10. GAUSSOV KVADRATICKÝ ZÁKON RECIPROCITY

Nech p je nepárne prvočíslo. Ako sme už povedali, prirodzené číslo a, pre ktoré platí, že $(a,p)=1$, nazývame kvadratickým zvyškom modulo p práve vtedy, keď kongruencia

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

má riešenie. Prirodzené číslo, ktoré nie je kvadratickým zvyškom modulo p, nazývame kvadratickým nezvyškom modulo p. Pre štúdium kvadratických zvyškov používame nasledujúci symbol.
Nech p je nepárne prvočíslo a $a \in \mathbb{N}$. Potom

$$\left(\frac{a}{p}\right) = 1, \text{ ak } a \text{ je kvadratický zvyšok modulo } p$$

$$\left(\frac{a}{p}\right) = -1, \text{ ak } a \text{ je kvadratický nezvyšok modulo } p.$$

Symbol $\left(\frac{a}{p}\right)$ pochádza od Legendra, a preto sa nazýva aj *Legendrov symbol.*

Úloha 209. Nech p je nepárne prvočíslo. Dokážte, že pre každé $a \in \mathbb{N}$ také, že $(a,p)=1$ platí

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

(Návod: Uvedomte si, že podľa malej Fermatovej vety, ktorú nájdeme v úlohe 126, platí $(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1) \equiv 0 \pmod{p}$.)

Úloha 210. Nech p je nepárne prvočíslo. Dokážte, že pre každé $a \in \mathbb{N}$ také, že $(a,p)=1$ platí

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(Návod: Uvedomte si, že kvadratické zvyšky sú podľa úlohy 154 primitívnymi koreňmi kongruencie $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ a podľa Lagrangeovej vety nemá táto kongruencia viac ako $\frac{p-1}{2}$ primitívnych koreňov.)

Úloha 211. Dokážte, že pre nepárne prvočíslo p platí

$$\left(\frac{1}{p}\right) = 1, \ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

(Návod: Použite úlohu 210.)

Úloha 212. Ak p je prvočíslo tvaru $4k+1$, potom -1 je kvadratický zvyšok modulo p a ak p je prvočíslo tvaru $4k+3$, potom -1 je kvadratický nezvyšok modulo p.

(Návod: Dosaďte do úlohy 211.)

Úloha A. Nech $a \in \mathbb{N}$. Potom prvočíselné delitele čísla a^2+1 môžu byť iba číslo 2 alebo prvočísla tvaru $4k+1$.

(Návod: Ak $p|a^2+1$, potom -1 je kvadratický zvyšok modulo p.)

Pomocou tejto skutočnosti sa dá dokázať, že existuje nekonečne veľa prvočísel tvaru $4k+1$. Podobne ako pri Euklidovom dôkaze nekonečnosti prvočíselnej množiny ukážeme, že ku každej konečnej množine prvočísel tvaru $4k+1$ existuje ďalšie, ktoré do nej nepatrí. Nech $p_1, p_2, ..., p_n$ sú prvočísla tvaru $4k+1$. Uvažujme číslo $A = (2p_1p_2 \cdots p_n)^2 + 1$. Ak prvočíslo $p|A$, tak platí $(2p_1p_2 \cdots p_n)^2 \equiv -1 \pmod{p}$ a teda $(\frac{-1}{p}) = 1$ a teda $p = 4k+1$. Ale evidentne $p \neq p_i, i = 1, 2, ..., n$.

Úloha 213. Nech p je nepárne prvočíslo a $(a,p) = 1$, $(b,p) = 1$. Potom

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Dokážte.

(Návod: Použite úlohu 210.)

Úloha 214. Dokážte, že pre nepárne prvočíslo p a čísla $a_1, \ldots, a_k$, také, že $(a_i, p) = 1$, $i = 1, \ldots, k$ platí

$$\left(\frac{a_1 \ldots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \ldots \left(\frac{a_k}{p}\right).$$

Ďalej dokážeme explicitný vzorec pre hodnotu Legendrovho symbolu.

Veta 12. Ak $p > 2$ je prvočíslo a $(a,p) = 1$, potom

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p_1} \left[\frac{2ak}{p}\right]},$$

kde $p_1 = \frac{p-1}{2}$.

Dôkaz vety 12 nájdeme v nasledujúcich úlohách.

Úloha 215. Nech $p > 2$ je prvočíslo a $x \in \mathbb{N}$. Potom

$$\left[\frac{2x}{p}\right] = 2\left[\frac{x}{p}\right] + \left[2\left\{\frac{x}{p}\right\}\right].$$

Dokážte.

