Kapitola 2

Kongruence, modulární inverze

2.1 Opakování z přednášky

Přirozené číslo n nazveme *prvočíslem*, jsou-li jeho děliteli pouze 1 a p. Číslo, které není prvočíslem nazýváme *složeným*. Množinu všech prvočísle značíme zpravidla $\mathbb{P}$.

Věta (Základní věta aritmetiky)**.** *Libovolné číslo $n \in \mathbb{N}$ lze rozložit na součin prvočísel, a to jednoznačně až na pořadí činitelů.*

Poznámka. Prvočíslo p je součinem jediného prvočísla, 1 je součinem prázdné množiny prvočísel.

Dávají-li a a b stejný zbytek po dělení m, nazýváme je *kongruentními modulo m*, což píšeme $a \equiv b \pmod{m}$. Máme následující charakterizaci kongruence.

$$a \equiv b \pmod{m} \iff a = b + m\,k \text{ pro nějaké } k \in \mathbb{Z} \iff m \mid a - b$$

Dále je kongruence modulo m *reflexivní*, tj. $a \equiv a$, *symetrická*, tj. $a \equiv b \Rightarrow b \equiv a$, a *tranzitivní*, tj. $a \equiv b$ a $b \equiv c$ dává $a \equiv c$. Jedná se tedy o relaci ekvivalence. Dále platí $a \equiv b \pmod{m}$ dává $a \equiv b + k \cdot m \pmod{m}$.

Kongruence podle téhož modulu lze sčítat a násobit stejným číslem, lze je násobit i umocnit na totéž číslo. Dále je-li $(m, k) = 1$, pak

$$a\,k \equiv b\,k \pmod{m} \Rightarrow a \equiv b \pmod{m}.$$

Pro $n \mid m$ nám kongruence modulo m dává kongruenci modulo m. Obráceně dostáváme m/n různých řešení, $a \equiv b$ nebo $a \equiv b + n$, $\ldots$, $a \equiv b + (m/n - 1)n \pmod{m}$. Dále je-li $[m_1, m_2] = m1\,m_2/(m_1, m_2)$, máme

$$a \equiv b \pmod{m_1} \text{ i } \pmod{m_2} \iff a \equiv b \pmod{[m_1, m_2]}.$$

Stejným číslem můžeme násobit i dělit obě strany *a modul*, tj.

$$a \cdot k \equiv b \cdot k \pmod{m \cdot k} \iff a \equiv b \pmod{m}.$$

Číslo b nazýváme *inverzí* k číslu a *modulo m* (nebo také modulární inverzí), jestliže

$$a \cdot b \equiv 1 \pmod{m}.$$

Věta. *Modulární inverze k a modulo m existuje jediná právě tehdy, když $(a, m) = 1$.*

Důkaz. Zobrazení násobení a je díky vlastnosti dělení kongruencí injektivní, má tedy zbytková třída reprezentovatelná vzor. Protože je počet tříd m, jedná se o bijekci a vzor je jediný.

Obráceně, pokud jsou a a m soudělné, násobení a není injektivní a nulová třída má nenulový vzor. Existuje tedy nenulové b tak, že $a \cdot b \equiv 0 \pmod{m}$ a inverze nemůže existovat. □

Věta (Čínská zbytková věta (Sun-Tsu))**.** *Nechť $m_1, \ldots m_k \in \mathbb{N}$ jsou po dvou nesoudělné. Poté má soustava*

$$x \equiv c_i \pmod{m_i}$$

pro í $= 1, \ldots, k$, $c_i \in \mathbb{Z}$ jediné řešení modulo $m_1 \cdot \cdots \cdot m_k$.

2.2 Příklady řešené na cvičení

Příklad 2.1. Najděte zbytek po dělení čísla 5^{30} číslem 91, to samé pro $5^{3\,000\,000}$.

