Chapter I

Čínská věta o zbytcích

I.1

I.1.1 Věta. (Čínská věta o zbytcích) Nechť $n_1, \ldots, n_k$, $k \geq 2$, jsou po dvou nesoudělná nenulová celá čísla, $m_1 = n_2 n_3 \cdots n_k$, $m_2 = n_1 n_3 \cdots n_k$, $\ldots$, $m_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$, $\ldots$, $m_k = n_1 \cdot n_{k-1}$. Potom:

(i) $mod(n_i, m_i) = 1$ pro každé $i = 1, 2, \ldots, k$ a existují čísla b_i, c_i taková, že $1 = b_i n_i + c_i m_i$.

(ii) Jsou-li $a_1, \ldots, a_k \in \mathbb{Z}$ a $a = a_1 c_1 m_1 + a_2 c_2 m_2 + \cdots + a_k c_k m_k$, pak $n_i \mid a - a_i$ pro každé $i = 1, 2, \ldots, k$.

(iii) Je-li $a \in \mathbb{Z}$, pak $n_i \mid a - a_i$ pro všechna i, právě když $n = n_1 n_2 \cdots n_k \mid a - a'$ (t. j. $a' \equiv a \ (mod\ n)$).

Důkaz. (i) Číslo m_i je součinem čísel nesoudělných s n_i. Tedy i n_i je nesoudělné s m_i. Existence čísel b_i, c_i vyplývá z rozšířeného Euklidova algoritmu. Je-li $2k+1$, $k \geq 1$, liché číslo, pak $0, 1, \ldots, k, -k, -k+1, \ldots, -1$ je též úplná redukovaná soustava zbytků modulo n. Je-li $n = 2k$, $k \geq 1$, sudé číslo, pak takovou soustavu tvoří čísla $0, 1, \ldots, k-1, -k, -k+1, \ldots, -1$.

Libovolná množina celých čísel je redukovaná soustava zbytků modulo 0 a jediná úplná soustava takových zbytků je celá množina $\mathbb{Z}$ všech celých čísel. Naopak libovolná neprázdná množina celých čísel je úplná soustava zbytků modulo 1 a redukované soustavy zbytků modulo 1 jsou prázdná množina a jednoprvkové množiny.

(ii) Zřejmě $n_i \mid m_j$ pro $j \neq i$, čili stačí věřit, že $n_i \mid a_i c_i m_i - a_i$. Je však $a_i c_i m_i = a_i - a_i b_i n_i$ a $a_i c_i m_i - a_i = -a_i b_i n_i$.

(iii) Čísla $n : 1, \ldots, n_k$ jsou po dvou nesoudělná, čili $non(n_1, \ldots, n_k) = n$. Zbytek je jasný. □

I.1.2 Poznámka. Předchozí věta má konstruktivní charakter. Jsou-li dána čísla $a_1, \ldots a_k$, pak číslo a lze získat pomocí Rozšířeného Euklidova Algoritmu

(viz **??**). Částečné případy této věty se objevily již na konci třetího století v pojednání „Matematickýá příručka mistra Suna“ jakožto druh hádanky (viz I.1.3(ii)). Hlubší výsledky v tomto směru byly publikovány v roce 1247 ve spisu „Matematické pojednání v devíti částech“, které obsahuje v devíti sekcích po devíti problémech (celkově tedy 81 tematických okruhů). Tento spis sepsal čínský matematik Č'in Čiu-Šao (1202–1261). Také indičtí počtáři se této problematice věnovali (Aryabhata, 476–550, v šestém století a Brahmagupta pak v století sedmém). Větu o zbytcích lze také nalézt v „Početnici“ sepsané roku 1202 Leonardem Bonaccim z Pisy (známým též jako Fibonacci). Kongruenční rovnosti lze nalézt již u starých Řeků (např. Nicomachus v prvním století).

