7. KONGRUENCIE

Nech $m \in \mathbb{N}$. Hovoríme, že dve čísla $a, b \in \mathbb{Z}$ sú *kongruentné modulo* m práve vtedy, keď majú ten istý zvyšok po delení číslom m. Symbolicky to môžeme zapísať

$$a \mod m = b \mod m.$$

Kvôli jednoduchosti budeme skutočnosť, že čísla a, b sú kongruentné modulo m, zapisovať nasledujúcim spôsobom, ktorý je v teórii čísel zaužívaný.

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

Úloha 106. Nech $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$. Potom

$$a \equiv b \pmod{m} \iff m | b - a.$$

Dokážte.

Úloha 107. Nech $a, b, c \in \mathbb{Z}$ a $m \in \mathbb{N}$. Potom:
a) $a \equiv a \pmod{m}$,
b) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$,
c) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.
Dokážte.

Úloha 108. Nech a_1, a_2, b_1, $b_2 \in \mathbb{Z}$ a $m \in \mathbb{N}$. Ak $a_1 \equiv b_1 \pmod{m}$ a $a_2 \equiv b_2 \pmod{m}$, potom

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m},$$
$$a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

Dokážte.

– – – – – – – – – – – –

Teraz ukážeme riešenie Pellovej rovnice, ktorú sme už spomínali na konci časti Diofantické rovnice vyššieho stupňa. Najprv dokážeme tvrdenie, pomocou ktorého dokážeme, že Pellova rovnica má aspoň jedno riešenie:
Dirichletova veta o aproximácii: *Nech α je iracionálne číslo. Potom existuje nekonečne veľa dvojíc x, y, $x \in \mathbb{Z}, y \in \mathbb{N}$ pre ktoré platí*

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^2} \ . \qquad (*)$$

Dôkaz: *Určite existuje aspoň jedna taká dvojica, lebo $|\alpha - [\alpha]| = |\{\alpha\}| < 1$. Predpokladajme, že existuje k takých dvojíc $x_1, y_1, ..., x_k, y_k$. Z iracionality α dostávame, že ani jeden z výrazov $|y_j \alpha - x_j|, j = 1, ..., k$ sa nerovná 0. Zvoľme prirodzené číslo N tak aby platilo $\frac{1}{N} < |y_j \alpha - x_j|, j = 1, ..., k$. Uvažujme zlomkové časti $\{l\alpha\}, l = 1, ..., N+1$. Z iracionality α vyplýva, že všetky tieto hodnoty sú rôzne, (prečo?). Interval $< 0, 1)$ môžeme rozdeliť na N intervalov tvaru $< \frac{l-1}{N}, \frac{l}{N}), l = 1, ..., N$. Máme $N+1$ hodnôt $\{l\alpha\}$ a N intevalov, teda aspoň jeden obsahuje dve rôzne. Teda existujú $1 \leq l_1, l_2 \leq N+1$ pre ktoré $|\{l_1\alpha\} - \{l_2\alpha\}| < \frac{1}{N}$.*

Teda $|[(l_1 - l_2)\alpha - [l_1\alpha] - [l_2\alpha]| < \frac{1}{N}$. *Predpokladajme* $l_1 > l_2$. *Položme* $y_{k+1} = l_1 - l_2, x_{k+1} = [l_1\alpha] - [l_2\alpha]$. *Potom platí* $|y_{k+1}\alpha - x_{k+1}| < \frac{1}{N}$. *Po vydelení* y_{k+1} *dostávame* $|\alpha - \frac{x_{k+1}}{y_{k+1}}| < \frac{1}{y_{k+1}N}$. *Ale určite* $y_{k+1} \leq N$ *a teda* x_{k+1}, y_{k+1} *spĺňa* $(*)$.*Dvojica* x_{k+1}, y_{k+1} *sa nerovná žiadnej z dvojíc* $x_j, y_j, j = 1, ..., k$ *(Prečo?).* □

Teraz prejdeme k Pellovej rovnici tak ako je definovaná vzťahom $(*)$ *na strane 24. V tomto prípade je* $\sqrt{A}$ *iracionálne číslo. Podľa Dirichletovej vety o aproximácii existuje nekonečne veľa dvojíc* x, y *v tomto prípade prirodzených čísel, takých, že*

$$\left|\sqrt{A} - \frac{x}{y}\right| < \frac{1}{y^2} \ .$$

Pre všetky takéto dvojice x, y *potom platí*

$$|x^2 - Ay^2| = |x - \sqrt{A}y||x + \sqrt{A}y| < \frac{1}{y}|x + \sqrt{A}y| < \sqrt{A} + \frac{x}{y} < 2\sqrt{A} + 1.$$

