvočísel. Každé přirozené číslo můžeme rozložit na součin prvočísel. Číslo 1 budeme považovat za součin prázdného souboru prvočísel. Dále budeme postupovat indukcí podle velikosti (tedy podle $\leq$). Číslo 2 je prvočíslo. Mějme $n \in \mathbb{N}$, $n > 2$, a předpokládejme, že všechna menší čísla umíme rozložit na součin prvočísel. Pokud není n prvočíslo, pak má n nějakého dělitele $m|n$, $m \neq 1$ a $m \neq n$, a můžeme psát $n = m \cdot k$. Přitom musí být $m, k < n$ a z indukčního předpokladu rozložíme m i k a tedy i n na součin prvočísel.

Poznámka. V předchozím odstavci jsme prováděli indukci dle velikosti. Uspořádání dělitelností na $\mathbb{N}$ má stejnou základní vlastnost: každý prvek má pouze konečně mnoho předchůdců. Důsledkem je, že důkazy indukcí lze provádět i dle uspořádání dělitelností.

Později ukážeme, že dané číslo lze rozložit jediným způsobem na součin prvočísel.

Snadno si uvědomíme, že existuje nekonečně mnoho prvočísel. Předpokládejme, že je pouze konečně mnoho prvočísel, a označme je $p_1, p_2, \ldots, p_k$. Uvažme číslo $p = p_1 \cdot p_2 \cdot$

$\ldots \cdot p_k + 1$. Musí existovat nějaký prvočíselný dělitel p, tedy pro vhodné $1 \leq i \leq k$ bude platit $p_i|p$. Z faktu, že $p_i|p$ a take $p_i|p_1 \cdot p_2 \cdot \ldots \cdot p_k$, plyne $p_i|1$ (podle Lemmatu 1.1), což je výsledný spor.

Dalším známým tvrzením je fakt, že každá dvě přirozená čísla mají největšího společného dělitele.

Definice. Pro trojici čísel $d, n, m \in \mathbb{N}$ řekneme, že d je *společný dělitel* n a m, pokud $d|n$ a zároveň $d|m$. Číslo d je *největší společný dělitel* n a m, $d = \text{NSD}(n, m)$, pokud navíc platí, že kdykoli k je společný dělitel n a m, pak $k|d$.

Existenci NSD budeme moci odvodit díky následující vlastnosti počítání s přirozenými čísly.

Dělení se zbytkem. Pro přirozené číslo m a nezáporné celé n existují nezáporná celá čísla k a r (tedy prvky $\mathbb{N} \cup \{0\}$) taková, že $n = km + r$ a přitom je $r < m$.

Číslo r se nazývá *zbytek po dělení čísla n číslem m* a je určeno jednoznačně. Důkaz tohoto tvrzení je snadný. Množina $\{km \ ; \ k \in \mathbb{N} \cup \{0\}\}$ všech nezáporných násobků čísla m obsahuje 0 a tedy lze najít největší k takové, že $km \leq n$, neboť číslo n je konečné. Potom je určitě $n - km < m$ a můžeme položit $r = n - km$.

Zbytek po vydělení čísla n číslem m se také nazývá n *modulo* m a budeme ho značit $n \bmod m$.

Příklad. $11 \bmod 3 = 2$, $254 \bmod 1500 = 254$, $14 \bmod 7 = 0$.

Pro počítání modulo platí následující tvrzení:

Pro $m \in \mathbb{N}$ a $n_1, n_2, r_1, r_2 \in \mathbb{N} \cup \{0\}$ takové, že $r_1 = n_1 \bmod m$ a $r_2 = n_2 \bmod m$, platí $(n_1 + n_2) \bmod m = (r_1 + r_2) \bmod m$.

Jeho platnost lze snadno ověřit. Máme dána dělení se zbytkem $n_1 = k_1 m + r_1$, $n_2 = k_2 m + r_2$ a $r_1 + r_2 = \overline{k}m + \overline{r}$. Počítejme: $n_1 + n_2 = (k_1 m + r_1) + (k_2 m + r_2) = (k_1 + k_2)m + r_1 + r_2 = (k_1 + k_2)m + \overline{k}m + \overline{r} = (k_1 + k_2 + \overline{k})m + \overline{r}$. Přitom $\overline{r} < m$ a tedy z jednoznačnosti zbytku plyne $\overline{r} = (n_1 + n_2) \bmod m$.

Dělení se zbytkem je klíčem k odvozování dalších vlastností dělitelnosti.

V následujícím odstavci popíšeme algoritmus pro hledání největšího společného dělitele čísel n a m, který je také důkazem existence NSD.

Eukleidův algoritmus. Mějme dvě čísla $n, m \in \mathbb{N}$.

1. krok: Vydělíme n číslem m se zbytkem r_1, tedy $n = k_1 m + r_1$, kde $k_1, r_1 \in \mathbb{N} \cup \{0\}$ a $r_1 < m$. Je-li $r_1 = 0$, pak $m|n$, $m = \text{NSD}(n, m)$ a jsme hotovi. Pokud $r_1 \neq 0$, pokračujeme dál.