Řešení. Můžeme počítat mocniny 5 modulo 91. Máme $5^2 = 25$, dále

$$\begin{aligned}
5^3 &= 125 \equiv 34 & 5^8 &\equiv 47 \cdot 5 = 235 \equiv -38 \\
5^4 &\equiv 34 \cdot 5 = 170 \equiv -12 & 5^9 &\equiv -38 \cdot 5 = -190 \equiv -8 \\
5^5 &\equiv -12 \cdot 5 = -60 \equiv 31 & 5^{10} &\equiv -8 \cdot 5 = -40 \\
5^6 &\equiv 31 \cdot 5 = 155 \equiv 64 & 5^{11} &\equiv -40 \cdot 5 = -200 \equiv -18 \\
5^7 &\equiv 64 \cdot 5 = 320 \equiv 47 & 5^{12} &\equiv -18 \cdot 5 = -90 \equiv 1
\end{aligned}$$

vše modulo 91. Víme tedy, že $5^{12} \equiv 1 \pmod{91}$, tudíž

$$5^{30} = \left(5^{12}\right)^2 \cdot 5^6 \equiv 5^6 \equiv 64 \pmod{91}.$$

Jelikož 3 000 000 je dělitelné 12, máme rovnou $5^{3\,000\,000} \equiv 1 \pmod{91}$. △

Jiné řešení. Máme rozklad $91 = 7 \cdot 13$. Víme, že

$$\begin{aligned}
5^2 \equiv -1 \pmod{13} &\Rightarrow 5^{30} \equiv (-1)^{15} = -1 \pmod{13} \\
5 \equiv -2 \text{ a } 2^3 \equiv 1 \pmod{7} &\Rightarrow 5^{30} \equiv (-2)^{30} = 2^{30} \equiv 1^{10} = 1 \pmod{7}
\end{aligned}$$

Tudíž je 5^{30} kongruentní -1 modulo 13 a 1 modulo 7.

Předpokládejme $x \in \{0, \ldots, 90\}$ takové, že $5^{30} \equiv x \pmod{91}$. Poté $5^{30} \equiv x \pmod{13}$ i $\pmod{7}$. Podle Čínské zbytkové věty existuje jediné takové x mezi 0 a 90. Můžeme například procházet $7k + 1$ a hledat mezi nimi nějaké číslo kongruentní -1 modulo 13.

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$7k+1$	1	8	15	22	29	36	43	50	57	64	71	78	85

Vidíme, že $64 = 13 \cdot 5 - 1$, takže hledaným zbytkem je číslo 64.

U čísla $5^{3\,000\,000}$ je počítání jednodušší. Modulo 7 spočítáme stejně zbytek 1, zbývá spočítat zbytek modulo 13.

$$5^{3\,000\,000} \equiv (-1)^{1\,500\,000} = 1 \pmod{13}$$

Máme tedy hned (použijeme opět Čínskou zbytkovou větu) $5^{3\,000\,000} \equiv 1 \pmod{91}$. △

Příklad 2.2. Dokažte, že $25 \mid 72^{2n+2} - 47^{2n} + 28^{2n-1}$ pro každé $n \in \mathbb{N}$.

Řešení. Víme, že

$$\begin{aligned} 72 &\equiv -3 \pmod{25} \\ 47 &\equiv -3 \pmod{25} \\ 28 &\equiv 3 \pmod{25} \end{aligned}$$

tudíž

$$\begin{aligned} 72^{2n+2} - 47^{2n} + 28^{2n-1} &\equiv (-3)^{2n+2} - (-3)^{2n} + 3^{2n-1} = \\ &= 3^{2n+2} - 3^{2n} + 3^{2n-1} = 3^{2n-1}(27 - 3 + 1) = 3^{2n-1} \cdot 25 \equiv 0 \pmod{25} \end{aligned}$$

což jsme měli dokázat. △

Příklad 2.3. Spočtěte 35^{-1} modulo 132.

