2 Euler a Číňané

Řešení
Verze ze dne 24. února 2025

Cíle cvičení: Ke zdárnému počítání kongruencí si osvojíme využití Eulerovy věty a naučíme se řešit soustavy lineárních kongruencí, což odpovídá nalezení vzoru v čínské větě o zbytcích.

Úlohy, které bychom určitě měli umět řešit:

Úloha 2.1. Určete hodnotu Eulerovy funkce

(a) $\varphi(600)$,

(b) $\varphi(7425)$ (mohlo by se hodit vědět, že $7425 = 27 \cdot 25 \cdot 11$).

Řešení. Stačí si vzpomenout na vzoreček pro výpočet hodnoty Eulerovy funkce na základě znalosti prvočíselného rozkladu $\varphi(\prod_i p_i^{r_i}) = \prod_i (p_i - 1)p_i^{r_i - 1}$.

(a) $\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 2^2 \cdot (3-1) \cdot (5-1)5 = 160$.

(b) $\varphi(7425) = \varphi(3^3 \cdot 5^2 \cdot 11) = 2 \cdot 3^2 \cdot 4 \cdot 5 \cdot 10 = 3600$.

Úloha 2.2. Spočítejte (a) poslední cifru čísla 1357^{246}, (b) $10^{200} \bmod 19$, (c) $3^{5^7} \bmod 28$.

Řešení. (a) Jelikož $\mathrm{NSD}(10, 7) = 1$, můžeme využít Eulerovu větu k výpočtu kongruence

$$1357^{246} \equiv 7^{246 \bmod 4} \equiv 7^2 \equiv 9 \pmod{10},$$

odkud plyne, že poslední cifra 1357^{246} je 9.

(b) Opět $\mathrm{NSD}(10, 19) = 1$, přičemž $\varphi(19) = 18$, takže

$$10^{200} \equiv 10^{200 \bmod 18} = 10^2 \equiv 5 \pmod{19}.$$

(c) Protože $\varphi(28) = 12$, $\varphi(12) = 4$ a dále $\mathrm{NSD}(3, 28) = 1 = \mathrm{NSD}(5, 12)$, využijeme dvakrát Eulerovu větu, díky níž

$$3^{5^7} \equiv 3^{(5^7) \bmod 12} \pmod{28}$$

a

$$5^7 \equiv 5^{7 \bmod 4} \equiv 5^3 \equiv 5 \pmod{12}.$$

Dostáváme tak, že

$$3^{5^7} \equiv 3^5 = 27 \cdot 9 \equiv (-1) \cdot 9 \equiv 19 \pmod{28}.$$

Tedy $3^{5^7} \bmod 28 = 19$.

Úloha 2.3. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 7$, $x \equiv 3 \pmod 8$;

(b) $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$, $4x + 3 \equiv 2 \pmod 5$;

(c) $10x \equiv 6 \pmod{32}$, $3x \equiv 1 \pmod 5$.

Řešení. Postupně budeme dosazovat obecné řešení prvních $i-1$ kongruencí do i-té kongruence.

(a) Okamžitě vidíme, že $x \equiv 2 \pmod 3$ právě když $x = 2 + 3a$ pro $a \in \mathbb{Z}$, proto dosazením za x do druhé kongruence dostaneme pomocí ekvivalentních úprav kongruencí

$$2 + 3a \equiv x \equiv 4 \pmod 7 \quad \Leftrightarrow \quad 3a \equiv 2 \pmod 7 \quad \Leftrightarrow \quad a \equiv 3 \pmod 7.$$

Nyní $a = 3 + 7b$, a proto $x = 2 + 3(3 + 7b)) = 11 + 21b$ pro libovolné $b \in \mathbb{Z}$. Dosazením vyjádření x pomocí b do třetí kongruence dostaneme

$$3 + 5b \equiv 11 + 21b \equiv x \equiv 3 \pmod 8 \quad \Leftrightarrow \quad 5b \equiv 0 \pmod 8 \quad \Leftrightarrow \quad b \equiv 0 \pmod 8,$$

proto $b = 8c$ a $x = 11 + 21 \cdot 8c = 11 + 168c$ pro libovolné $c \in \mathbb{Z}$.

(b) Kongruence nejprve převedeme na tvar

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 4, \quad x \equiv 1 \pmod 5$$

a pak stejným postupem jako v (a) spočteme obecné řešení tvaru $11 + 60m$ pro $m \in \mathbb{Z}$.