Teda pre tieto dvojice je hodnota $|x^2 - Ay^2|$ *ohraničená. Z toho vyplýva, že nadobúda iba konečne veľa hodnôt v množine prirodzených čísel a teda niektoré prirodzené číslo, označme ho* m, *musí nadobudnúť nekonečne veľa krát. Pre nekonečne veľa dvojíc prirodzených čísel* x, y *potom platí* $|x^2 - Ay^2| = m$. *Preto existujú také dve rôzne dojice prirodzených čísel* x, y, u, v, *že* $|x^2 - Ay^2| = m$, $|u^2 - Av^2| = m$ *pre ktoré platí* $x \equiv u \pmod m, y \equiv v \pmod m$. *Po vynásobení dostávame* $|x^2 - Ay^2||u^2 - Av^2| = m^2$. *Keď si uvedomíme* $|x^2 - Ay^2| = |x - \sqrt{A}y||x + \sqrt{A}y|$ *a* $|u^2 - Av^2| = |u - \sqrt{A}v||u + \sqrt{A}v|$ *dostávame po príslušných úpravách* $(xu - Ayv)^2 - A(uy - xv)^2 = m^2$.*Položme* $X = |xu - Ayv|, Y = |uy - xv|$. *A teda*

$$|X^2 - AY^2| = m^2. \qquad (**)$$

Z úlohy 108 vyplýva, že $m|Y$ *a preto aj* $m|X$. *Ukážeme, že* $Y \neq 0$. *Ak by* $Y = 0$, *dostávame* $\frac{x}{y} = \frac{u}{v} = r$. *Preto* $x = ry, u = rv$ *z toho po úprave vyplýva* $y^2|r^2 - A| = m = v^2|r^2 - A|$ *a teda* $y = v$, *preto aj* $x = u$. *Dostávame spor s tým, že dvojice* x, y, u, v *sú rôzne. Ak položíme* $X = mX', Y = mY'$ *dostávame podľa* $(**)$

$$X'^2 - AY'^2 = \pm 1.$$

Ak je v poslednej rovnosti 1 *tak* X', Y' *sú riešenia Pellovej rovnice v* $\mathbb{N}$. *Ak je tam* -1 *umocníme poslednú rovnosť na druhú a dostávame, že* $X'^2 + AY'^2, 2X'Y'$ *sú riešenia v* $\mathbb{N}$. *Teda sme dokázali, že Pellova rovnica, tak ako je definovaná vzťahom* $(*)$ *na strane 24, má aspoň jedno riešenie v množine prirodzených čísel.*

Teraz si ukážeme ako nájdeme všetky riešenia tejto rovnice v množine prirodzených čísel. Nech x_0, y_0 *sú také prirodzené čísla, že*

$$x_0 + y_0\sqrt{A} = \min\{x + y\sqrt{A}, x, y \in \mathbb{N}, x^2 - y^2A = 1\}.$$

Je zrejmé, že aj x_0, y_0 *je riešenie tejto rovnice. Toto riešenie sa nazýva* **fundamentálne riešenie**. *Dokážeme, že ak* $x, y \in \mathbb{N}$ *a* $x^2 - Ay^2 = 1$, *tak existuje* $n \in \mathbb{N}$, *že*

$$x + y\sqrt{A} = (x_0 + y_0\sqrt{A})^n. \qquad (***)$$

Predpokladajme, že to neplatí. Potom existuje také $n \in \mathbb{N}$*, že*

$$(x_0 + y_0\sqrt{A})^n < x + y\sqrt{A} < (x_0 + y_0\sqrt{A})^{n+1},$$

a teda

$$1 < (x + y\sqrt{A})(x_0 - y_0\sqrt{A})^n < (x_0 + y_0\sqrt{A}),$$

pretože $x_0 - y_0\sqrt{A} = (x_0 + y_0\sqrt{A})^{-1}$*. Je zrejmé, že* $(x + y\sqrt{A})(x_0 - y_0\sqrt{A})^n = c + d\sqrt{A}$*, kde* c, d *je tiež riešenie našej rovnice. Teda sme našli riešenie* c, d *také, že* $1 < c + d\sqrt{A} < x_0 + y_0\sqrt{A}$*. Ľahko sa preverí, že* $c, d \in \mathbb{N}$ *a preto dostávame spor s minimalitou* $x_0 + y_0\sqrt{A}$*.*

– – – – – – – – – – – –

Úloha 109. Nech $a, b, c \in \mathbb{Z}$ a $m \in \mathbb{N}$. Ak $(m, c) = 1$, potom

$$ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}.$$

Dokážte.

Úloha 110. Nech $a, b, c \in \mathbb{Z}$, $c|a$, $c|b$ a $m \in \mathbb{N}$, $c|m$. Potom

$$a \equiv b \pmod{m} \implies \tfrac{a}{c} \equiv \tfrac{b}{c} \pmod{|\tfrac{m}{c}|}.$$

Dokážte.