Řešení. Počítáme $(132, 35)$ a Bézoutovy koeficienty (například) pomocí úprav matice.

$$\begin{pmatrix} 1 & 0 & 132 \\ 0 & 1 & 35 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & 27 \\ 0 & 1 & 35 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & 27 \\ -1 & 4 & 8 \end{pmatrix} \sim \begin{pmatrix} 4 & -15 & 3 \\ -1 & 4 & 8 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 4 & -15 & 3 \\ -9 & 34 & 2 \end{pmatrix} \sim \begin{pmatrix} 13 & -49 & 1 \\ -9 & 34 & 2 \end{pmatrix} \sim \begin{pmatrix} 13 & -49 & 1 \\ -35 & 132 & 0 \end{pmatrix}$$

Máme tedy $13 \cdot 132 - 49 \cdot 35 = 1$, neboli $-49 \cdot 35 \equiv 1 \pmod{132}$. Hledanou modulární inverzí je tedy $-49 \equiv 83 \pmod{132}$. △

Jiné řešení. Víme, že $132 = 2^2 \cdot 3 \cdot 11$ a $35 = 5 \cdot 7$, takže $(35, 132) = 1$ a modulární inverze existuje. Použijeme metodu rozkladu. Hledáme tedy x takové, že

$$35\,x \equiv 1 \pmod{4}, \quad \pmod{3} \text{ i } \pmod{11}$$

Neboť $36 = 4 \cdot 9$, vidíme, že $x \equiv -1 \pmod{4}$. Rovněž $36 = 3 \cdot 12$, tedy také $x \equiv -1 \pmod{3}$. Nakonec $33 = 3 \cdot 11$, takže

$$\begin{aligned} 35\,x \equiv 2\,x \equiv 1 &\pmod{11} \mid \cdot 6 \\ 12\,x \equiv x \equiv 6 &\pmod{11} \end{aligned}$$

Z $(4, 3) = 1$ víme, že $x \equiv -1 \pmod{4 \cdot 3 = 12}$, tedy mezi čísly tvaru $12\,k - 1$ hledáme číslo tvaru $11\,l - 6$. Jinými slovy hledáme mezi čísly tvaru $11\,l + 7$ číslo dělitelné 12.

l	0	1	2	3	4	5	6	7	8	9	10	11
$11\,l+7$	7	18	29	40	51	62	73	84	95	106	117	128

Vidíme, že se jedná o číslo 84, hledanou modulární inverzí je tedy 83.

Při hledání x jsme si úlohu rozložili na řešení soustavy kongruencí

$$\begin{aligned} 35\,x &\equiv 1 \pmod 4 \\ 35\,x &\equiv 1 \pmod 3 \\ 35\,x &\equiv 1 \pmod{11} \end{aligned}$$

kterou jsme si převedli na

$$\begin{aligned} x &\equiv -1 \pmod{12} \\ x &\equiv 6 \pmod{11}. \end{aligned}$$

Tuto soustavu lze řešit také tak, že si z první kongruence vyjádříme $x = 12\,k - 1$, které následně dosadíme do druhé kongruence, kterou řešíme. Pak máme

$$\begin{aligned} 12\,k - 1 &\equiv 6 \pmod{11} \\ 12\,k &\equiv 7 \pmod{11} \\ k &\equiv 7 \pmod{11} \end{aligned}$$

tedy $k = 11\,l + 7$. Následně $x = 12\,k - 1 = 12 \cdot (11\,l + 7) - 1 = 132\,l + 83$, tedy $x \equiv 83 \pmod{132}$. △

Příklad 2.4. Spočítejte 55^{-1} modulo 132.

Řešení. Máme rozklady $132 = 2^2 \cdot 3 \cdot 11$ a $55 = 5 \cdot 11$. Tedy $(132, 55) = 11 > 1$ a modulární inverze neexistuje. Skutečně například $12 \not\equiv 0 \pmod{132}$, ale $55 \cdot 12 = 5 \cdot 132 \equiv 0 \pmod{132}$. △

Příklad 2.5. Dokažte, že $n = (893^5 + 4)^{20} - 1$ je dělitelné číslem $176 = 11 \cdot 16$.

