11. PRIMITÍVNE KORENE

Z Eulerovej vety vieme, že pre $m \in \mathbb{N}$ a $a \in \mathbb{N}$, $(a, m) = 1$ existuje také číslo k , že

$$a^k \equiv 1 \pmod{m}.$$

Označme pre $(a, m) = 1$

$$\mathrm{rad_m}\, a = \min\{k = 1, 2, \ldots, a^k \equiv 1 \pmod{m}\}.$$

Hodnotu $\mathrm{rad_m}\, a$ nazývame *rád čísla a modulo m.*

Úloha 228. Nech $a, m \in \mathbb{N}$ a $(a, m) = 1$. Ak

$$a^k \equiv 1 \pmod{m},$$

potom $\mathrm{rad_m}\, a \,|\, k$. Dokážte.

(Návod: Vyjadrite $k = q \cdot \mathrm{rad_m}\, a + r,\ 0 \leq r < \mathrm{rad_m}\, a$.)

Možnosti použitia pojmu rád čísla modulo m si ukážeme na dôkazoch nasledujúcich tvrdení.

Tvrdenie 1. Nech p_1, p_2 sú rôzne prvočísla. Potom $(2^{p_1} - 1, 2^{p_2} - 1) = 1$.

Ako obvykle, dôkaz nájdete v nasledujúcich úlohách.

Úloha A. Nech p je prvočíslo a $p|(2^{p_1} - 1, 2^{p_2} - 1)$. Potom $2^{p_1} \equiv 1 \pmod{p}$, $2^{p_2} \equiv 1 \pmod{p}$.

Nech p je prvočíslo z úlohy A a $r = rad_p 2$.

Úloha B. Použitím úlohy 228 dokážte, že $p_1 = r = p_2$.

Tvrdenie 2. Nech $p_1, p_2 \geq 3$ sú rôzne prvočísla. Potom $(2^{p_1} + 1, 2^{p_2} + 1) = 3$.

Úloha C. Nech $p > 3$ je prvočíslo. Potom
a) $3|2^p + 1$,
b) $9 \not| 2^p + 1$.

(Návod: Na dôkaz časti a) použite kongruenciu $2 \equiv -1 \pmod{3}$ a na dôkaz časti b) použite rovnosť $rad_9 2 = 6$.)

Úloha D. Nech $p|(2^{p_1} + 1, 2^{p_2} + 1)$. Potom $2^{2p_1} \equiv 1 \pmod{p}$, $2^{2p_2} \equiv 1 \pmod{p}$.

Úloha E. Nech p je prvočíslo z úlohy D. Označme $r = rad_p 2$. Použitím úlohy 228 a úlohy D dokážte, že $r = 2$.

Úloha F. Dokážte tvrdenie 2.

Úloha G. Dokážte, že pre rôzne prvočísla p_1, p_2 platí $(3^{p_1}-1, 3^{p_2}-1) = 2$.

Úloha H. Dokážte, že pre rôzne prvočísla p_1, p_2 platí $(3^{p_1}+1, 3^{p_2}+1) = 4$.

(Návod: To, že $3^p + 1$ nie je deliteľné ôsmimi, dokážte pomocou binomickej vety.)

Poznamenajme, že postupom z úloh A až H môžeme dokázať nasledujúcu všeobecnejšiu vlastnosť:

Pre nepárne čísla r, s platí: $(q^s+1, q^r+1) = q^{(r,s)}+1$, $(q^s-1, q^r-1) = q^{(r,s)}-1$ pre ľubovoľné q.

Úloha 229. Pre každé k a prvočíslo p existuje najviac k primitívnych riešení kongruencie

$$x^k \equiv 1 \pmod{p}.$$

Dokážte.

(Návod: Tvrdenie je dôsledkom Lagrangeovej vety.)

Číslo a budeme nazývať *primitívnym koreňom modulo* m, ak $\mathrm{rad_m}\, a = \varphi(m)$ alebo

$$\{a^\circ \bmod \mathrm{m},\ a \bmod \mathrm{m}, \ldots, a^{\varphi(m)-1} \bmod \mathrm{m}\} = R_m.$$

V tomto prípade taktiež hovoríme, že prvok a *generuje* redukovaný zvyškový systém modulo m.