(c) Nejprve ekvivalentně upravíme první kongruenci pomocí krácení modulu a obou stran na tvar

$$5x \equiv 3 \pmod{16} \;\Leftrightarrow\; x \equiv (-3) \cdot 5x \equiv -9 \equiv 7 \pmod{16}.$$

Druhou kongruenci poté ekvivalentně převedeme na tvar $x \equiv 2 \pmod 5$ a pak obvyklým postupem spočítáme řešení $7 + 80m$ pro libovolné $m \in \mathbb{Z}$.

Úloha 2.4. Při přípravě na Velikonoce nakoupil Ota spoustu vajíček. Když je rozděloval do krabic po osmi, tak měl v poslední krabici jen dvě, zatímco když je rozděloval do krabic po pětadvaceti, tak byly v poslední krabici tři. Kolik vajec Ota nakoupil, jestliže jich bylo méně než 500? Nalezněte všechny možnosti.

Řešení. Zadání popisuje soustavu kongruencí

$$x \equiv 2 \pmod 8, \quad x \equiv 3 \pmod{25},$$

kde x je počet vajec. Nejjednodušší je asi z druhé kongruence položit $x = 25k + 3$ a dosazením do první máme

$$\begin{aligned} 25k + 3 &\equiv 2 \pmod 8, \\ k &\equiv -1 \pmod 8, \end{aligned}$$

je tedy $x = 25(8\ell - 1) + 3 = 200\ell - 22$, což nabývá hodnot mezi 0 a 500 pro $\ell = 1, 2$, konkrétně 178 a 378.

Úloha 2.5. Najděte příklady, na kterých bude vidět nezbytnost předpokladu nesoudělnosti čísel m_i v čínské větě o zbytcích – jednak případ, kdy soustava bude mít (modulo součin m_i) více řešení, jednak kdy nebude mít žádné.

Řešení. Například soustava kongruencí

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 1 \pmod 4 \end{aligned}$$

nemá řešení.

Úloha 2.6. Určete zbytek 5^{6000} po dělení 70. (Nápověda: Nelze přímo aplikovat Eulerovu větu; namísto toho můžeme např. zvlášť určit zbytky mod 7 a 10 a výsledky „spojit“ pomocí ČZV.)

Řešení. Jelikož $\mathrm{NSD}(70,5) = 5 \neq 1$, nelze přímo aplikovat Eulerovu větu, která by v tomto případě dala nesprávný výsledek 1 (jelikož $\varphi(70) = 24 \mid 6000$). Namísto toho zjistíme, jaké zbytky dává $m = 5^{6000}$ po dělení 7 a 10, přičemž zkombinováním těchto informací skrze čínskou zbytkovou větu určíme hledanou hodnotu.

Předně $\varphi(7) = 6 \mid 6000$, takže

$$m \equiv 5^0 = 1 \pmod 7.$$

Zbytek m po dělení 10 určíme snadno tím způsobem, že si uvědomíme, že poslední cifra mocnin pětky je vždy 5. Dostáváme tedy soustavu kongruencí

$$m \equiv 1 \pmod 7, \quad m \equiv 5 \pmod{10},$$

kterou standardní cestou vyřešíme s výsledkem

$$m \equiv 15 \pmod{70}.$$

Dalším možným postupem by bylo určit hodnoty $m \bmod 14 = 1$ a $m \bmod 5 = 0$ a opět aplikovat ČZV. Ještě jiný postup by spočíval ve vydělení kongruence pěti, pokud si uvědomíme, že výsledné číslo musí být dělitelné pěti – označme ho $5x$. Potom

$$\begin{aligned} 5^{6000} = 5 \cdot 5^{5999} &\equiv 5x \pmod{70} \\ 5^{5999} &\equiv x \pmod{14} \end{aligned}$$

na což už lze použít Eulerovu větu ($\varphi(14) = 6$) a zůstane nám výpočet $5^5 \bmod 14$, který lze provést např. takto:

$$x \equiv 5^5 = 5 \cdot 25^2 \equiv 5 \cdot (-3)^2 = 5 \cdot 3^2 = 15 \cdot 3 \equiv 1 \cdot 3 = 3 \pmod{14}.$$

Odtud tedy $m = 5x \equiv 15 \pmod{70}$. Alternativní metoda výpočtu x by spočívala v tom, že jelikož $5x \equiv 5^6 \equiv 1 \pmod{14}$, je x inverzním prvkem k 5 v okruhu $\mathbb{Z}_{14}$, přičemž snadno nahlédneme, že tímto prvkem je 3.

A na závěr záplava úloh pro zábavu i poučení:

Úloha 2.7. Spočítejte (a) $100^{99^{98}} \bmod 39$, (b) $100^{99^{98}} \bmod 40$.