2. krok: Podle Lemmatu 1.1 má dvojice n, m stejné společné dělitele jako dvojice m, r_1. Přejdeme k číslům m a r_1. Vydělíme m číslem r_1 se zbytkem r_2, tedy $m = k_2 r_1 + r_2$, kde $k_2, r_2 \in \mathbb{N} \cup \{0\}$ a $r_2 < r_1$. Je-li $r_2 = 0$, pak $r_1 | m$, $r_1 = \text{NSD}(m, r_1) = \text{NSD}(n, m)$ a jsme hotovi. Pokud $r_2 \neq 0$, pokračujeme dál.

.....

i-tý krok: Vydělíme r_{i-2} číslem r_{i-1} se zbytkem r_i, tedy $r_{i-2} = k_i r_{i-1} + r_i$, kde $k_i, r_i \in \mathbb{N} \cup \{0\}$ a $r_i < r_{i-1}$. Je-li $r_i = 0$, pak $r_{i-1} | r_{i-2}$, $r_{i-1} = \text{NSD}(r_{i-2}, r_{i-1}) = \text{NSD}(r_{i-3}, r_{i-2}) = ... = \text{NSD}(m, r_1) = \text{NSD}(n, m)$ a jsme hotovi. Pokud $r_i \neq 0$, pokračujeme dál.

.....

Posloupnost zbytků $r_1, r_2, r_3, ...$ je ostře klesající, $r_1 > r_2 > r_3 > ...$, a proto po konečném počtu kroků dojdeme ke zbytku $r_i = 0$ a algoritmus vždy skončí nalezením největšího společného dělitele $r_{i-1} = \text{NSD}(n, m)$.

Věta 1.2 *Pro každá dvě čísla $n, m \in \mathbb{N}$ existuje největší společný dělitel $d = NSD(n, m)$. Navíc lze nalézt dvě nezáporná čísla $k, l \in \mathbb{N} \cup \{0\}$ tak, že $d = kn - lm$.*

Důkaz. Existence NSD plyne z Eukleidova algoritmu. K důkazu zbytku tvrzení si nejdřív uvědomíme, že $d = \text{NSD}(n, m)$ lze vyjádřit ve tvaru $d = k'n + l'm$, kde $k', l' \in \mathbb{Z}$. Podle Eukleidova algoritmu v prvním kroku vyjádříme $r_1 = n - k_1 m$, podobně $r_2 = m - k_2 r_1$ a po dosazení $r_2 = m - k_2(n - k_1 m) = -k_2 n + (1 + k_2 k_1)m$. Snadno postupně vyjádříme všechny zbytky r_i jako celočíselnou kombinaci n a m a tedy i $\text{NSD}(n, m)$.

Proveďme ještě úpravu na požadovaný tvar $d = kn - lm$, $k, l \in \mathbb{N} \cup \{0\}$. Pro získaný tvar $d = k'n + l'm$, $k', l' \in \mathbb{Z}$, zvolme $t \in \mathbb{N} \cup \{0\}$ tak, aby $tm + k' \geq 0$ a zároveň $tn - l' \geq 0$. Pak bude $d = k'n + l'm = k'n + l'm + tnm - tnm = (tm + k')n - (tn - l')m$ a položíme $k = tm + k'$ a $l = tn - l'$. □

Příklad. Hledejme největšího společného dělitele $n = 42$ a $m = 1295$.

1. krok: Vydělíme 42 číslem 1295 se zbytkem r_1, tedy $42 = 0 \cdot 1295 + 42$, $r_1 = 42$.
2. krok: Vydělíme 1295 číslem $r_1 = 42$ se zbytkem r_2, tedy $1295 = 30 \cdot 42 + 35$, $r_2 = 35$.
3. krok: Vydělíme $r_1 = 42$ číslem $r_2 = 35$ se zbytkem r_3, tedy $42 = 1 \cdot 35 + 7$, zbytek $r_3 = 7$.
4. krok: Vydělíme $r_2 = 35$ číslem $r_3 = 7$ se zbytkem r_4, tedy $35 = 5 \cdot 7 + 0$, zbytek $r_4 = 0$.

Našli jsme $\text{NSD}(42, 1295) = r_3 = 7$. Číslo 7 lze tudíž vyjádřit ve tvaru $7 = k \cdot 42 - l \cdot 1295$ pro vhodné nezáporné koeficienty k a l. Pokusme se nejdříve podle Eukleidova algoritmu vyjádřit 7 jako celočíselnou kombinaci 42 a 1295:

podle 1.-ho kroku vyjádříme $r_1 = 42 = 42 - 0 \cdot 1295 = 42$,
podle 2.-ho kroku vyjádříme $r_2 = 35 = 1295 - 30 \cdot r_1 = 1295 - 30 \cdot 42$
a podle 3.-ho kroku vyjádříme $r_3 = 7 = r_1 - 1 \cdot r_2 = 42 - (1295 - 30 \cdot 42) = 31 \cdot 42 - 1295$.