Ďalej sa budeme zaoberať existenciou primitívnych koreňov. Ukážeme si, kedy existujú a kedy neexistujú.

Najskôr dokážeme nasledujúcu vetu.

Veta 14. Pre každé prvočíslo p existuje primitívny koreň modulo p.

Na to, aby sme dokázali vetu 14, použijeme nasledujúce tvrdenie.

Lema 1. Nech $m \in \mathbb{N}$ a $(a, m) = 1 = (b, m)$. Ak $(\mathrm{rad_m}\, a, \mathrm{rad_m}\, b) = 1$, potom

$$\mathrm{rad_m}\, a \cdot b = \mathrm{rad_m}\, a \cdot \mathrm{rad_m}\, b.$$

Úloha 230. Dokážte, že

$$\mathrm{rad_m}\, a \cdot b \mid \mathrm{rad_m}\, a \cdot \mathrm{rad_m}\, b$$

pre $a, b, m \in \mathbb{N}$ a $(a, m) = 1 = (b, m)$.

(Návod: Použite úlohu 228.)

Úloha 231. Nech platia predpoklady lemy 1. Označme

$$r = \mathrm{rad_m}(a \cdot b).$$

Dokážte, že

$$a^r \equiv b^{\varphi(m)-r} \pmod{m}.$$

(Návod: Vieme, že $a^r \cdot b^r \equiv 1 \pmod{m}$. Použite Eulerovu vetu.)

Úloha 232. Nech platia predpoklady lemy 1. Dokážte, že pre $r = \mathrm{rad_m}(a \cdot b)$ platí

$$a^{r \cdot \mathrm{rad_m}\, b} \equiv 1 \pmod{m}\,.$$

(Návod: Použite úlohu 230.)

Úloha 233. Dokážte, že ak platia predpoklady lemy 1, potom $\mathrm{rad_m}\, a \mid \mathrm{rad_m}(a \cdot b)$.

(Návod: Použite úlohu 5 a úlohu 1.)

Úloha 234. Nech platia predpoklady lemy 1. Dokážte, že $\mathrm{rad_m}\, b \mid \mathrm{rad_m}\, a \cdot b$.

Úloha 235. Dokážte lemu 1.

Teraz budeme dokazovať vetu 14. Je logické očakávať, že primitívnym koreňom modulo p bude prvok s najväčším rádom modulo p.

Úloha 236. Nech $a, b \in \mathbb{N}$ a nech $a \not| b$. Potom existuje prvočíslo q a číslo $\alpha \geq 1$ také, že $q^\alpha || a$ a $q^\alpha \not| b$. Dokážte.

(Návod: Uvažujte kanonické rozklady čísel a, b.)

Úloha 237. Nech p je prvočíslo a $(a, p) = 1$. Nech $q^\alpha \| \mathrm{rad_p}\, a$. Označme $r = \mathrm{rad_p}\, a$. Dokážte, že

$$\mathrm{rad_p}\, a^{\frac{r^p}{q^\alpha}} = q^\alpha\,.$$

(Návod: Použite úlohu 228.)

Úloha 238. Nech p je prvočíslo, $(a, p) = 1$ a $(b, p) = 1$. Nech $r_1 = \mathrm{rad_p}\, a$, $r_2 = \mathrm{rad_p}\, b$. Nech $r_1 \neq r_2$. Nech q je také prvočíslo, že $q^\alpha \| r_1$ a $q^\alpha \not| r_2$. Dokážte, že
a) $\mathrm{rad}\, b^{(q^\alpha, r_2)} = \frac{r_2}{(q^\alpha, r_2)}$,
b) $(\mathrm{rad}\, a^{\frac{r_1}{q^\alpha}}, \mathrm{rad}\, b^{(q^\alpha, r_2)}) = 1$,
c) $\mathrm{rad}(a^{\frac{r_1}{q^\alpha}} \cdot b^{(q^\alpha, r_2)}) = q^\alpha \cdot \frac{r_2}{(q^\alpha, r_2)} > r_2$.

(Návod: Použite lemu 1 a úlohu 235.)