I.1.3 Příklad. (i) (Hádanka Mistra Suna) Nalezněmež celé číslo a takové, že $a \equiv 1 \ (mod\ 3)$, $a \equiv 2 \ (mod\ 5)$ a $a \equiv 3 \ (mod\ 7)$.
Je tedy $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, $m_1 = 35$, $m_2 = 21$ a $m_3 = 15$. Dále $1 = 12n_1 - m_1 = -4n_2 + m_2 = -2n_3 + m_3$, čili $a = -m_1 + 2m_2 + 3m_3 = -35 + 42 + 45 = 52$. Snadná kontrola ukazuje, že $3 \mid 51 = 52 - 1$, $5 \mid 50 = 52 - 2$ a $7 \mid 49 = 52 - 3$. Našim konvergenčním rovnostem vyhovují také čísla $157 = 52 + 105$ a $-53 = 52 - 105$.

(ii) Nechť $n_1 = 2$, $n_2 = 3$ a $n_3 = 5$. Je $m_1 = 15$, $m_2 = 10$, $m_3 = 6$, $1 = -7n_1 + m_1 = -3n_2 + m_2 = m_3$. Nyní $a = 15a_1 + 10a_2 + 6a_3$. Například je-li $a_1 = a_2 = a_3 = 1$, pak dostaneme $a = 31$. Avšak číslo $1 = 31 - 30$ snadno vyhoví

Nechť $u = 123684$ a $v = 413456$. Potom $u \equiv 33 \ (mod\ 99)$, $u \equiv 8 \ (mod\ 98)$, $u \equiv 9 \ (mod\ 97)$, $u \equiv 89 \ (mod\ 95)$, $v \equiv 32 \ (mod\ 99)$, $v \equiv 92 \ (mod\ 98)$, $v \equiv 42 \ (mod\ 97)$, $v \equiv 16 \ (mod\ 95)$. Toto vše zjistíme postupem popsaným v důkazu věty **??**. Dalším postupem zjistíme, že $u + v \equiv 65 \ (mod\ 99)$, $u + v \equiv 2 \ (mod\ 98)$, $u + v \equiv 51 \ (mod\ 97)$, $u + v \equiv 10 \ (mod\ 95)$. Nyní použijeme větu **??**.

Buď $n_1 = 99$, $n_2 = 98$, $n_3 = 97$, $n_4 = 95$. Pomocí Euklidova algoritmu můžeme zjistit, že čísla n_1, n_2, n_3, n_4 jsou po dvou nesoudělná. Nicméně tento fakt je zřejmý téměř ihned, neboť $99 = 3^2 \cdot 11$, $98 = 2 \cdot 7^2$, 97 je prvočíslo a $95 = 5 \cdot 19$. Dále máme $n = n_1 n_2 n_3 n_4 = 89403930$, $m_1 = 903070$, $m_2 = 912285$, $m_3 = 921690$, $m_4 = 941094$.

Teď však potřebujeme nalézt c_1 takové, že $c_1 m_1 \equiv 1 \ (mod\ 99)$. Je-li však $m_1 \equiv t_1 \ (mod\ 99)$, kde $0 \leq t_1 < 99$, pak $c_1 t_1 \equiv 1 \ (mod\ 99)$. Euklidovým algoritmem zjistíme, že $t_1 = 91$. Tedy $c_1 m_1 = 903070 c_1 \equiv 91 c_1 \equiv 1 \ (mod\ 99)$. Řešíme poslední kongruenční rovnici a získáme $c_1 = 37$ (I ...). Takže $37 m_1 \equiv 1 \ (mod\ 99)$. Stejným postupem nacházíme kongruenční rovnosti $c_2 m_2 = 912285 c_2 \equiv c_2 \equiv 1 \ (mod\ 98)$, $c_2 = 33$, $35 m_2 \equiv 1 \ (mod\ 98)$, $c_3 m_3 = 921690 c_3 \equiv 93 c_3 \equiv 1 \ (mod\ 97)$, $c_3 = 24$, $24 m_3 \equiv 1 \ (mod\ 97)$,

$m_4 = 941094c_4 \equiv 24c_4 \equiv 1 \ (mod\ 95)$, $c_4 = 4$, $4m_4 \equiv 1 \ (mod\ 97)$.