Našli jsme koeficienty $k = 31$, $l = 1$ a vyjádření $\text{NSD}(42, 1295) = 7 = 31 \cdot 42 - 1295$.

Příklad. Zkusme řešit stejný úkol pro čísla $n = 12$ a $m = 4$. Protože $4|12$, je podle definice $\mathrm{NSD}(12, 4) = 4$. Nabízí se vyjádření $4 = 0 \cdot 12 + 4$. Převeďme toto vyjádření podle důkazu Věty 1.2 do požadovaného tvaru. Zvolme $t = 1$, pak bude $4 = 0 \cdot 12 + 4 + 1 \cdot 12 \cdot 4 - 1 \cdot 12 \cdot 4 = 4 \cdot 12 - 11 \cdot 4$, tedy $k = 4$ a $l = 11$. Nejmenší vhodná čísla jsou $k = 1$ a $l = 2$.

Máme-li k dispozici prvočíselné rozklady n a m, pak z nich můžeme zjistit $\mathrm{NSD}(n, m)$. V prvním z předchozích příkladů máme $n = 42 = 2 \cdot 3 \cdot 7$ a $m = 1295 = 5 \cdot 7 \cdot 37$ rozklady na součin prvočísel. Tyto rozklady se "překrývají" pouze na jednom místě a to v prvočísle 7, proto je $\mathrm{NSD}(42, 1295) = 7$. V následujících odstavcích se pokusíme tento postup zdůvodnit.

Lemma 1.3 (ekvivalentní definice prvočísla) *Číslo $p \in \mathbb{N}$ je prvočíslo právě když platí pro každá $n, m \in \mathbb{N}$ pokud $p|n \cdot m$, pak $p|n$ nebo $p|m$.*

Důkaz. Předpokládejme, že p je prvočíslo. Podle naší definice jedinými děliteli p jsou 1 a p. Nechť $p|n \cdot m$ a ať například p nedělí n. Pak $\mathrm{NSD}(p, n) = 1$, neboť p má pouze dva dělitele. Vyjádřeme $\mathrm{NSD}(p, n) = 1 = kp - ln$ s nezápornými koeficienty k, l. Vynásobením m dostaneme $m + lnm = kmp$ a z předpokladu $p|n \cdot m$ plyne $p|m$ podle Lemmatu 1.1 (3) a jsme hotovi.

Důkaz druhé z implikací je snadný. Dokazujeme, že p je prvočíslo. Ať $p = nm$. Z předpokladu plyne buď $p|n$ nebo $p|m$. Pokud například $p|n$, pak $n = p$ (neboť $n \leq p \leq n$) a $m = 1$. □

Jednoznačnost prvočíselných rozkladů. Již víme, že dané číslo $n \in \mathbb{N}$ má rozklad na součin prvočísel. Nyní ukážeme, že takový rozklad je jediný. Ať $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$ jsou dva prvočíselné rozklady n. Budeme postupovat indukcí podle délky prvního rozkladu, tedy podle r. Je-li $r = 0$, pak takovýto (prázdný) rozklad považujeme za rozklad čísla $n = 1$ a proto je nutně i $s = 0$. Předpokládejme, že $r > 0$ a že dva rozklady stejného čísla jsou shodné až na pořadí prvočísel, pokud je alespoň jeden z těchto rozkladů kratší než r. Z rovnosti rozkladů vidíme, že $p_r|q_1 q_2 ... q_s$, a protože je p_r prvočíslo, pak $p_r|q_1$ nebo $p_r|q_2 ... q_s$. Postupnou aplikací Lemmatu 1.3 nalezneme $1 \leq i \leq s$ takové, že $p_r|q_i$. Musí být $p_r = q_i$ (neboť $p_r \neq 1$) a oba rozklady můžeme zkrátit: $p_1 p_2 ... p_{r-1} = q_1 q_2 ... q_{i-1} q_{i+1} ... q_s$. Z indukčního předpokladu je $r - 1 = s - 1$ a tyto zkrácené rozklady jsou až na pořadí prvočísel shodné. Z toho snadno plyne jednoznačnost původních rozkladů, tedy $r = s$ a po vhodném přečíslování $p_1 = q_1$, $p_2 = q_2$, ..., $p_r = q_r$.

Teď již můžeme vysvětlit vztah prvočíselných rozkladů a největších společných dělitelů a také *nejmenších společných násobků.*

Definice. Pro trojici čísel $k, n, m \in \mathbb{N}$ řekneme, že k je *společný násobek* n a m, pokud $n|k$ a zároveň $m|k$. Číslo k je *nejmenší společný násobek* n a m, $k = \mathrm{NSN}(n, m)$, pokud navíc platí, že kdykoli l je společný násobek n a m, pak $k|l$.