(Návod: Uvažujte nasledujúce dve možnosti: $\left\{\frac{x}{p}\right\} < \frac{1}{2}$ alebo $\left\{\frac{x}{p}\right\} > \frac{1}{2}$.)

Úloha 216. Nech $x \in \mathbb{N}$ a $p > 2$ je prvočíslo. Potom

$$x \mod p \leq \frac{p-1}{2}$$

práve vtedy, keď $2 \left| \left[\frac{2x}{p} \right] \right.$.

(Návod: Uvedomte si, že podľa úlohy 7, $x \pmod p = p \cdot \left\{ \frac{x}{p} \right\}$ a výraz $\left[2 \left\{ \frac{x}{p} \right\} \right]$ v úlohe 215 nadobúda iba hodnoty $0, 1$.)

Úloha 217. Nech $p > 2$ je prvočíslo a $p_1 = \frac{p-1}{2}$. Nech $x \in \mathbb{N}$. Potom existuje práve jedno číslo $r \in \{0, \ldots, p_1\}$ také, že

$$x \equiv (-1)^{\left[\frac{2x}{p} \right]} r \pmod p.$$

Dokážte.

(Návod: Použite úlohu 216.)

Úloha 218. Nech $(a, p) = 1$ a $p_1 = \frac{p-1}{2}$. Ak pre $r_1, r_2 \in \{0, 1, \ldots, p_1\}$ platí

$$ar_1 \equiv ar_2 \pmod p,$$

potom $r_1 = r_2$. Dokážte.

Úloha 219. Nech $p > 2$ je prvočíslo a $(a, p) = 1$. Nech $p_1 = \frac{p-1}{2}$ a nech pre $j = 1, \ldots, p_1$ platí

$$a \cdot j \equiv (-1)^{\left[\frac{2aj}{p} \right]} r_j \pmod p,$$

kde $r_j \in \{1, \ldots, p_1\}$. Dokážte, že $\{r_1, \ldots, r_{p_1}\} = \{1, \ldots, p_1\}$.

Úloha 220. Dokážte, že pre prvočíslo $p > 2$ a $(a, p) = 1$ platí

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{j=1}^{p_1} \left[\frac{2aj}{p} \right]} \pmod p.$$

(Návod: Vynásobte kongruencie z úlohy 219.)

Z úlohy 220 bezprostredne vyplýva veta 12.

Úloha 221. Nech $p > 2$ je prvočíslo. Potom

$$\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}.$$

Dokážte.

(Návod: Použite vetu 12 a úpravu $\left(\frac{2}{p} \right) = \left(\frac{2(1+p)}{p} \right) = \left(\frac{4 \cdot \frac{p+1}{2}}{p} \right) = \left(\frac{\frac{p+1}{2}}{p} \right)$.)

Úloha B. Číslo $a^2 - 2$, $a \in \mathbb{N}$ môže obsahovať v kanonickom rozklade iba 2 a prvočísla tvaru $8k + 1$, $8k - 1$.

Úloha C. Číslo $a^2 + 2$, $a \in \mathbb{N}$ môže obsahovať v kanonickom rozklade iba 2 a prvočísla tvaru $8k + 1$, $8k + 3$.

(Návod: Použite postup z úlohy A a úlohu 221.)

Úloha 222. Ak p je nepárne prvočíslo a $a \in \mathbb{N}$ je nepárne číslo, potom

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p_1} \left[\frac{ak}{p}\right]},$$

kde $p_1 = \frac{p-1}{2}$. Dokážte.

(Návod: Využite rovnosť $\left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right)$ a $\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)$ a použite úlohu 220 a vetu 12.)

Pomocou úlohy 222 dokážeme nasledujúce tvrdenie, ktoré je známe pod názvom *Gaussov kvadratický zákon reciprocity.*

Veta 13. Nech $p \neq q$ sú dve nepárne prvočísla. Potom

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Úloha 223. Nech platí označenie z vety 13. Nech $p_1 = \frac{p-1}{2}$, $q_1 = \frac{q-1}{2}$. Dokážte, že

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{p_1} \left[\frac{qj}{p}\right] + \sum_{k=1}^{a_1} \left[\frac{pk}{q}\right]}.$$

Úloha 224. Nech $p \neq q$ sú dve nepárne prvočísla. Uvažujme množinu

$$D = \left\{[qj, pk];\ j = 1, \ldots, \tfrac{p-1}{2},\ k = 1, \ldots, \tfrac{q-1}{2}\right\}.$$

Dokážte, že D má $\frac{p-1}{2} \cdot \frac{q-1}{2}$ prvkov.

Úloha 225. Nech D je množina z úlohy 224. Označme

$$D_1 = \{[qj,\, pk] \in D;\ q \cdot j < p \cdot k\}$$

Dokážte, že D_1 má

$$\sum_{k=1}^{p_1} \left[\frac{p \cdot k}{q}\right]$$

prvkov.