Tvrdenia v úlohách 106 až 110 nám dávajú návod, ako možno transformovať vlastnosti operácií s rovnosťami na kongruencie. Tvrdenie úlohy 109 sa často nazýva *zákon o krátení v kongruencii*. Čitateľ iste pochopí, že podmienka $(m, c) = 1$ má pre platnosť tvrdenia veľmi dôležitý význam.

Úloha 111. Nech $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$. Ak $a \equiv b \pmod{m}$, potom

$$m|a \iff m|b.$$

Dokážte.

Úloha 112. Nech $a, b \in \mathbb{Z}$ a $m, m_1 \in \mathbb{N}$. Ak $m_1|m$, potom

$$a \equiv b \pmod{m} \implies a \equiv b \pmod{m_1}.$$

Dokážte.

Dokázané tvrdenie teraz použijeme na odvodenie niektorých známych kritérií deliteľnosti.

Úloha 113. Nech $n \in \mathbb{N}$. Potom

$$10^n \equiv 1 \pmod{9}.$$

Dokážte.

(Návod: Postupujte matematickou indukciou alebo priamo pomocou binomickej vety rozviňte $10^n = (9 + 1)^n$.)

Úloha 114. Označme symbolom $cs(a)$ ciferný súčet prirodzeného čísla a. Dokážte, že

$$a \equiv cs(a) \pmod 9.$$

(Návod: Použite úlohu 113.)
Úloha 115. Nech $cs(a)$ označuje ciferný súčet čísla a. Dokážte, že pre každé $a \in \mathbb{N}$.
a) $9|a \iff 9|cs(a)$,
b) $3|a \iff 3|cs(a)$.

(Návod: Použite úlohy 111, 112, 114.)

Úloha 116. Nech $n \in \mathbb{N}$. Potom

$$10^n \equiv (-1)^n \pmod{11}.$$

Dokážte.

Úloha 117. Prirodzené číslo je deliteľné 11 práve vtedy, keď je rozdiel súčtu cifier na párnych miestach a súčtu cifier na nepárnych miestach deliteľný 11. Dokážte.

Úloha 118. Nech $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$. Ak $a \equiv b \pmod m$, potom $(a, m) = (b, m)$. Dokážte.

Tvrdenie, ktoré teraz dokážeme, sa nazýva *Eulerova veta*.

Veta 7. Nech $m \in \mathbb{N}$**. Ak** $a \in \mathbb{N}$ **a** $(a, m) = 1$**, potom**

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

Dôkaz vety 7 si rozdelíme do niekoľkých úloh.

Úloha 119. Nech $a, b, m \in \mathbb{N}$. Ak $(a, m) = 1, (b, m) = 1$, potom $(ab, m) = 1$. Dokážte.

(Návod: Použite napríklad vetu 2 alebo úlohu 30.)

V nasledujúcej časti budeme používať takéto označenie. Nech a, m sú z Vety 7 a $a_1, ..., a_{\varphi(m)}$ sú všetky čísla patriace do množiny $\{1, ..., m\}$, ktoré sú nesúdeliteľné s číslom m. Množinu $\{a_1, ..., a_{\varphi(m)}\}$ budeme nazývať *redukovaným zvyškovým systémom modulo* m a označovať symbolom R_m.

Úloha 120. Ak $aa_i \equiv aa_j \pmod m$, potom $a_i = a_j$. Dokážte.

(Návod: Použite úlohu 109.)

Úloha 121. Pre každé $i \leq \varphi(m)$ existuje $j(i) \leq \varphi(m)$ také, že

$$aa_i \equiv a_{j(i)} \pmod m.$$

Ak $i_1 \neq i_2$, potom $j(i_1) \neq j(i_2)$. Dokážte.

(Návod: Použite úlohu 118. Pri dôkaze druhej časti použite úlohu 120.)

Úloha 122. Ak $b_i \equiv c_i \pmod{m}$ pre $i = 1, ..., k$, potom

$$b_1...b_k \equiv c_1...c_k \pmod{m}$$

pre $b_i, c_i \in \mathbb{Z}$. Dokážte.

Úloha 123. Dokážte, že

$$(aa_1)...(aa_{\varphi(m)}) \equiv a_1...a_{\varphi(m)} \pmod{m}.$$

Úloha 124. Dokážte, že

$$(a_1...a_{\varphi(m)}, m) = 1.$$

(Návod: Použite úlohu 119.)

Úloha 125. Pomocou úloh 109, 123 a 124 dokážte vetu 7.

Leonard Euler pochádzal z mesta Bazilej vo Švajčiarsku. Bol členom Petrohradskej akadémie vied. Je autorom približne 800 vedeckých prác. Zaoberal sa trigonometriou, analýzou, newtonovskou mechanikou, variačným počtom a tiež aj teóriou čísel. Napísal mnoho učebníc a bol taktiež aktívny aj v oblastiach mimo matematiky. Napísal napríklad knihy o delostrelectve a stavbe lodí.