Mějme tedy dva rozklady $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ a $m = p_1^{l_1} p_2^{l_2} ... p_r^{l_r}$, kde $p_1, p_2, ..., p_r$ jsou *po dvou různá* prvočísla a $k_1, k_2, ..., k_r, l_1, l_2, ..., l_r$ jsou nezáporné celočíselné mocniny (mohou tedy být rovny 0). Máme-li dále nějakého dělitele d čísla n, tedy $n = d \cdot c$ pro vhodné

$c \in \mathbb{N}$, pak musejí být prvočíselné rozklady d a c částí prvočíselného rozkladu n. Toto platí díky *jednoznačnosti* rozkladu. Tedy lze psát prvočíselný rozklad $d = p_1^{k_1'} p_2^{k_2'} ... p_r^{k_r'}$, kde $k_1' \leq k_1$, $k_2' \leq k_2$, ..., $k_r' \leq k_r$. Naopak, číslo v tomto tvaru je zjevně dělitelem n. Proto je

$\mathrm{NSD}(n,m) = p_1^{\min(k_1,l_1)} p_2^{\min(k_2,l_2)} ... p_r^{\min(k_r,l_r)}$

$\mathrm{NSN}(n,m) = p_1^{\max(k_1,l_1)} p_2^{\max(k_2,l_2)} ... p_r^{\max(k_r,l_r)}$.

Tímto jsme také ukázali *existenci* nejmenších společných násobků.

Z předchozího také snadno plyne, že je-li $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ rozklad n takový, že $p_1, p_2, ..., p_r$ jsou po dvou různá prvočísla, pak má n právě $(k_1+1)\cdot(k_2+1)...(k_r+1)$ různých dělitelů.

Úkol. Podle předchozího odstavce ukažte, že pro $n, m \in \mathbb{N}$ platí: $\mathrm{NSN}(n,m) = nm/\mathrm{NSD}(n,m)$.

Příklad. Pro čísla $1500 = 2^2 \cdot 3 \cdot 5^3$ a $6050 = 2 \cdot 5^2 \cdot 11^2$ tedy je $\mathrm{NSD}(1500, 6050) = 2 \cdot 5^2 = 50$ a $\mathrm{NSN}(1500, 6050) = 2^2 \cdot 3 \cdot 5^3 \cdot 11^2 = 181500$. Počet všech různých dělitelů čísla 1500 je $(2+1)(1+1)(3+1) = 3 \cdot 2 \cdot 4 = 24$.

Úkol. Nyní umíme zjišťovat NSD dvěma způsoby: Eukleidovým algoritmem a pomocí prvočíselných rozkladů. Neuvedli jsme ale algoritmus, kterým lze dané číslo rozložit na součin prvočísel. Zkuste takový algoritmus navrhnout a zamyslet se nad efektivitou obou postupů.

Definice. Je-li $\mathrm{NSD}(n,m) = 1$, čísla n a m se nazývají *nesoudělná*. V opačném případě říkáme, že n a m jsou *soudělná*.

Lemma 1.4 *Jsou-li n a m nesoudělná a také n a l nesoudělná, pak jsou i n a $m \cdot l$ nesoudělná. Jsou-li n a m nesoudělná a obě dělí číslo l, pak $n \cdot m | l$.*

Důkaz. Dokažme první část tvrzení. Pokud $\mathrm{NSD}(n, m \cdot l) \neq 1$, pak existuje nějaké prvočíslo $p | \mathrm{NSD}(n, m \cdot l)$. Pak $p|m$ nebo $p|l$. Řekněme, že $p|m$. Pak je p společný dělitel n a m a $\mathrm{NSD}(n,m) \neq 1$.

Dokažme druhou část tvrzení. Víme, že l je společný násobek n a m. Přitom $\mathrm{NSN}(n,m) = nm/\mathrm{NSD}(n,m) = nm/1 = nm$. Tudíž $nm|l$. □

Následující tvrzení se zabývá řešitelností soustav rovnic typu $x \bmod n = r$.

Věta 1.5 (Čínská věta o zbytcích) *Mějme po dvou nesoudělná čísla $n_1, ..., n_k \in \mathbb{N}$ a nezáporná celá čísla $r_1, ..., r_k \in \mathbb{N} \cup \{0\}$ taková, že $r_1 < n_1$, ..., $r_k < n_k$. Soustava rovnic*

$x \bmod n_1 = r_1$

$x \bmod n_2 = r_2$

.....

.....

$x \bmod n_k = r_k$

má vždy nezáporné řešení $x \in \mathbb{N} \cup \{0\}$. Existuje jediné nezáporné řešení $x < n_1 n_2 ... n_k$.

Důkaz. Můžeme jistě předpokládat, že $n_i \neq 1$ pro všechna $i = 1, ..., k$. Zkusme nejprve nalézt nějaké řešení. Označme $\overline{n}_i = n_1 n_2 ... n_{i-1} n_{i+1} ... n_k$ pro $i = 1, 2, ..., k$. Podle předpokladu je $\mathrm{NSD}(\overline{n}_i, n_i) = 1$ (viz Lemma 1.4) a tedy existuje vyjádření $1 = t_i \overline{n}_i - s_i n_i$ pro vhodná nezáporná t_i, s_i. Z poslední rovnosti plyne, že $t_i \overline{n}_i \bmod n_i = 1$ a tedy $r_i t_i \overline{n}_i \bmod n_i = r_i$. Zároveň samozřejmě $r_i t_i \overline{n}_i \bmod n_j = 0$ pro $j \neq i$. Nyní vidíme, že $x = r_1 t_1 \overline{n}_1 + r_2 t_2 \overline{n}_2 + ... + r_k t_k \overline{n}_k$ je řešením dané soustavy.