Řešení. (a) Postupujeme podobně jako v 2.2 (c). Protože $\varphi(39) = 24$ a $\mathrm{NSD}(22, 39) = 1$, dostaneme s využitím Eulerovy věty kongruenci:

$$100^{99^{98}} \equiv 22^{(99^{98}) \bmod 24} \pmod{39}.$$

Dále počítáme

$$99^{98} \equiv 3^{98} \equiv 3 \cdot 3^{97} \pmod{24}.$$

Základ mocniny a modul jsou soudělné, proto nemůžeme využít Eulerovu větu přímo, ale protože

$$3^{97} \equiv 3^{97 \bmod 4} \equiv 3^1 \equiv 3 \pmod 8,$$

dostáváme s využitím vlastností kongruencí (konkrétně té, která nám umožňuje vydělit konstantou modul a obě strany kongruence)

$$99^{98} \equiv 3 \cdot 3^{97} \equiv 3 \cdot 3 \equiv 9 \pmod{3 \cdot 8}.$$

Nyní zbývá například (ne zas tak moc) hrubou silou spočítat, že $22^3 \bmod 3 = 1$ a tudíž

$$100^{99^{98}} \equiv 22^9 \equiv (22^3)^3 \equiv 1^3 \equiv 1 \pmod{39}.$$

(b) Tentokrát Eulerovu větu kvůli soudělnosti základu modulu využít nemůžeme, ale ani ji naštěstí nepotřebujeme, místo toho si všimneme, že $40 \mid 100^2 \mid 100^{99^{98}}$, a proto $100^{99^{98}} \bmod 40 = 0$.

Úloha 2.8. Určete poslední dvě cifry čísla $999^{888^{777}}$ a poslední tři cifry čísla 249^{19}.

Řešení. Stačí si jen všimnout, že $999^2 \equiv (-1)^2 \equiv 1 \pmod{100}$, proto

$$999^{888^{777}} \equiv ((-1)^2)^{888^{777}/2} \equiv 1^{888^{777}/2} \equiv 1 \pmod{100},$$

tudíž poslední dvě cifry druhé mocniny jsou 01.

V druhém případu nás zajímá hodnota $249^{19} \bmod 1000$. Nejprve spočítáme

$$249^2 \equiv (250-1)^2 \equiv 250 \cdot (250-2) + 1 \equiv 62 \cdot 4 \cdot 250 + 1 \equiv 1 \pmod{1000},$$

proto $249^{19} \bmod 1000 = 249$ a poslední 3 cifry mocniny jsou 249.

Úloha 2.9. Dokažte, že pro každé prvočíslo $p \neq 2$ platí $p \mid 1^p + 2^p + 3^p + \ldots + p^p$.

Řešení. Podle Eulerovy (respektive Malé Fermatovy) věty pro každé $i = 1, \ldots, p-1$ platí, že $i^p \equiv i \pmod{p}$, proto

$$1^p + 2^p + 3^p + \ldots + p^p \equiv 1 + 2 + 3 + \ldots + p - 1 + 0 \equiv \frac{p(p-1)}{2} \equiv 0 \pmod{p},$$

neboť p je liché prvočíslo, $\frac{p-1}{2}$ je přirozené a tudíž p dělí číslo $\frac{p(p-1)}{2}$.

Úloha 2.10. Dokažte, že

(a) 13 dělí $23^{32} + 29^{33} + 36^{34}$,

(b) $9 \mid 4^n + 6n - 1$ pro každé n přirozené.

Řešení. (a) Pomocí modulární aritmetiky, resp. Eulerovy věty zjistíme, že platí $23^{32} \equiv 9 \pmod{13}$, $29^{33} \equiv 1 \pmod{13}$, $36^{34} \equiv 3 \pmod{13}$ a součet je tedy modulo 13 roven 0.

(b) Dokážeme indukcí dle n. Pro $n = 1$ tvrzení zřejmě platí.

Platí-li tvrzení pro $n \geq 1$, pak $4^n \equiv 1 - 6n \pmod{9}$, proto

$$4^{n+1} + 6(n+1) - 1 \equiv 4 \cdot (4^n) + 6n + 5 \equiv 4 \cdot (1 - 6n) + 6n + 5 \equiv -18n + 9 \equiv 0 \pmod{9}$$

Úloha 2.11. Najděte všechna $x \in \mathbb{Z}$ splňující $26^5 x \equiv 16 \pmod{11}$.

Řešení. Nejprve pomocí Eulerovy věty spočítáme

$$26^5 \equiv 4^5 \equiv 2^{10} \equiv 2^{(10)} \equiv 1 \pmod{11},$$

Nyní snadno vyřešíme ekvivalentní kongruenci $x \equiv 5 \pmod{11}$ a snadno určíme všechna řešení $5 + 11k$ pro libovolné $k \in \mathbb{Z}$.