Řešení. Neboť $(11, 16) = 1$, stačí dokázat, že n je dělitelné 11 i 16. Díky $880 = 80 \cdot 11 = 55 \cdot 16$ víme, že $893 \equiv 2 \pmod{11}$ a $893 \equiv -3 \pmod{16}$. Poté

$$\begin{aligned} n &\equiv (2^5 + 4)^{20} - 1 = 36^{20} - 1 && \text{díky } 893 \equiv 2 \pmod{11} \\ &\equiv 3^{20} - 1 && \text{neboť } 36 \equiv 3 \pmod{11} \\ &\equiv (-2)^{10} - 1 = 2^{10} - 1 && \text{jelikož } 3^2 \equiv -2 \pmod{11} \\ &\equiv (-1)^2 - 1 = 0 \pmod{11} && \text{protože } 2^5 \equiv -1 \pmod{11}. \end{aligned}$$

Podobně

$$\begin{aligned} n &\equiv \Big((-3)^5 + 4\Big)^{20} - 1 && \text{kvůli } 893 \equiv -3 \pmod{16} \\ &\equiv (-3 + 4)^{20} - 1 = 1^{20} - 1 = 0 && \text{protože } (-3)^4 = 81 \equiv 1 \pmod{16}. \end{aligned}$$

Tudíž také $n \equiv 0 \pmod{176}$, což jsme měli dokázat. △

Příklad 2.6. Dokažte, že pro každé $n \in \mathbb{N}$ je $4^{2n+1} - 10n - 4$ dělitelné 25.

Nápověda. Použijte $16^n - 1 = (16-1)(1 + 16 + \cdots + 16^{n-1} \equiv 15n \pmod{25}$.
Řešení. Nejprve indukcí dokážeme tvrzení z nápovědy. Pro $n = 1$ máme $16 - 1 = 15 \equiv 15 \pmod{25}$. Předpokládejme nyní, že tvrzení platí pro n a počítejme pro $n+1$:

$$16^{n+1} - 1 = 16 \cdot (16^n - 1) + 16 - 1 \overset{\text{I. P.}}{\equiv} 16 \cdot 15n + 16 - 1 = \\ = 225n + 15 \cdot (n+1) \equiv 15 \cdot (n+1) \pmod{25}$$

neboť $25 \mid 225$. Pak je důkaz jednoduchý:

$$4^{2n+1} - 10n - 4 = 4 \cdot (16^n - 1) - 10n \equiv 4 \cdot 15n - 10n = 50n \equiv 0 \pmod{25}$$

tedy opravdu 25 dělí $4^{2n+1} - 10n - 4$ pro každé $n \in \mathbb{N}$. △

Příklad 2.7. Dokažte, že číslo $5^{20} + 2^{30}$ je složené.

Řešení. Chceme najít nějaké číslo (větší než 1), které dělí naše $5^{20} + 2^{30}$. Víme, že

$$5^2 \equiv -1 \pmod{13} \qquad\qquad 2^6 \equiv -1 \pmod{13}$$

(první kongruence je jasná, u druhé si vzpomeneme na cvičení 2.1). Pak

$$5^{20} + 2^{30} = \left(5^2\right)^{10} + \left(2^6\right)^5 \equiv (-1)^{10} + (-1)^5 = 1 - 1 = 0 \pmod{13}$$

a tedy $13 \mid 5^{20} + 2^{30}$ a jedná se skutečně o číslo složené. △
Jiné řešení. Protože $5^{20} + 2^{30} = (5^4)^5 + (2^6)^5$ je součet dvou lichých mocnin, můžeme si vzpomenout na vzoreček a říci, že jako součin se jedná o číslo složené.