Jedným z dôsledkov Eulerovej vety je nasledujúci zaujímavý vzťah medzi aritmetickými a geometrickými postupnosťami, ktorý dávame čitateľovi na precvičenie.

Tvrdenie. Každá aritmetická postupnosť prirodzených čísel obsahuje geometrickú potupnosť.

Úloha A. Označme $A = \{a + kr : k = 0, 1, ...\}$ pre $a, r \in \mathbb{N}$. Potom

$$\forall\, x \in \mathbb{N};\ x \in A \iff x \equiv a \pmod{r}.$$

Úloha B. Nech $a, r \in \mathbb{N}$, a $(a, r) = 1$. Označme $q = a^{\varphi(r)}$ a $A = \{a + kr : k = 0, 1, ...\}$. Dokážte, že $aq^n \in A$ pre $n = 1, 2, ...$

(Návod: Použite Eulerovu vetu a úlohu A.)

Úloha C. Dokážte tvrdenie.

Veta 7 bola známa najskôr pre prípad, keď $m = p$ bolo prvočíslo. V tomto prípade sa veta 7 nazýva *malá Fermatova veta*. Je pomenovaná po svojom objaviteľovi. Pierre Fermat (1601-1665) sa neživil matematikou, ale bol právnik.

Vytvoril však veľké matematické dielo. Malá Fermatova veta je obsahom nasledujúcej úlohy.

Úloha 126. Nech p je prvočíslo. Ak $a \in \mathbb{N}$ a $(a,p)=1$, potom

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokážte.

(Návod: Použite vetu 7.)

Malú Fermatovu vetu môžeme dokázať aj bez použitia Eulerovej vety. Takýto dôkaz nájdeme v nasledujúcich úlohách.

Úloha A. Dokážte, že malá Fermatova veta je ekvivalentná s tvrdením: Pre každé prvočíslo p a prirodzené číslo a platí

$$a^p \equiv a \pmod{p}.$$

Úloha B. Nech p je prvočíslo. Potom pre $1 < k < p$ je binomický koeficient $\binom{p}{k}$ deliteľný p.

Úloha C. Dokážte malú Fermatovou vetu pomocou úloh A, B a s použitím matematickej indukcie podľa a.

Veta 7 nám ukazuje jednu zaujímavú možnosť.

Úloha 127. Ak $a, m \in N$ a $(a,m)=1$, potom existuje $a' \in \mathbb{N}$, $a' < m$ také, že

$$aa' \equiv 1 \pmod{m}.$$

Dokážte.

(Návod: Označme $a' = a^{\varphi(m)-1} \pmod{m}$. Toto a' niekedy označujeme aj $\frac{1}{a} \mod m$.)

Úloha 128. Ak $a, m \in \mathbb{N}$, potom $(a,m)=1$ práve vtedy, keď existuje $a' \in \mathbb{N}$ také, že

$$aa' \equiv 1 \pmod{m}.$$

Dokážte.

(Návod: Použite úlohu 17.)

Vidíme, že kongruencie a rovnosti majú podobné vlastnosti. Uvažujme teraz kongruencie obsahujúce neznámu. *Lineárnou kongruenciou s neznámou* x nazývame kongruenciu

$$ax \equiv b \pmod{m} \tag{12}$$

pre $a, b, m \in \mathbb{N}$. Riešením tejto kongruencie nazývame každé celé číslo x, ktoré vyhovuje rovnici (12). Ak toto riešenie naviac patrí do množiny $\{0, ..., m-1\}$, budeme ho nazývať *primitívnym riešením.*

Úloha 129. Ak x je riešením kongruencie (12), potom $x \mod m$ je primitívnym riešením kongruencie (12). Dokážte.

Úloha 130. Ak $(a, m) = 1$, potom kongruencia (12) má práve jedno primitívne riešenie. Dokážte.

(Návod: Použite úlohu 128.)
Úloha 131. Ak x je riešením kongruencie (12), potom aj čísla $x + tm, t \in \mathbb{Z}$ sú riešenia kongruencie (12). Dokážte.

Úloha 132. Ak $(a, m) = 1$ a x_0 je primitívnym riešením kongruencie (12), potom $x \in \mathbb{Z}$ je riešením kongruencie (12) práve vtedy, keď $x \equiv x_0 \pmod{m}$. Dokážte.

Úloha 133. Kongruencia (12) má riešenie práve vtedy, keď $(a, m)|b$. Dokážte.

(Návod: Použite vetu 2.)

Úloha 134. Ak $(a, m)|b$ a x_0 je primitívne riešenie kongruencie

$$\tfrac{a}{(a,m)}x \equiv \tfrac{b}{(a,m)} \pmod{\tfrac{m}{(a,m)}},$$

potom $x = x_0 + t\frac{m}{(a,m)}, t = 0, ..., (a, m)-1$ sú všetky primitívne riešenia kongruencie (12). Dokážte.