Úloha 2.12. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 13x \equiv 15 \pmod{27} \\ 2x \equiv 1 \pmod{3}. \end{cases}$

Řešení. Z první kongruence plyne, že $x \equiv 0 \pmod{3}$, zatímco druhá říká, že $x \equiv 2 \pmod{3}$, proto je množina řešení prázdná.

Úloha 2.13. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x^2 \equiv 1 \pmod{3}$, $x^2 \equiv 1 \pmod{7}$;

(b) $x^2 \equiv -1 \pmod{66}$;

(c) $x^2 \equiv -1 \pmod{65}$.

Řešení. (a) Z prvního cvičení víme, že rovnice $x^2 \equiv 1 \pmod{p}$ má pro prvočíslo p řešení právě $\pm 1 + k \cdot p$ pro $k \in \mathbb{Z}$. Dostaneme 4 možné soustavy (kombinace) lineárních kongruencí, které vyřešíme stejným postupem jako v úloze 2.3 a dostaneme tak množinu všech řešení

$$\{1 + 21m \mid m \in \mathbb{Z}\} \cup \{8 + 21m \mid m \in \mathbb{Z}\} \cup \{13 + 21m \mid m \in \mathbb{Z}\} \cup \{20 + 21m \mid m \in \mathbb{Z}\}.$$

(b) Protože řešení kongruence $x^2 \equiv -1 \pmod{66}$ by řešilo i kongruenci $x^2 \equiv -1 \pmod{3}$, která zjevně žádné řešení nemá. Je množina všech řešení naší kongruence prázdná.

(c) Nejprve vyřešíme soustavu kongruencí $\begin{cases} x^2 \equiv -1 \pmod{5} \\ x^2 \equiv -1 \pmod{13} \end{cases}$, což lze provést hrubou silou počítáním v tělesech $\mathbb{Z}_5$ a $\mathbb{Z}_{13}$, tedy $x \equiv \pm 2 \pmod{5}$ a $x \equiv \pm 5 \pmod{13}$ a poté opětovným použitím čínské věty o zbytcích dostaneme množinu všech řešení

$$\{8 + 65m \mid m \in \mathbb{Z}\} \cup \{-8 + 65m \mid m \in \mathbb{Z}\} \cup \{18 + 65m \mid m \in \mathbb{Z}\} \cup \{-18 + 65m \mid m \in \mathbb{Z}\}.$$

Úloha 2.14. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 3^x \equiv 1 \pmod{13} \\ 3x \equiv 1 \pmod{13}. \end{cases}$

Řešení. Z druhé kongruence dostáváme vyjádření $x = 9 + 13a$, které když dosadíme do druhé kongruence a využijeme Eulerovu větu, dostaneme

$$3^x \equiv 3^{(9+13a) \bmod 12} \equiv 3^{(9+a) \bmod 12} \equiv 1 \pmod{13}.$$

Všimneme-li si, že $3^i \equiv 1 \pmod{13} = 1$, právě když $3 \mid i$, pak řešíme kongruenci $9 + a \equiv 0 \pmod{3}$. Tudíž $a = 3k$ a obecné řešení je tvaru $9 + 39k$ pro $k \in \mathbb{Z}$.

Úloha 2.15. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod{7}$.

Řešení. Pro $x \equiv 0 \pmod{7}$ zřejmě rovnice žádné řešení nemá a pokud $x \not\equiv 0 \pmod{7}$ platí podle Eulerovy věty, že $x^6 \equiv 1 \pmod{7}$. Tudíž se kongruence redukuje na $x(1 + y) \equiv 0 \pmod{7}$, což je díky tomu, že 7 je prvočíslo ekvivalentní podmínce $x \equiv 0 \pmod{7}$ nebo $y \equiv 6 \pmod{7}$, a proto máme řešení právě pro $x \not\equiv 0$,$y \equiv 6 \pmod{7}$.

Úloha 2.16. Najděte všechna $x \in \{0, 1, \ldots, 76\}$ splňující $x^2 + 8x \equiv 62 \pmod{77}$.

Řešení. Převeďme na $x^2 + 8x + 15 = (x + 3)(x + 5) \equiv 0 \pmod{77}$, pomocí Čínské věty o zbytcích vyřešíme modulo 7, resp. 11 čtyři možné případy a zvedneme zpět modulo 77 a dostaneme řešení $30, 39, 72, 74$.

⋆ **Úloha 2.17.** Najděte všechna čísla n taková, že $\varphi(n) = 18$.