Úloha 239. Nech p je prvočíslo a b je také číslo, že

$$\mathrm{rad_p}\, b = \max\{\mathrm{rad_p}\, a;\, a = 1, 2, \dots\}\,.$$

Dokážte, že pre každé a, ktoré je nesúdeliteľné s p, platí

$$\mathrm{rad_p}\, a \mid \mathrm{rad_p}\, b\,.$$

(Návod: Použite úlohu 238.)

Prvok b budeme nazývať *prvkom s maximálnym rádom modulo p.*

Úloha 240. Nech b je prvok s maximálnym rádom modulo p a $r = \mathrm{rad_p}\, b$. Potom každý prvok $a \in \{1, \ldots, p-1\}$ je koreňom kongruencie

$$x^r \equiv 1 \pmod{p}.$$

Dokážte.

(Návod: Použite úlohu 239.)

Úloha 241. Nech p je prvočíslo a b je prvok s maximálnym rádom modulo p. Dokážte:

a) $1, b, \ldots, b^{r-1}$ sú riešením kongruencie

$$x^r \equiv 1 \pmod{p}.$$

b) Pre $0 \leq j \leq k \leq r-1$ platí: Ak

$$b^j \equiv b^k \pmod{p},$$

potom $j = k$.

c) Dokážte, že prvok s maximálnym rádom modulo p je primitívnym koreňom modulo p.

(Návod: Vynásobte kongruenciu b^{r-k} a pri dôkaze časti c) použite úlohy 238, 239 a 227.)

Cvičenie 1. Nech p je nepárne prvočíslo a g je primitívny koreň modulo p. Dokážte, že g^s je primitívny koreň modulo p vtedy a len vtedy keď $(s, p-1) = 1$.

Cvičenie 2. Nech p je nepárne prvočíslo a $a \in \mathbb{Z}, (a,p) = 1$ a $a \equiv g^k \pmod{p}$, kde g je primitívny koreň modulo p. Dokážte, že $\left(\frac{a}{p}\right) = (-1)^k$.

Cvičenie 3. Nech p je nepárne prvočíslo. Dokážte, že v $\mathbb{R}_p$ existuje práve $\frac{p-1}{2}$ kvadratických zvyškov.

– – – – – – – – – – – –

Existencia primitívnych koreňov modulo p - nepárne prvočíslo, nám umožní urobiť jednoduchší dôkaz Gaussovho kvadratického zákona reciprocity. Uvedieme trochu modifikovaný dôkaz z článku [SZ1]. *Budeme používať jednoduché vlastnosti permutácií.*

Nech $(a,p) = 1$, číslu a môžeme priradiť permutáciu

$$\lambda_a : \mathbb{R}_p \to \mathbb{R}_p,\ \lambda_a(x) = ax \mod p,\ x \in \mathbb{R}_p.$$

Ak g je primitívny koreň modulo p ľahko vidíme, že λ_g je cyklická permutácia $(1, g, ..., g^{p-2})$. Preto platí $sgn\lambda_g = -1$. Je zrejmé, že $a \equiv b \pmod{p}$ tak $\lambda_a = \lambda_b$ a

pre ľubovoľné c, d platí $\lambda_{cd} = \lambda_c \lambda_d$. Preto pre $a \equiv g^k \pmod{p}$ platí $sgn\lambda_a = (-1)^k$ a teda podľa cvičenia 2 dostávame

$$\left(\frac{a}{p}\right) = sgn\lambda_a. \qquad (*)$$

Teraz môžeme vysloviť Gaussovu lemu, ale v inej podobe:
Nech μ je počet takých $j \leq \frac{p-1}{2}$ pre, ktoré $aj \mod p > \frac{p-1}{2}$. Potom

$$\left(\frac{a}{p}\right) = (-1)^\mu. \qquad (**)$$

Dôkaz. *Použijeme $(*)$. Znamienko permutácie λ_a je rovnaké ako znamienko súčinu $\prod_{i<j}(aj \mod p - ai \mod p)$. Pre $i < j \leq \frac{p-1}{2}$ sa činiteľ $aj \mod p - ai \mod p$ rovná činiteľu $a(n-i) \mod p - a(n-j) \mod p$ preto v súčine dajú kladnú hodnotu. Uvedený súčin bude mať preto rovnaké znamienko ako súčin*
$\prod_{i \leq \frac{p-1}{2} < j}(aj \mod p - ai \mod p) = \prod_{i,k \leq \frac{p-1}{2}}(a(p-k) \mod p - ai \mod p) =$
$\prod_{i,k \leq \frac{p-1}{2}}(p - ak \mod p - ai \mod p)$. *Tento súčin znova obsahuje rovnaké činitele pre $u < v, i = u, k = v$ a $i = v, k = u$. Teda bude mať rovnaké znamienko ako $\prod_{i \leq \frac{p-1}{2}}(p - 2ai \mod p)$. Je zrejmé že znamienko posledného súčinu je $(-1)^\mu$.* □