Máme $c_1m_1 = 37 \cdot 903070 = 33413590$, $c_2m_2 = 33 \cdot 912285 = 30105405$, $c_3m_3 = 24 \cdot 921690 = 22120560$, $c_4m_4 = 4 \cdot 941094 = 3764396$.

Nyní volme $a_1 = 65$, $a_2 = 2$, $a_3 = 51$, $a_4 = 10$ (důvod viz výše) a spočteme součet $a = a_1c_1m_1 + a_2c_2m_2 + a_3c_3m_3 + a_4c_4m_4$. Pomocí mechanických prostředků (a třeba i ručně) dostaneme $a = 2171883350 + 60210810 + 1128148560 + 37643760 = 3397886480$. Ovšem toto číslo je velké a my počítáme modulo $n = 89403930$. Po dělení se zbytkem zjistíme, že $a \equiv 537140 \ (mod\ n)$. Je totiž $a = 38n + 537140$.

Podle Čínské věty o zbytcích je $u + v \equiv 537140 \ (mod\ n)$. Jinak napsáno $89403930 \mid u + v - 537140$ a $123684 + 413456 = u + v = 89703930w + 537140$ pro vhodné $w \geq 0$. Asi hned vidíme, že $w = 0$ a tak $u + v = 537140$, což jsme mohli ovšem zjistit ručně v nepatrném čase. Avšak předchozí zdlouhavý postup ilustruje aritmetiku používanou některými mechanickými prostředky.

I.1.4 Příklad. Nechť $k \geq 2$ a nechť $p_1, \ldots, p_k$ je k různých prvočísel (vybraných libovolně). Podle I.1.1 existuje celé celé číslo a takové, že $a \equiv -i + 1 \ (mod\ p_i^2)$ pro každé $i = 1, 2, \ldots, k$. Tedy $p_i^2 \mid a + i - 1$, a tak žádné z po sobě jdoucích čísel $a, a + 1, \ldots, a + k - 1$ není bezčtvercové (a tím spíše ne prvočíslo).

Čísla 8, 9 tvoří první dvojici po sobě jdoucích čísel, která nejsou bezčtvercová. Další dvojicí jsou čísla 24, 25. Teď ale nalezněme trojici.

Například hledejme a takové, že $a \equiv 0 \ (mod\ 4)$, $a \equiv -1 \ (mod\ 9)$ a $a \equiv -2 \ (mod\ 25)$. Je $n_1 = 4$, $n_2 = 9$, $n_3 = 25$, $m_1 = 225$, $m_2 = 100$, $m_3 = 36$ a $1 = -4 \cdot 56 + 225 = -9 \cdot 11 + 100 = 13 \cdot 25 - 9 \cdot 36$. Takže $a = 0 - 100 + 18 \cdot 36 = 548$. A hle, $548 = 4 \cdot 127$, $549 = 9 \cdot 61$ a $550 = 25 \cdot 22 = 25 \cdot 2 \cdot 11$ (127 a 61 jsou prvočísla). Ještě si všimněme, že 547 je i prvočíslo a $551 = 19 \cdot 29$ je bezčtvercové. Čtveřici jsme tudíž nenašli.

Nejmenší dvojicí neobsahující prvočíslo je dvojice 8, 9. Trojice pak 8, 9, 10, čtveřice 24, 25, 26, 27 a pětice 24, 25, 26, 27, 28. Nejmenší trojicí po sobě jdoucích kladních čísel, která jsou bezčtvercová, je trojice 48, 49, 50.

I.1.5 Věta. Nechť $n_1, \ldots, n_k$, $k \geq 2$ jsou nenulová celá čísla. Následující podmínky jsou ekvivalentní pro libovolná čísla $a_1, \ldots, a_k \in \mathbb{Z}$:

(i) $nsd(n_i, n_j)a_i - a_j$ pro všechna $1 \leq i, j \leq k$ $(i \neq j)$.

(ii) Existuje číslo $a \in \mathbb{Z}$ takové, že $a \equiv a_i \ (nsd\ n_i)$ pro všechna $i = 1, 2, \ldots, k$.