(Návod: Použite úlohu 132.)

Vidíme, že kongruencia (12) buď nemá žiadne riešenie alebo má práve (a, m) primitívnych riešení.

– – – – – – – – – – –

Eulerova veta sa dá použiť na výpočet hodnoty a', ak $(a, m) = 1$. Ak m je malé číslo, hodnotu a' môžeme nájsť preskúšaním. Ale ak m je veľké číslo, je tento postup veľmi prácny. Vtedy môžeme použiť to, že z Eulerovej vety vyplýva $a' \equiv a^{\varphi(m)-1} \pmod{m}$. Využijeme, že vypočítať mocninu je podstatne rýchlejšie ako preskúmať všetky možnosti. Napríklad chceme vypočítať $\frac{1}{5} \pmod{101} = a'$. Hneď dostávame, že $a' \equiv 5^{\varphi(101)-1} \pmod{101} = 5^{99} \pmod{101} = (5^3)^{33} \pmod{101} = 24^{33} \pmod{101} = 40^{11} \pmod{101} = 40 \cdot ((40)^2)^5 \pmod{101} = 40 \cdot 85^5 \pmod{101} = ...$

Ďalšie použitie Eulerovej vety spočíva v riešení kongruencií tvaru

$$x^\alpha \equiv a \pmod{m}, \qquad (**)$$

kde $(a,m)=1$ *a* $(\alpha,\varphi(m))=1$. *Položme* $\alpha'=\alpha^{\varphi(\varphi(m))-1} \pmod{\varphi(m)}$. *Podľa Eulerovej vety dostávame* $\alpha\cdot\alpha'\equiv 1 \pmod{\varphi(m)}$. *Keď umocníme* $(**)$ *na* α', *dostávame* $x^{\alpha\cdot\alpha'}\equiv a^{\alpha'} \pmod{m}$. *Ale* $\alpha\cdot\alpha'=k\cdot\varphi(m)+1$, *a teda opäť podľa Eulerovej vety dostávame* $x^{\alpha\cdot\alpha'}\equiv x \pmod{m}$ *a teda* $x\equiv a^{\alpha'} \pmod{m}$.

Cvičenie 1. *Riešte kongruenciu* $x^5\equiv 2 \pmod{169}$.

– – – – – – – – – – – –

Teraz sa vrátime k úvahám z predchádzajúcej kapitoly, teda k odvodeniu vzorca pre Eulerovu funkciu φ pomocou čínskej zvyškovej vety. Najskôr si ju sformulujeme a dokážeme. Predtým si zavedieme nasledujúce užitočné označenie. Ak $m\in\mathbb{N}$, potom množinu $\{0,...,m-1\}$ budeme označovať symbolom $\mathbb{Z}_m$ a budeme ju nazývať *úplným zvyškovým systémom modulo* m. Teraz prejdeme k čínskej zvyškovej vete.

Veta 8. Nech $m_1,...,m_k\in\mathbb{N}$ **a** $(m_i,m_j)=1$ **pre** $i\neq j$**. Označme** $m=m_1...m_k$**. Ak** $b_1,...,b_k\in\mathbb{Z}$**, potom existuje jediné číslo** $x\in\mathbb{Z}_m$**, ktoré vyhovuje kongruenciám**

$$\begin{gathered} x\equiv b_1 \pmod{m_1}\\ ...\\ x\equiv b_k \pmod{m_k}. \end{gathered}$$

Toto tvrdenie nám teda hovorí o nejakom čísle x, ktoré môžeme nazvať primitívnym riešením sústavy kongruencií. Dôkaz tohto tvrdenia budú obsahovať nasledujúce úlohy. Najskôr dokážeme jednoznačnosť čísla x.

Úloha 135. Nech $m\in\mathbb{N}$ a $x_1,x_2\in\mathbb{Z}_m$. Ak $x_1\equiv x_2 \pmod{m}$, potom $x_1=x_2$. Dokážte.

Úloha 136. Nech $m_1,...,m_k\in\mathbb{N}$ a $(m_i,m_j)=1$ pre $i\neq j$. Ak pre $x_1,x_2\in\mathbb{Z}$ platí

$$\begin{gathered} x_1\equiv x_2 \pmod{m_1}\\ ...\\ x_1\equiv x_2 \pmod{m_k}, \end{gathered}$$

potom

$$x_1\equiv x_2 \pmod{m_1...m_k}.$$

Dokážte.

(Návod: Postupujte matematickou indukciou vzhľadom na k, použite vetu 3 a jej dôsledok.)

Úloha 137. Dokážte, že existuje najviac jedno $x\in\mathbb{Z}_m$, ktoré vyhovuje kongruencii z vety 8.

(Návod: Použite úlohy 135 a 136.)

Teraz postačuje dokázať iba existenciu prirodzeného čísla x s uvedenými vlastnosťami. Budeme predpokladať, že platí označenie a predpoklady vety 8.