Podľa Úlohy 216 hneď vidíme, že hodnota μ z predošlého tvrdenia má rovnakú paritu ako $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{2ai}{p}\right]$ a teda dostávame pôvodnú verziu Gaussovej lemy a podľa identít z úloh 222, 224, 225, 226 dostávame Gaussov kvadratický zákon reciprocity.

– – – – – – – – – – – –

Dokázali sme, že primitívny koreň modulo m existuje v prípade, keď $m = p$ je prvočíslo. Teraz dokážeme, že existuje aj v prípadoch, keď $m = p^\alpha$, $m = 2p^\alpha$, kde p je nepárne prvočíslo a $\alpha \geq 1$.

Úloha 242. Nech $x, m, n \in \mathbb{N}$ a $(x, m) = 1 = (x, n)$. Ak $m|n$, potom $rad_m x | rad_n x$. Dokážte.

(Návod: Použite úlohu 228.)

Úloha 243. Nech $x \in \mathbb{N}$ a p je prvočíslo. Ak pre $\alpha > 1$ platí

$$x^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha},$$

potom

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

Dokážte.

(Návod: Vieme, že $x^{p-1} = 1 + kp$ podľa úlohy 126. Dosaďte do vzťahu (14).)

Úloha 244. Dokážte, že existuje primitívny koreň x modulo p, kde p je nepárne prvočíslo, taký, že

$$x^{p-1} \not\equiv 1 \pmod{p^2}. \tag{15}$$

(Návod: Uvedomte si, že ak x nespĺňa vzťah (15), potom $x+p$ spĺňa vzťah (15).)

Teraz dokážeme, že $x \in \mathbb{N}$, ktoré vyhovuje vzťahu (15), je primitívnym koreňom modulo p^α. V nasledujúcej časti predpokladáme, že p je nepárne prvočíslo, $\alpha > 1$ a $q = p^\alpha$.

Úloha 245. Ak x je primitívny koreň modulo p, potom $p-1|rad_q x$. Dokážte.

(Návod: Použite úlohu 242.)

Úloha 246. Ak x je primitívny koreň modulo p, potom

$$rad_q x = (p-1)p^\beta,$$

kde $0 \leq \beta \leq \alpha$. Dokážte.

(Návod: Použite úlohu 245, Eulerovu vetu, úlohu 228 a $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.)

Úloha 247. Ak x je primitívny koreň modulo p, ktorý vyhovuje vzťahu (15), potom

$$rad_q x = \varphi(p^\alpha).$$

Dokážte.

(Návod: Použite úlohy 243 a 246.)

Úloha 248. Dokážte, že ak p je nepárne prvočíslo, potom existuje primitívny koreň modulo p^α.

Ďalej budeme riešiť prípad primitívneho koreňa modulo $2p^\alpha$ pre nepárne prvočíslo p.

Úloha 249. Dokážte, že ak p je nepárne prvočíslo, potom $\varphi(2p^\alpha) = \varphi(p^\alpha)$.

(Návod: Použite multiplikatívnosť funkcie φ.)

Úloha 250. Dokážte, že ak p je nepárne prvočíslo, potom existuje nepárny primitívny koreň modulo p^α.

(Návod: Ak x je primitívny koreň modulo p^α, potom aj $x+p^\alpha$ je primitívny koreň modulo p^α.)

Úloha 251. Dokážte, že ak p je nepárne prvočíslo, potom existuje primitívny koreň modulo $2p^\alpha$.

(Návod: Použite úlohu 250.)

Veta 15. Primitívny koreň modulo m existuje práve vtedy, keď $m \in \{2, 4, p^\alpha, 2p^\alpha;\ p$ je nepárne prvočíslo$\}$.