Odečteme-li od x číslo n_i, zbytek po vydělení číslem n_i se nezmění, tedy $x \bmod n_i = x - n_i \bmod n_i$. Proto můžeme nahradit řešení x řešením $x \bmod n_1 n_2 ... n_k$ (totiž $x \bmod n_1 n_2 ... n_k = x - \alpha_i n_i$ pro vhodné nezáporné α_i).

Našli jsme tedy řešení, které splňuje podmínku $x < n_1 n_2 ... n_k$. Zbývá ukázat jeho jednoznačnost. Mějme $x, y < n_1 n_2 ... n_k$ dvě řešení. Ať je například $x \geq y$. Budeme zkoumat číslo $x - y$. Obě řešení dávají stejný zbytek modulo n_i, proto odečtením dostaneme $x - y \bmod n_i = 0$ pro všechna $i = 1, ..., k$. Jinými slovy $n_i | x - y$ pro všechna i. Podle Lemmatu 1.4 pak $n_1 n_2 ... n_k | x - y$, ale zároveň $x - y < n_1 n_2 ... n_k$. To je možné pouze v případě $x - y = 0$, tedy $x = y$. □

V dalších kapitolách budeme potřebovat následující zobrazení definované na přirozených číslech odvozené z dělitelnosti.

Definice. Zobrazení, které přirozenému číslu přiřazuje počet menších nesoudělných čísel se nazývá Eulerova funkce a značí se φ. Tedy $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = |\{m \in \mathbb{N} \ ; \ m \leq n \text{ a } \mathrm{NSD}(n, m) = 1\}|$.

Hodnotu Eulerovy funkce lze vypočítat z prvočíselného rozkladu daného čísla.

Lemma 1.6 *Platí $\varphi(1) = 1$. Je-li p^k mocnina prvočísla, $k > 0$, pak $\varphi(p^k) = p^k - p^{k-1}$. Jsou-li n a m nesoudělná, pak $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.*

Důkaz. První rovnost plyne přímo z definice.

Pro $k = 1$ v druhé rovnosti vychází $\varphi(p) = p^1 - p^0 = p - 1$, což je skutečně počet menších čísel nesoudělných s prvočíslem p. Pro obecné kladné k by podle tvrzení Lemmatu mělo číslo p^{k-1} značit počet menších čísel *soudělných* s p^k. Čísla soudělná s p^k jsou tvaru $p \cdot l$, neboť dělitelé p^k jsou právě $1, p, p^2, ..., p^k$. Proto je $\{pl \ ; \ l = 1, 2, ..., p^{k-1}\}$ množina všech menších soudělných čísel, velikost této množiny je p^{k-1} a tudíž $\varphi(p^k) = p^k - p^{k-1}$.

Ať je $\mathrm{NSD}(n, m) = 1$. Zaveďme zobrazení $f : \{l \ ; \ l = 0, 1, 2, ..., nm - 1\} \to \{(r, s) \ ; \ r = 0, 1, 2, ..., n-1 \text{ a } s = 0, 1, 2, ..., m-1\}$ takto: $f(l) = (l \bmod n, l \bmod m)$. Podle Věty 1.5 je f bijekce. Zbývá ukázat, že $\mathrm{NSD}(l, nm) = 1$ právě když $\mathrm{NSD}(l \bmod n, n) = 1$ a zároveň $\mathrm{NSD}(l \bmod m, m) = 1$. Pokud jsou $l \bmod n$ a n soudělná, pak jsou l a n soudělná a tudíž i l a nm soudělná. Pokud jsou naopak l a nm soudělná, pak jsou podle Lemmatu 1.4 buď l a n soudělná nebo l a m soudělná. Předpokládejme, že jsou například l a n soudělná. Snadno podle Lemmatu 1.1 zjistíme, že pak musejí být $l \bmod n$ a n soudělná. □

Přímý důsledek lemmatu:

Důsledek 1.7 *Je-li* $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ *rozklad čísla* n*, kde* $p_1, ..., p_r$ *jsou po dvou různá prvočísla a* $k_1, ..., k_r > 0$*, pak* $\varphi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1})...(p_r^{k_r} - p_r^{k_r - 1})$.

Příklad. Spočítejme Eulerovu funkci v čísle 1500. Rozklad na součin kladných mocnin různých prvočísel je $1500 = 2^2 \cdot 3 \cdot 5^3$ a tedy $\varphi(1500) = (2^2 - 2^1)(3^1 - 3^0)(5^3 - 5^2) = 2 \cdot 2 \cdot 100 = 400$.

Úkol. Najděte všechna $n \in \mathbb{N}$, pro která je $\varphi(n) = 4$. Najděte všechna $n \in \mathbb{N}$, pro která je $\varphi(n) = n - 2$.