Úloha 226. Označme

$$D_2 = \{[qj,\, pk] \in D;\ p \cdot k < q \cdot j\}.$$

Dokážte, že množina D_2 má

$$\sum_{j=1}^{q_1} \left[\frac{q \cdot j}{p}\right]$$

prvkov.

Úloha 227. Pomocou úloh 223, 224, 225 a 226 dokážte vetu 13.

Veta 13 je pomenovaná po svojom autorovi. Karl Fridrich Gauss patril k velikánom svojej doby, podobne ako Euler, Fermat a Lagrange. Zaoberal sa taktiež fyzikou a na podnet pruského kráľa aj geodéziou. Ten ho poveril vytvorením do tej doby najpresnejšej mapy svojho územia. Práce, ktoré popri tom K. Gauss vykonával, ho priviedli na základné myšlienky z diferenciálnej geometrie.

Úloha D. Číslo a^2-3, $a \in \mathbb{N}$ môže obsahovať v kanonickom rozklade iba číslo 2 a prvočísla tvaru $12k+1$ a $12k+11$. Dokážte.

(Návod: Použite postup z úlohy A a úlohu 221.)

Úloha E. Aké prvočísla môže obsahovať vo svojom kanonickom rozklade číslo a^2+3, kde $a \in \mathbb{N}$?

Aby sme mohli Legendrov symbol vypočítať pre väčšie prvočíslo, je výhodné rozšíriť jeho definíciu pre zložené moduly. Ak $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ je nepárne číslo a $a \in \mathbb{N}$, potom hodnotu

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \cdots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}$$

nazývame *Jacobiho symbol*. Jeho výpočet nám umožňujú niektoré vlastnosti analogické s Lagrangeovým symbolom. Ich dôkaz je predmetom nasledujúcich úloh, ktoré sú pre svoju jednoduchosť uvedené bez súvislého textu.

Úloha F. Dokážte:
a) $(\frac{a_1}{m}) = (\frac{a_2}{m})$ keď $a_1 \equiv a_2 \pmod{m}$,
b) $(\frac{a_1 a_2}{m}) = (\frac{a_1}{m})(\frac{a_2}{m})$,
c) $(\frac{a}{m_1 m_2}) = (\frac{a}{m_1})(\frac{a}{m_2})$.

Úloha G. Nech r a s sú nepárne celé čísla. Dokážte:
a) $\frac{(rs-1)}{2} \equiv \frac{(r-1)}{2} + \frac{(s-1)}{2} \pmod 2$,
b) $\frac{(r^2s^2-1)}{8} \equiv \frac{(r^2-1)}{8} + \frac{(s^2-1)}{8} \pmod 2$.

(Návod: V dôkaze časti a) využite, že $(r-1)(s-1) \equiv 0 \pmod 4$ a $rs-1 \equiv (r-1)+(s-1) \pmod 4$. V dôkaze časti b) využite, že $(r^2-1)(s^2-1) \equiv 0 \pmod{16}$ a $r^2s^2-1 \equiv (r^2-1)+(s^2-1) \pmod{16}$.)

Úloha H. Dokážte:
a) $\sum_{i=1}^{l} \frac{(r_i-1)}{2} \equiv \frac{(r_1 \cdots r_l-1)}{2} \pmod 2$,
b) $\sum_{i=1}^{l} \frac{(r_i^2-1)}{8} \equiv \frac{(r_1^2 \cdots r_l^2-1)}{8} \pmod 2$.

(Návod: Použite úlohu B a postupujte matematickou indukciou.)

Úloha CH. Dokážte:
a) $(\frac{-1}{m}) = (-1)^{\frac{(m-1)}{2}}$,
b) $(\frac{2}{m}) = (-1)^{\frac{(m^2-1)}{8}}$,
c) $(\frac{m}{n}) \cdot (\frac{n}{m}) = (-1)^{\frac{(m-1)}{2} \cdot \frac{(n-1)}{2}}$.

(Návod: Použite úlohu C a úlohu 211.)

Časť *c* z predchádzajúcej úlohy sa nazýva *zákon reciprocity pre Jacobiho symbol*. Tento nám umožňuje vlastný výpočet Legendrovho symbolu.

Poznámka. Ak m je zložené číslo, potom rovnosť $(\frac{a}{m}) = 1$ nezaručuje riešiteľnosť kongruencie $x^2 \equiv a \pmod{m}$. Napríklad ak $m = 15 = 3 \cdot 5$, $(\frac{2}{3}) = -1$, $(\frac{2}{5}) = -1$, ale $(\frac{2}{15}) = 1$.