Úloha 138. Dokážte, že pre $i = 1, ..., k$ platí $(\frac{m}{m_i}, m_i) = 1$.

Úloha 139. Dokážte, že pre $i, j = 1, ..., k$, $i \neq j$ platí

$$\frac{m}{m_i} \equiv 0 \pmod{m_j}.$$

Úloha 140. Dokážte, že pre $i, j = 1, ..., k$, $i \neq j$ platí

$$\left(\frac{m}{m_i}\right)^{\varphi(m_i)} \equiv 1 \pmod{m_i}$$

a

$$\left(\frac{m}{m_i}\right)^{\varphi(m_i)} \equiv 0 \pmod{m_j}.$$

(Návod: Použite úlohy 138 a 139.)

Úloha 141. Označme

$$x_0 = b_1\left(\frac{m}{m_1}\right)^{\varphi(m_1)} + ... + b_k\left(\frac{m}{m_k}\right)^{\varphi(m_k)}.$$

Dokážte, že x_0 vyhovuje kongruenciám z vety 8.

(Návod: Použite úlohu 140.)

Úloha 142. Nech x_0 má význam ako v úlohe 141. Označme $x = x_0 \mod m$. Dokážte, že x spĺňa požiadavky vety 8.

Týmto sme dokázali čínsku zvyškovú vetu.

Cvičenie 1. Nájdite $x \in \{0, 1, 2, ..., 104\}$, aby

$$x \equiv 1 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 6 \pmod{6}.$$

Praktické použitie čínskej zvyškovej vety si môžeme predstaviť aj tak, že potrebujeme oznámiť n informácií n prijímateľom. Prijímateľom priradíme navzájom nesúdeliteľné čísla $m_1, m_2, ..., m_n$ a informáciám čísla $x_1 \in \mathbb{Z}_{m_1}, x_2 \in \mathbb{Z}_{m_2}, ..., x_n \in \mathbb{Z}_{m_n}$. Pomocou čínskej zvyškovej vety nájdeme $x_1 \in \mathbb{Z}_{m_1...m_n}$ také, že $x \equiv x_j \pmod{m_j}, j = 1, 2, ..., n$. Táto hodnota x v sebe už nesie všetky informácie $x_1, x_2, ..., x_n$.

Úloha 143. Nech $m_1, m_2 \in \mathbb{N}$ a $(m_1, m_2) = 1$. Označme $m = m_1 m_2$. Ak $b_1, b_2 \in \mathbb{Z}$, potom existuje jediné číslo $x \in \mathbb{Z}_m$, ktoré vyhovuje kongruenciám

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}.$$

Dokážte.

(Návod: Aplikujte tvrdenie vety 8 pre $k = 2$.)

Ďalšie použitie čínskej zvyškovej vety je pri určovaní počtu riešení polynomickej kongruencie.

Tvrdenie. *Nech $f(x)$ je polynom s celočíselnými koeficientami a $m_1, m_2 \in \mathbb{N}, (m_1, m_2) = 1$. Označme N_1 počet primitívnych riešení kongruencie $f(x) \equiv 0 \pmod{m_1}$ a N_2 počet primitívnych riešení kongruencie $f(x) \equiv 0 \pmod{m_2}$. Potom kongruencia $f(x) \equiv 0 \pmod{m_1 \cdot m_2}$ má $N_1 \cdot \mathbb{N}_2$ primitívnych riešení.*

Dôkaz. Nech x je primitívne riešenie kongruencie $f(x) \equiv 0 \pmod{m_1 \cdot m_2}$. Potom x mod m_1 je primitívne riešenie kongruencie $f(x) \equiv 0 \pmod{m_1}$ a x mod m_2 je primitívne riešenie kongruencie $f(x) \equiv 0 \pmod{m_2}$.

Naopak, ak x_1 je primitívne riešenie kongruencie $f(x) \equiv 0 \pmod{m_1}$ a x_2 je primitívne riešenie kongruencie $f(x) \equiv 0 \pmod{m_2}$, tak podľa čínskej zvyškovej vety existuje práve jedno $x \in \mathbb{Z}_{m_1 \cdot m_2}$, že platí $x \equiv x_1 \pmod{m_1}$,$x \equiv x_2 \pmod{m_2}$ a teda $f(x) \equiv 0 \pmod{m_1}$,$f(x) \equiv 0 \pmod{m_2}$ a teda $f(x) \equiv 0 \pmod{m_1 \cdot m_2}$.

Podobný postup teraz použijeme na dôkaz toho, že funkcia φ je multiplikatívna. Nebudeme používať výsledky uvedené v predchádzajúcej kapitole.

Úloha 144. Dokážte, že pre $m \in \mathbb{N}$ platí $|R_m| = \varphi(m)$.

(Návod: Tvrdenie v úlohe vyplýva z definície funkcie φ.)