Řešení. Protože číslo $18 = 2 \cdot 3^2$ musí být tvaru $\prod_i (p_i - 1) p_i^{r_i - 1}$ pro prvočíselný rozklad $n = \prod_i p_i^{r_i}$, obsahuje prvočíselný rozklad n nejvýše dvě různá prvočísla a snadnou diskusí zjistíme, že jsou možné pouze hodnoty 19, $27 = 3^3$, $38 = 2 \cdot 19$, $54 = 2 \cdot 3^3$.

⋆ **Úloha 2.18.** Najděte všechna čísla $n > 1$ taková, že $\varphi(n) \mid n$.

Řešení. Nechť $n = \prod_i p_i^{r_i}$ je prvočíselný rozklad a předpokládejme, že p_1 je v něm nejmenší; pak $\varphi(n)$ je násobkem $p_1 - 1$, z podmínky $\varphi(n) \mid n$ je tedy také n násobkem $p_1 - 1$. Ovšem p_1 je nejmenší prvočíselný dělitel n, tedy nutně $p_1 = 2$. Je-li tedy n tvaru $2^k \cdot m$, kde m je liché a $k \geq 1$, pak $\varphi(n) = 2^{k-1} \cdot \varphi(m)$ a naše podmínka je $\varphi(m) \mid 2m$. Za každého prvočíselného dělitele m se ovšem v rozkladu $\varphi(m)$ vyskytne další dvojka, z čehož (díky lichosti m) plyne, že m má nejvýše jednoho prvočíselného dělitele.

Nechť tedy $n = 2^k p^\ell$, kde $p \neq 2$; potom $\varphi(n) = 2^{k-1} p^{\ell-1}(p - 1)$ a naše podmínka je $(p - 1) \mid 2p$. Jelikož $p - 1$ je s p nesoudělné, dostáváme $(p - 1) \mid 2$, čímž dostáváme jedinou možnost $p = 3$. Tedy $n = 2^k \cdot 3^l$ pro $k \in \mathbb{N}$, $l \in \mathbb{N} \cup \{0\}$; tato čísla vskutku vyhovují, jak se snadno ověří.

⋆ **Úloha 2.19.** Označme $\sigma(n)$ součet všech dělitelů přirozeného čísla n. Najděte vzorec pro výpočet $\sigma(n)$, pokud znáte prvočíselný rozklad čísla n. Inspirujte se důkazem vzorce pro Eulerovu funkci

Řešení. Řešení třeba tady.

⋆ **Úloha 2.20.** Nechť a a m jsou přirozená čísla a označme jako S posloupnost $\{a^k \bmod m\}_{k\in\mathbb{N}}$. V případě nesoudělnosti a a m je dle Eulerovy věty S periodická s periodou dělící $\varphi(m)$. Ale i v případě, že a a m jsou soudělná, je od jistého indexu dál S také periodická s periodou dělící $\varphi(m)$. Jak je to možné?

Řešení. Nechť m' je největší dělitel m takový, že $\mathrm{NSD}(m', a) = 1$, a označme $d = m/m'$. Dle čínské zbytkové věty stačí ukázat onu periodičnost modulo m' a d. Jelikož $m' \mid m$, tak $\varphi(m') \mid \varphi(m)$, a díky $\mathrm{NSD}(m', a) = 1$ a Eulerově větě je $S \bmod m'$ vskutku periodická s periodou dělící $\varphi(m)$.

Dle své definice má d pouze ty prvočíselné dělitele, které má a; odtud plyne, že dostatečně vysoké mocniny a budou dělitelné d. Od jistého indexu je tedy $S \bmod d$ identicky nulová, tedy periodická posloupnost.

Sladká tečka pro soutěživce:

Úloha 2.21. (USAMO 1991) Dokažte, že pro každé $n \in \mathbb{N}$ je posloupnost

$$2 \bmod n,\ 2^2 \bmod n,\ 2^{2^2} \bmod n,\ \ldots$$

od jistého členu dál konstantní. (Nápověda: Možný přístup – uvažte nejmenší n, pro které to neplatí, a dojděte ke sporu. Platí $\varphi(n) < n$.)

Řešení. Zde.

Úloha 2.22. (Domácí kolo 64. MO A) Nechť $a, b \in \mathbb{N}$ jsou nesoudělná a posloupnost $\{x_n\}_{n\in\mathbb{N}}$ splňuje $x_{n+1} = ax_n + b$ pro všechna $n \in \mathbb{N}$. Dokažte, že každý člen této posloupnosti (vyjma prvního) dělí nekonečně mnoho jejích dalších členů.

Řešení. Zde.