Odvodíme tedy pro připomenutí vzorečky pro součty lichých a rozdíly libovolných mocnin. Máme částečný součet geometrické řady

$$q^n - 1 = (q-1) \cdot (1 + q + \cdots + q^{n-1}). \tag{2.1}$$

Napíšeme-li si $q = \frac{a}{b}$ pro nějaká a, $b > 0$ a vynásobíme-li následně (2.1) b^n s tím, že na pravé straně násobíme první závorku b a druhou b^{n-1}, dostaneme vzorec pro rozdíl mocnin:

$$a^n - b^n = (a-b) \cdot (b^{n-1} + a\,b^{n-2} + a^2\,b^{n-3} + \cdots + a^{n-3}\,b^2 + a^{n-2}\,b + a^{n-1}). \tag{2.2}$$

Vzorec pro součet *lichých* mocnin lze již odvodit z (2.2). Dosazením $a = -c$ a s využitím toho, že pro liché mocniny a máme minus a pro sudé mocniny plus, dostáváme

$$-c^n - b^n = (-c-b) \cdot (b^{n-1} - c\,b^{n-2} + c^2\,b^{n-3} - \cdots + c^{n-3}\,b^2 - c^{n-2}\,b + c^{n-1})$$

z čehož po vynásobení -1 máme

$$c^n + b^n = (c+b) \cdot (b^{n-1} - c\,b^{n-2} + c^2\,b^{n-3} - \cdots + c^{n-3}\,b^2 - c^{n-2}\,b + c^{n-1}).$$

V našem případě pak

$$5^{20} + 2^{30} = \left(5^4\right)^5 + \left(2^6\right)^5 = \left(5^4 + 2^6\right) \cdot \left(5^{16} - 5^{12}\,2^6 + 5^8\,2^{12} - 5^4\,2^{18} + 2^{24}\right)$$

tedy $5^{20} + 2^{30}$ je číslo složené. Všimněme si, že $5^4 + 2^6 = 689 = 13 \cdot 53$. △

Příklad 2.8. Odvoďte pravidla pro dělitelnost 11, 9, 7 pomocí dekadického zápisu.

Řešení. Vezměme číslo $n \in \mathbb{N}$ a zapišme si ho jako $n = \sum_{i=0}^{r} a_i \, 10^i$ pro $a_i \in \{0, \ldots, 9\}$. Začneme s dělitelností devíti. Neboť je $10 \equiv 1 \pmod 9$, máme

$$n = \sum_{i=0}^{r} a_i \, 10^i \equiv \sum_{i=0}^{r} a_i \pmod 9$$

čímž dostáváme známé pravidlo – n je dělitelné devíti právě, když je dělitelný jeho ciferný součet. Iterací dostaneme, že je dělitelné n právě, když je dělitelný jeho superciferný součet. Protože $9 = 3^2$, platí tento důkaz i pro trojku. Dělitelnost jedenácti lze řešit podobně, jelikož $10 \equiv -1 \pmod{11}$. Následně

$$n = \sum_{i=0}^{r} a_i \, 10^i \equiv \sum_{i=0}^{r} a_i \, (-1)^i = \sum_{i \text{ sudé}} a_i - \sum_{i \text{ liché}} a_i \pmod{11}$$

a dostáváme, že n je dělitelné jedenácti právě tehdy, když je dělitelný rozdíl součtů jeho sudých cifer a jeho cifer lichých. Opět můžeme postup iterovat. Pro dělitelnost sedmi již nelze použít čistě dekadický zápis, nicméně můžeme použít následující pozorování. Máme $7 \cdot 11 \cdot 13 = 1\,001$. Zapíšeme-li si n jako $n = \sum_{j=0}^{s} b_j \cdot 1\,000^j$ pro $b_j \in \{0, \ldots, 999\}$, můžeme díky $1\,000 \equiv -1 \pmod{1\,001}$ říct, že

$$n = \sum_{j=0}^{s} b_j \cdot 1\,000^j \equiv \sum_{j=0}^{s} b_j \, (-1)^j = \sum_{j \text{ sudé}} b_j - \sum_{j \text{ liché}} b_j \pmod{1\,001}$$

a tedy i modulo 7, 11 i 13. Můžeme tedy říci, že je n dělitelné 7, 11 nebo 13 právě tehdy, je-li dělitelný rozdíl součtů jejich sudých a lichých trojčíslí. I tento postup lze samozřejmě iterovat, abychom nakonec skončili mezi 0 a 999. △