Teda na to, aby sme dokázali multiplikatívnosť funkcie φ nám stačí dokázať, že pre $m, n \in \mathbb{N}, (m, n) = 1$ platí

$$|R_{mn}| = |R_m||R_n|.$$

Úloha 145. Nech $a, m, n \in \mathbb{N}$. Ak $(a, mn) = 1$, potom $(a \mod m, m) = 1$ a $(a \mod n, n) = 1$. Dokážte.

Nech $m, n \in \mathbb{N}$, $(m, n) = 1$. Definujme zobrazenie

$$F : R_{mn} \to R_m \times R_n$$

nasledujúcim spôsobom: pre $a \in R_{mn}$

$$F(a) = (a \mod m, a \mod n).$$

Definícia funkcie F je korektná vďaka úlohe 145.

Úloha 146. Dokážte, že F je injektívne zobrazenie.

Úloha 147. Dokážte, že F je surjektívne zobrazenie.

(Návod: Použite úlohu 143.)

Úloha 148. Dokážte, že φ je multiplikatívna aritmetická funkcia.

Cvičenie. Dokážte rovnosť z úlohy 103 pomocou multiplikatívnosti aritmetickej funkcie

$$\Phi(n) = \sum_{d|n} \varphi(n).$$

Úloha 149. Nech p je prvočíslo a $\alpha \in \mathbb{N}$. Dokážte, že

$$\varphi(p^\alpha) = p^\alpha\Big(1 - \tfrac{1}{p}\Big).$$

(Návod: Použite úlohu 21.)

Úloha 150. Nech $n \in \mathbb{N}$ a $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ je kanonický rozklad čísla n. Potom

$$\varphi(n) = n\Big(1 - \tfrac{1}{p_1}\Big)...\Big(1 - \tfrac{1}{p_k}\Big).$$

Dokážte.

Existujú aj ďalšie dôkazy platnosti tohto vzorca. Jeden z nich je založený na tvrdení, ktoré nazývame *princíp zapojenia a vypojenia*. Je však pomerne neprehľadný.

Teraz sa budeme zaoberať kongruenciami, v ktorých sa neznáma x vyskytuje s druhou mocninou. Tieto kongruencie nazývame *kvadratické kongruencie*.

Nech $m \in \mathbb{N}$. Číslo $a \in \mathbb{N}$ nazývame kvadratickým zvyškom modulo m, ak kongruencia

$$x^2 \equiv a \pmod{m}.$$

má riešenie.
Pripomeňme, že uvažujeme $a \neq 0$.

Úloha 151. Nech $a, m \in \mathbb{N}$. Dokážte, že

$$(m-a)^2 \equiv a^2 \pmod{m}.$$

Ďalej sa budeme zaoberať prípadom, keď $m = p$ je pevne zvolené nepárne prvočíslo.

Úloha 152. Nech $a, b \in \mathbb{Z}_p$. Ak

$$a^2 \equiv b^2 \pmod{p},$$

potom $a = b$ alebo $a = p - b$. Dokážte.

(Návod: Pri riešení úloh 151 a 152 je vhodné použiť úlohu 106 alebo úlohu 21.)

Použitím úloh 151 a 152 dokážte:

Úloha 153. V množine $\mathbb{Z}_p$ je práve $\frac{p-1}{2}$ kvadratických zvyškov.

Úloha 154. Ak a je kvadratický zvyšok modulo p a $(a, p) = 1$, potom

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

(Návod: Uvedomte si, že $x^2 \equiv a \pmod{p}$ pre $(x, p) = 1$ a použite úlohu 126.)

Vidíme, že kongruencia $x^2 \equiv a \pmod{p}$ má riešenie iba pre polovicu čísel $a \in \{1, ..., p-1\}$.

Teraz si ukážeme, ako môžeme riešiť všeobecnejšie kvadratické kongruencie s prvočíselným modulom p. Budeme sa zaoberať kongruenciami typu

$$x^2 + ax + b \equiv 0 \pmod{p} \tag{13}$$

kde $a, b \in \mathbb{Z}_p$.

Ak a je kvadratický zvyšok modulo p, potom symbolom $sq_p a$ budeme z dôvodov jednoznačnosti označovať najmenšie prirodzené riešenie kongruencie

$$x^2 \equiv a \pmod{p}.$$

Existuje algoritmus pre výpočet $sq_p a$.

Úloha 155. Ak $x \in \mathbb{Z}_p$ je riešením kongruencie $x^2 \equiv a \pmod{p}$, potom $x = sq_p a$ alebo $x = p - sq_p a$. Dokážte.

(Návod: Použite úlohu 152.)