1.B Kongruence a faktorizace celých čísel

Relaci dělitelnosti můžeme zavést na množině všech celých čísel. Tedy $m|n$ pro $n, m \in \mathbb{Z}$, pokud existuje $k \in \mathbb{Z}$ tak, že $n = km$. I v tomto případě zůstává v platnosti Lemma 1.1. Relace dělitelnosti ovšem již není slabě antisymetrická, například $1| - 1$ & $- 1|1$. Rozdíl ale není tak velký. Pokud $m|n$, pak pro absolutní hodnoty platí $|m| \leq |n|$, a proto z $m|n$ &$n|m$ vyplývá $|m| = |n|$. Naopak vždy $n| - n$. Čísla se stejnou absolutní hodnotou tedy v relaci dělitelnosti na $\mathbb{Z}$ splývají a pro nenulová $n, m \in \mathbb{Z}$ platí $m|n$ v $\mathbb{Z}$ právě když $|m| \mid |n|$ v $\mathbb{N}$.

Dělitelnost na $\mathbb{Z} \setminus \{0\}$ tedy "vypadá" stejně jako dělitelnost na $\mathbb{N}$. Dále platí $n|0$ pro každé $n \in \mathbb{Z}$. V dělitelnosti na $\mathbb{Z}$ tudíž přibude největší prvek 0. Z toho plyne, že základní vlastnosti dělitelnosti na přirozených číslech platí i pro celá čísla. Například:

Každá dvě celá čísla mají v $\mathbb{Z}$ *největšího společného dělitele i nejmenší společný násobek.*

Pro $n, m \in \mathbb{Z}$ tedy platí, že $\mathrm{NSD}(n, 0) = \pm n$ a $\mathrm{NSD}(n, m) = -\mathrm{NSD}(n, m) = \mathrm{NSD}(|n|, |m|)$.

Přeformulujme dělení se zbytkem pro $\mathbb{Z}$:

Dělení se zbytkem pro $\mathbb{Z}$**.** Pro každá dvě celá čísla n a m, $m \neq 0$, existují celá čísla k a r tak, že $n = km + r$ a přitom $|r| < |m|$.

Tvrzení lze snadno nahlédnout, podobně jako pro přirozená čísla. Zbytek sice není určen jednoznačně, ale přesto tato formulace zaručuje dobré fungování Eukleidova algoritmu v $\mathbb{Z}$.

Příklad. Zvolme $n = 5$ a $m = 3$. Máme dvě možné volby $k = 1$, pak $5 = 1 \cdot 3 + 2$ se zbytkem 2, a $k = 2$, pak $5 = 2 \cdot 3 - 1$ se zbytkem -1. Eukleidův algoritmus pak může mít různý průběh. Například

$5 = 1 \cdot 3 + 2$, zbytek $r_1 = 2$
$3 = 1 \cdot 2 + 1$, zbytek $r_2 = 1$
$2 = 2 \cdot 1 + 0$, tedy $\mathrm{NSD}(5, 3) = 1$

a nebo

$5 = 2 \cdot 3 - 1$, zbytek $r_1 = -1$
$3 = -3 \cdot -1 + 0$ a $\mathrm{NSD}(5,3) = -1$.
V prvním případě probíhá algoritmus pouze v přirozených číslech.

Pro pevné $k \in \mathbb{Z}$ zaveďme na celých číslech ekvivalenci *modulo* k, značíme $\equiv_k$, takto: $n \equiv_k m$ právě když $k|n-m$. Tedy $n \equiv_k m$ právě když n a m dávají stejné zbytky po dělení k.

Lemma 1.8 *Pro každé $k \in \mathbb{Z}$ je relace $\equiv_k$ ekvivalence na $\mathbb{Z}$. Přitom kdykoli n_1, n_2, m_1, $m_2 \in \mathbb{Z}$ jsou taková, že $n_1 \equiv_k n_2$ a $m_1 \equiv_k m_2$, pak $n_1 + m_1 \equiv_k n_2 + m_2$.*

Důkaz. Ukažme například, že $\equiv_k$ je tranzitivní. Ať je $n \equiv_k m$ a $m \equiv_k l$. Pak $n - l = (n-m) + (m-l)$ a podle Lemmatu 1.1 platí $k|(n-l)$.

Zbývá spočítat $(n_1 + m_1) - (n_2 + m_2) = (n_1 - n_2) + (m_1 - m_2)$, což opět podle Lemmatu 1.1 dává $k|(n_1 + m_1) - (n_2 + m_2)$. □

Jinými slovy, pokud v součtu vyměníme (některá) čísla za ekvivalentní, dostaneme ekvivalentní výsledek. To umožňuje provádět "ekvivalentní úpravy" jako při počítání s rovností. Pokud například $n \equiv m + l$, pak $n - l \equiv m$, neboť z reflexivity je $-l \equiv -l$.

V Lemmatu jsou vypsány vlastnosti *kongruence*.

Definice. Relace $\sim$ na $\mathbb{Z}$ se nazývá *kongruence*, pokud je $\sim$ ekvivalence a pro všechna $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ taková, že $n_1 \sim n_2$ a $m_1 \sim m_2$, platí $n_1 + m_1 \sim n_2 + m_2$.