Dôkaz existencie primitívnych koreňov v uvedených prípadoch je už urobený v predchádzajúcich úlohách. Zostáva nám teda dokázať, že v inom prípade primitívny koreň neexistuje. To nám vyplynie z nasledujúcej vety.

Veta 16. Ak $m \notin \{2, 4, p^\alpha, 2p^\alpha, p-$**nepárne prvočíslo**$\}$**, potom pre** $x \in \mathbb{N}$**,** $(x, m) = 1$ **platí**

$$x^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}. \tag{17}$$

Dôkaz nájdete v nasledujúcich úlohách.

Úloha 252. Ak $m \in \mathbb{N}$ a $m > 2$, potom $2|\varphi(m)$. Dokážte.

Úloha 253. Nech $m \notin \{2, 4, p^\alpha, 2p^\alpha, p -$ nepárne prvočíslo$\}$. Potom m je možné vyjadriť v tvare

$$m = m_1 m_2, \tag{18}$$

kde m_1, m_2 sú nepárne čísla, $m_1, m_2 > 1$ a $(m_1, m_2) = 1$ alebo

$$m = 2^\alpha m_1, \tag{19}$$

kde $2 \nmid m_1$ a $\alpha > 2$. Dokážte.

Úloha 254. Nech m má tvar (18). Potom $\varphi(m_1)|\frac{\varphi(m)}{2}$ a $\varphi(m_2)|\frac{\varphi(m)}{2}$. Dokážte.

Úloha 255. Nech m má tvar (18). Potom

$$x^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_1}$$

a

$$x^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_2}.$$

Dokážte.

Úloha 256. Dokážte platnosť kongruencie (17), ak m má tvar (18).

Zostáva nám dokázať platnosť kongruencie (17) pre čísla tvaru (19).

Úloha 257. Nech $x \in \mathbb{N}$ a $2 \not| x$. Potom

$$x^2 \equiv 1 \pmod 8.$$

Dokážte.

(Návod: Uvažujte $x = 2k + 1$ a $x^2 = 4k(k + 1) + 1$.)

Úloha 258. Dokážte, že pre $\alpha > 2$ platí

$$x^{\frac{\varphi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}.$$

(Návod: Postupujte matematickou indukciou podľa úlohy 257. Uvedomte si, že $\varphi(2^\alpha) = 2^{\alpha-1}$.)

Úloha 259. Dokážte platnosť kongruencie (17), ak m má tvar (19).

Na záver tejto kapitoly si pomocou pojmu rád a úlohy 228 ukážeme špeciálny prípad už spomínanej Dirichletovej vety.

Tvrdenie 1. Nech p je prvočíslo. Potom existuje nekonečne veľa prvočísel tvaru $kp + 1$.

Dôkaz bude analogický, ako bol Euklidov dôkaz nekonečnosti množiny prvočísel. Využijeme pri ňom nasledujúce tvrdenie.

Tvrdenie 2. Nech $a \in \mathbb{N}$ a p je také prvočíslo, že $(a - 1, p) = 1$. Potom existuje prvočíslo q také, že $(a, q) = 1$ a $q = kp + 1$.

Dôkaz nájdeme v nasledujúcich úlohách.

Úloha CH. Dokážte, že ak q je prvočíslo a $q|a^p - 1$, potom $a^p \equiv 1 \pmod q$ a $(a, q) = 1$.

Úloha J. Nech a, p spĺňajú predpoklady tvrdenia 2. Potom $(a - 1, \frac{a^p-1}{a-1}) = 1$. Dokážte.

Úloha K. Nech q je prvočíslo a $q|\frac{a^p-1}{a-1}$. Potom $a \not\equiv 1 \pmod q$ a $rad_q a = p$. Dokážte.

Úloha L. Nech q je prvočíslo z úlohy K. Potom $q = kp + 1$. Dokážte.

(Návod: Použite úlohu 228 a malú Fermatovu vetu.)

Úlohou L sme dokázali Tvrdenie 1. Tvrdenie 2 vyplýva z nasledujúcej úlohy.

Úloha M. Nech $p_1, ..., p_r$ sú prvočísla tvaru $kp + 1$. Potom $a = p \cdot p_1 \cdot ... \cdot p_r$ spĺňa podmienky tvrdenia 1. Dokážte.