Důkaz. (i) implikuje (ii). Budeme postupovat indukcí podle k. Buď nejblíže $k = 2$. Je $r = nsd(n_1, n_2) = bn_1 + cn_2$ pro vhodná celá čísla b, c. Ovšem $a_1 - a_2 = dr$, $d \in \mathbb{Z}$, čili $a_1 - a_2 = dbn_1 + dcn_2$ a položíme $a = a_1 - dbn_1$. Je $a = a_2 + dcn_2$ a ihned vidíme, že $n_1 \mid a - a_1$ a $n_2 \mid a - a_2$.

Nyní buď $k \geq 2$. Podle indukčního předpokladu existuje $a' \in \mathbb{Z}$ takové, že $n_i \mid a - a_i$ pro $i = 1, 2, \ldots, k$. Pro každé $i = 1, 2, \ldots, k$ je $nsd(n_i, n_{k+1} \mid a_i - a_{k+1}$, a tudíž $nsd(n_i, n_{k+1} \mid a' - a_{k+1}$. Odtud $nsd(nsn(n_1, \ldots, n_k), n_{k+1} = nsn(nsd(n_1, n_{k+1}), \ldots, nsd(n_k, n_{k+1})) \mid a' - a_{k+1}$.

Nyní podle již dokázaného případu (kdy $k = 2$) existuje číslo $a \in \mathbb{Z}$ tak, že $a \equiv a'$ $(mod\ ndn(n_1, \ldots, n_k))$, $a \equiv a_{k+1}$ $(mod\ n_{k+1})$. Z první kongruenční rovnosti ihned plyne $a \equiv a'$ $(mod\ n_i)$ pro každé $i = 1, 2, \ldots, k$. Pak ovšem $a \equiv a_i$ $(mod\ n_i)$ (neb $n_i \mid a'a_i$).

(ii) implikuje (i). Tato implikace je velmi snadná. Je totiž $n_i \mid a - a_i$, $n_j \mid a - a_j$, a tudíž $nsd(n_i, n_j) \mid (a - a_j \mid -(a - a_i) = a_i - a_j$. □

I.1.6 Poznámka. I předchozí věta má vlastně konstruktivní důkaz, který dává návod, jak číslo a nalézt. Máme ovšem k dispozici i důkazy existenční. Ilustrujme si to na případě $k = 2$.

Nechť n_1, n_2 jsou kladná čísla, $r = nsd(n_1, n_2 2)$ a $s = nsn(n_1, n_2)$. Podle **??** je $rs = n_1 n_2 = n$. Uvažujme K množinu uspořádaných dvojic čísel (i, j) takových, že $0 \leq i < n_1$, $0 \leq j < n_2$ a $r \mid i - j$. Chceme se přesvědčit o tom, že množina K obsahuje přesně s různých dvojic.

Předně je $n_2 = t$ pro nějaká $t \geq 1$. Pro každé i a v, kde $0 \leq i < n_i$ a $0 \leq v < t$, položme $b(i, v) = [vr + i]_{n_2}$ (viz **??**). Pak ovšem $r \mid i - b(i, v)$ (neboť $r \mid n_2 ar \mid vr$) a $(i, b(i, v)) \in K$. Kolik je ale dvojic tohoto typu? To rychle zjistíme.

Nechť i_1, i_2 a v_1, v_2 jsou taková čísla (s příslušnými vlastnostmi), že skýtají tu samou dvojici. Tedy $(i_1, b(i_1, v_1)) = (i_2, b(i_2, v_2))$, z čehož ihned plyne $i_1 = i_2 = i$, $tr = n_2 \mid (v_1 - v_2)r, t \mid v_1 - v_2$, $(v_1 - v_2) < t$ a $v_1 = v_2$. Ověřili jsme, že $i_1, b(i_1, v_1)) \neq (i_2, b(i_2, v_2))$ pro $(i_1, v_1) \neq (i_2, v_2)$. Celkový počet různých dvojic typu $(i, b(i, v))$ je tedy $n_1 t$. Jelikož $rs = n_1 n_2 = n_1 rt$, je $s = n_1 t$ a vidíme, že $|K| \geq s$.