Úloha 156. Dokážte, že pre každé celé číslo x platí

$$x^2 + ax + b \equiv (x + \tfrac{p+1}{2}a)^2 - \tfrac{(p+1)^2a^2 - 4b}{4} \pmod{p}.$$

Úloha 157. Kongruencia (13) má riešenie práve vtedy, keď číslo

$$\tfrac{(p+1)^2a^2 - 4b}{4} = D$$

je kvadratický zvyšok modulo p. Jej riešenia sú určené vzťahmi

$$x \equiv -\tfrac{p+1}{2}a + sq_p D \pmod{p}$$

$$x \equiv -\tfrac{p+1}{2}a + p - sq_pD \pmod{p}.$$

(Návod: Použite úlohy 152 a 155.)

Úloha 158. Nájdite všetky kvadratické zvyšky modulo 7.

(Riešenie: 0, 1, 2, 4.)

Úloha 159. Riešte kvadratickú kongruenciu

$$x^2 + 2x + 6 \equiv 0 \pmod{7}.$$

Úloha 160. Pokúste sa zovšeobecniť postup z úloh 155, 156 a 180 na ľubovoľný modul. Bude platiť tvrdenie úlohy 155 ?

Kvadratických zvyškov sa týka jeden z najelegantnejších výsledkov elementárnej teórie čísel, takzvaný *Gaussov kvadratický zákon reciprocity*. Budeme sa mu venovať neskôr.

Túto časť ukončíme tvrdením, ktoré nazývame *Wilsonova veta*.

Veta 9.Nech p je nepárne prvočíslo. Potom

$$(p-1)! \equiv -1 \pmod{p}.$$

V ďalšej časti budeme predpokladať, že p je nepárne prvočíslo.

Úloha 161. Ak $a \in \mathbb{Z}_p$ a

$$a^2 \equiv 1 \pmod{p},$$

potom $a = 1$ alebo $a = p - 1$. Dokážte.

Úloha 162. Ak $a, b_1, b_2 \in \mathbb{Z}_p$ a

$$ab_1 \equiv 1 \pmod{p}$$

a

$$ab_2 \equiv 1 \pmod{p},$$

potom $b_1 = b_2$. Dokážte.

Ak $a \in \mathbb{Z}_p$ a $a \neq 0$, potom podľa úlohy 128 existuje a' také, že $aa' \equiv 1 \pmod{p}$. Podľa úlohy 162 existuje v množine $\mathbb{Z}_p$ iba jediné také a'. Budeme ho nazývať inverzným prvkom k a modulo p. V prípade, že nebude hroziť nejednoznačnosť, budeme ho označovať a^{-1}, pričom p vynecháme.

Úloha 163. Ak $a \in \mathbb{Z}_p$, potom $a = a^{-1}$ práve vtedy, keď‘ $a = 1$ alebo $a = p - 1$. Dokážte.

(Návod: Použite úlohu 161.)

Úloha 164. Nech $a, b \in \mathbb{Z}_p$. Potom $a^{-1} = b^{-1}$ práve vtedy, keď $a = b$. Dokážte.

Označme pre $a \in \{2, ..., p-2\}$

$$I_a = \{a, a^{-1}\}.$$

Úloha 165. Dokážte, že

$$\bigcup_{a=2}^{p-2} I_a = \{2, ..., p-2\}.$$

Úloha 166. Dokážte, že pre všetky $a, b \in \{2, ..., p-2\}$ platí : $I_a \cap I_b \neq \emptyset$ práve vtedy, keď $a = b$ alebo $a = b^{-1}$ a vtedy platí, že $I_a = I_b$.

Úloha 167. Dokážte, že existuje $\frac{p-3}{2}$ prvkov $a_1, ..., a_{\frac{p-3}{2}}$ takých, že platí

$$\bigcup_{j=1}^{\frac{p-3}{2}} I_{a_j} = \{2, ..., p-2\}$$

a $I_{a_j} \cap I_{a_i} = \emptyset$ ak $i \neq j$.

Uvažujte najmenšie také k, že $\bigcup\limits_{j=1}^{k} I_{a_j} = \{2, ..., p-2\}$ pre nejaké $a_1, ..., a_k$.

Úloha 168. Dokážte, že

$$(p-2)! \equiv 1 \pmod{p}.$$

(Návod: Použite úlohu 167.)

Úloha 169. Dokážte vetu 9.

Použitie Wilsonovej vety si ukážeme na dôkaze nasledujúceho tvrdenia.

Tvrdenie. Nech p je nepárne prvočíslo a

$$1 + \tfrac{1}{2} + \cdots + \tfrac{1}{p} \;=\; \tfrac{A}{p!}.$$

Potom $A \equiv -1 \pmod{p}$.

Úloha A. Dokážte, že čísla

$$p!,\ \tfrac{p!}{2}, \ldots,\ \tfrac{p!}{p-1}$$

sú deliteľné číslom p.

Úloha B. Dokážte tvrdenie.

Úloha C. Dokážte, že súčet $1 + \frac{1}{2} + \cdots + \frac{1}{p}$ nie je celé číslo pre žiadne p.