Označení. Ať je $\sim$ ekvivalence na množině X. Označme $[x]_\sim = \{y \in X \ ; \ y \sim x\}$, tedy $[x]_\sim$ je třída prvku x v ekvivalenci $\sim$.

Všimli jsme si, že zbytek n mod m není v $\mathbb{Z}$ jednoznačně určený. Z rovnosti $n = lm + r$ ale plyne $r \equiv_m n$ a můžeme mluvit o (jediné) zbytkové třídě $[n]_{\equiv_m}$.

Zopakujme si, že systém všech tříd ekvivalence $\sim$ na množině X tvoří *rozklad množiny* X. To znamená, že pro každé $x, y \in X$ platí buď $[x]_\sim = [y]_\sim$ nebo $[x]_\sim \cap [y]_\sim = \emptyset$, a přitom (samozřejmě) $X = \bigcup_{x \in X} [x]_\sim$.

Příklad. Rozklad podle kongruence $\equiv_1$ má jedinou třídu, tedy všechna čísla jsou kongruentní. Rozklad podle kongruence $\equiv_0$ má pouze jednoprvkové třídy, tedy žádná dvě různá čísla nejsou kongruentní.

Popis kongruencí na $\mathbb{Z}$. Ukážeme, že $\equiv_k$, $k \in \mathbb{Z}$, jsou jediné kongruence na celých číslech.

Nejdříve si uvědomme, že každá kongruence $\sim$ na $\mathbb{Z}$ je jednoznačně určená třídou 0, tedy množinou $[0]_\sim$. Totiž pro $n, m \in \mathbb{Z}$ platí, že $n \sim m$ právě když $n - m \sim 0$. Pokud je $n - m \sim 0$, pak (podle definice) $k|n-m$ a tedy $n \sim m$. Pokud naopak $n \sim m$, pak $k|n-m$ a tedy $n - m \sim 0$. Vidíme, že $[n]_\sim = \{n + l \ ; \ l \sim 0\}$.

Zbývá tedy pro danou kongruenci $\sim$ najít $k \in \mathbb{Z}$ tak, aby $[0]_\sim = \{t \cdot k \ ; \ t \in \mathbb{Z}\}$. Pak bude z jednoznačnosti $\sim = \equiv_k$.

Pokud je $[0]_\sim = \{0\}$, pak $\sim = \equiv_0$.

Ať $[0]_\sim \neq \{0\}$ a ať je $k \in [0]_\sim$ prvek s nejmenší nenulovou absolutní hodnotou. Je-li $l \sim 0$, pak je i $l + k \sim k$, neboť $k \sim k$, a tedy $l + k \sim 0$. Z $l \sim 0$ také plyne $l - k \sim -k$, tedy z $0 \sim k$ plyne $-k \sim 0$ a z tranzitivity $l - k \sim 0$. Ukázali jsme inkluzi $\{t \cdot k \ ; \ t \in \mathbb{Z}\} \subseteq [0]_\sim$.

Dokažme opačnou inkluzi. Zvolíme $l \in [0]_\sim$ a budeme dokazovat, že $k|l$. Vydělme $l = sk + r$ se zbytkem r, $|r| < |k|$. Máme $sk + r = l \sim 0$, tudíž $r = l - sk \sim -sk$. Jak jsme již dokázali $-sk \sim 0$, proto $r \sim 0$, což díky volbě k nutně dává $r = 0$. Vidíme, že $l = sk$ a $k|l$.

Označení. Pro $T, S \subseteq \mathbb{Z}$ dvě podmnožiny $\mathbb{Z}$ položíme $T + S = \{n + m \ ; \ n \in T, \ m \in S\}$ (součet podmnožin po prvcích).

Faktorizace. Ať je $\sim$ kongruence na $\mathbb{Z}$ (tedy $\sim = \equiv_k$ pro vhodné k) a ať T a S jsou třídy $\sim$. Platí, že $T + S$ je opět třída kongruence $\sim$.

Zvolme $n, n_1 \in T$ a $m, m_1 \in S$. Z vlastností kongruence plyne $n + m \sim n_1 + m_1$ a tedy všechny prvky $T + S$ jsou navzájem kongruentní. Je-li naopak $l \sim n + m$, pak $l - n \sim m$ a dostaneme $l = n + (l - n) \in T + S$.

Ukázali jsme, že existuje třída R kongruence $\sim$ taková, že $T + S = R$. To nám umožňuje zavést *sčítání tříd* $\sim$. Množina $\{T \ ; \ T \text{ třída } \sim\}$ všech tříd kongruence $\sim$ se sčítáním tříd se nazývá *faktor* $\mathbb{Z}$ *podle kongruence* $\sim$. Pro faktor budeme používat značení $\mathbb{Z}/\sim$.

Příklady. 1) Kongruence $\equiv_0$ má pouze jednoprvkové třídy a proto $\mathbb{Z}/\equiv_0 = \mathbb{Z}$.