Nechť $(i, j) \in K$. Je $|i - j($ $| = wr$ pro nějaké $w \geq 0$, a tedy buďto $j = i + wr$ a nebo $j = i - wr$. V prvním případě je zřejmě $w < t$ a $(i, j) = (i, b(i, w))$. V druhém případě buď $u = [-w]_t$. Pak $0 \leq u < t$, $t \mid w + u$, $n_2 = tr \mid (t - w - u)r$ a $i + ur \equiv i + (t + w)r \equiv i - wr = j$ $(mod\ n_2)$. Takže $n_2 \mid i + wr - j$, z čehož plynou rovnosti $j = b(i, u)$ a $(i, j) = (i, b(i, u))$.

Nyní víme, že množina K sestává prostě z dvojic tvaru $(i, b(i, u))$. Počet těchto dvojic je s, a tudíž $|K| = s$.

Pro k takové, že $0 \leq k < s$ buď $C(k) = ([k]_{n_1}, [k]_{n_2})$. Jelikož $n_1 \mid k - [k]_{n_1}$ a $n_2 \mid k - [k]_{n_2}$, tak $r \mid [k]_{n_1} - [k]_{n_2}$, a tedy dvojice $C(k) \in K$. Je-li $0 \leq l < s$ takové, že $C(k) = C(l)$, pak $n_1 \mid k - [k]_{n_1}$, $n_1 \mid l - [k]_{n_1}$, čili $n_1 \mid k - l$. Symetricky $n_2 \mid k - l$ a tudíž $k - l \in sn(n_1, n_2)$. Pak ale $s \mid k - l$ a $k = l$. Je tedy jasné, že C je injektivní (čili prosté) zobrazení intervalu $\{0, 1, \ldots, s - 1\}$ do množiny K. Ta má ale s prvků, a tak zobrazení C je bijekce.

Nechť $a_1, a_2 \in \mathbb{Z}$ jsou taková čísla, že $r \mid a_1 - a_2$. Potom $([a_1]_{n_1}, [a_2]_{n_2}) \in K$ a existuje a, $0 \leq a < s$ tak, že $[a_1]_{n_1}$ a $[a_2]_{n_2} = [a]_{n_1}$, neboli $n_1 \mid a - a_1$ a $n_2 \mid a - a_2$.

I.1.7 Příklad. Věta I.1.5 zobecňuje Čínskou větu o zbytcích a lze ji obdobně používat. Například by se hodila při řešení následující úlohy (srovnej s I.1.4):

Jest nám nalézti aspoň jedno číslo a takové, že $2 \cdot 9 = 18 \mid a$, $2 \cdot 25 = 50 \mid a + 2$, $2 \cdot 49 = 98 \mid a + 4$. Tuto úlohu si vyřešíme, ale budeme postupovat přímou metodou.

Předně $a = 18v$. Jelikož $a + 2 = 50u$, tak porovnáním dekadických zápisů daných čísel vidíme, že $v = 10k + 1$ a nebo $v = 10k + 6$, $k \geq 0$. Zkusme štěstí a volme $v = 10k + 1$, $a = 180k + 18$, $a + 2 = 180k + 20 \equiv 0 \ (mod\ 50)$, $3k + 2 \equiv 0 \ (mod\ 5)$ a $k = 10l + 1, 6$. Opět zkusme $k = 10l + 1$. Pak $98 \mid a + 4 = 180l + 202$, $98 \mid 820l + 6$, $49 \mid 410l + 3$, $49 \mid 18l + 3 = 3(6l + 1)$, čili $3(6l+1) = 49w = 49 \cdot 3 \cdot z$, $6l + 1 = 49z$. Tato poslední rovnost je však splněna pro $l = 1 = z$. Pak dostaneme $a = 8 \cdot 1800 + 198 = 14400 + 198 = 14598$. A vskutku, $14598 = 18 \cdot 811$, $14600 = 50 \cdot 292$, $14602 = 98 \cdot 149$. Naší úloze vyhoví také $a = 102798$ či $a = -73602$.