2) Všechna čísla jsou kongruentní v $\equiv_1$ a proto má faktor $\mathbb{Z}/\equiv_1$ jediný prvek, označme ho T, a platí $T + T = T$.

3) Podívejme se podrobněji na kongruenci $\equiv_3$. Označme pro zkrácení v tomto příkladu $\sim = \equiv_3$. Třída $[0]_\sim$ má prvky

$$\ldots\ldots, \ -9, \ -6, \ -3, \ 0, \ 3, \ 6, \ 9, \ \ldots\ldots$$

Číslo 1 není prvkem $[0]_\sim$ a proto $[1]_\sim \cap [0]_\sim = \emptyset$. Prvky $[1]_\sim$ jsou

$$\ldots\ldots, \ -8, \ -5, \ -2, \ 1, \ 4, \ 7, \ 10, \ \ldots\ldots$$

Platí $[1]_\sim = \{1\} + [0]_\sim$. Dále zbývá například číslo 2. Prvky $[2]_\sim$ jsou

$$\ldots\ldots, \ -7, \ -4, \ -1, \ 2, \ 5, \ 8, \ 11, \ \ldots\ldots$$

Opět $[2]_\sim = \{2\} + [0]_\sim$.

Získali jsme $\mathbb{Z} = [0]_\sim \cup [1]_\sim \cup [2]_\sim$ rozklad celých čísel. Faktor $\mathbb{Z}/\sim$ má tedy tři prvky a sčítání tříd můžeme zapsat do tabulky:

$+$	$[0]_\sim$	$[1]_\sim$	$[2]_\sim$
$[0]_\sim$	$[0]_\sim$	$[1]_\sim$	$[2]_\sim$
$[1]_\sim$	$[1]_\sim$	$[2]_\sim$	$[0]_\sim$
$[2]_\sim$	$[2]_\sim$	$[0]_\sim$	$[1]_\sim$

Do tabulky vyplňujeme součty tříd v levém sloupci a v horním řádku. Vidíme, že například $[1]_\sim + [2]_\sim = [3]_\sim = [0]_\sim$. Pro sčítání tříd platí $[i]_\sim + [j]_\sim = [r]_\sim$, kde r je nějaký zbytek $i + j$ modulo 3.

Zbytek 1 mod 3 není v $\mathbb{Z}$ jednoznačně určený. Máme $1 = 0 \cdot 3 + 1$ nebo $1 = 1 \cdot 3 - 2$. Oba zbytky 1 a -2 jsou samozřejmě kongruentní modulo 3.

Tvar faktoru $\mathbb{Z}/\equiv_k$. V tomto odstavci bude $\sim$ značit $\equiv_k$ pro pevně zvolené $k \in \mathbb{Z}$. Víme, že dělitelnost nerozlišuje znaménko, proto můžeme předpokládat, že $k \geq 0$.

Třída $[0]_\sim$ má prvky

$$....., \ -3k, \ -2k, \ -k, \ 0, \ k, \ 2k, \ 3k, \ .....$$

Třída $[1]_\sim$ má prvky

$$....., \ -3k+1, \ -2k+1, \ -k+1, \ 1, \ k+1, \ 2k+1, \ 3k+1, \ .....$$

Třída $[i]_\sim$ má prvky

$$....., \ -3k+i, \ -2k+i, \ -k+i, \ i, \ k+i, \ 2k+i, \ 3k+i, \ .....$$

Vidíme, že $\mathbb{Z} = \bigcup_{i=0,\ldots,k-1}[i]_\sim$ je rozklad celých čísel a faktor $\mathbb{Z}/\sim$ má tedy k prvků. Faktor $\mathbb{Z}/\sim$ se obvykle značí $\mathbb{Z}_k$ (někdy také $\mathbb{Z}/k\mathbb{Z}$).

Místo počítání se třídami faktoru v tomto případě obvykle pracujeme s *reprezentací tříd vybranými prvky*. Můžeme si představit $\mathbb{Z}_k$ jako množinu $\{0, 1, 2, ..., k-1\}$ se sčítáním $i + j = (i + j) \bmod k$, kde zbytek modulo k volíme *nezáporný*. Vyplňme část tabulky sčítání ve faktoru pomocí reprezentantů:

$+$	0	1	2	.....	$k-3$	$k-2$	$k-1$
0	0	1	2	.....	$k-3$	$k-2$	$k-1$
1	1	2	3	.....	$k-2$	$k-1$	0
2	2	3	4	.....	$k-1$	0	1
.							
.							
.							
$k-3$	$k-3$	$k-2$	$k-1$	.....	$k-6$	$k-5$	$k-4$
$k-2$	$k-2$	$k-1$	0	.....	$k-5$	$k-4$	$k-3$
$k-1$	$k-1$	0	1	.....	$k-4$	$k-3$	$k-2$

Úkol. Ukažte, že $\{5, -4, 12, 3, -6\}$ je reprezentace tříd kongruence $\equiv_5$ vybranými prvky. Vyplňte tabulku sčítání ve faktoru pomocí reprezentantů.

$+$	5	-4	12	3	-6
5					
-4					
12			$?$		
3					
-6					