Rády a primitívne prvky

Denys Andrukhovskyi
denys.andrukhovskyi@trojsten.sk

1 Úvod

Pri štúdiu teórie čísel my často sa stretávame s modulárnou aritmetikou. A už máme nejakú predstavu o vlastnostiach zvyškov, napr. čosi o správaní sa zvyškov nám hovorí Malá Fermatova veta a Eulerova veta, čínska veta o zvyškoch atď. Dnes však sa dozvieme viac o vlastnostiach zvyškov. A na to budeme využívať *rády a primitívne prvky.*

Začneme ale z toho, že spomenieme si, ako znie Malá Fermatova veta a jej všeobecná verzia – Eulerova veta. Klasický dôkaz využije veľmi užitočnú vlastnosť zvyškových tried. Konkrétne, pre prvočísla rovnica $ax \equiv y \pmod{p}$ má práve jedno riešenie na množine $\{1, 2, \ldots, p-1\}$ pre každé y z tej istej množiny. Inými slovami, funkcia $f : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$ s predpisom $f(x) = ax \pmod{p}$ nadobúda každú hodnotu práve raz.

Veta 1 (Malá Fermatova veta)**.** *Pre ľubovoľné prvočíslo p a celé číslo a platí:*

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

Dôkaz. Prípad $p \mid a$ je triviálny. Pre ostatne prípady stačí ukázať, že funkcia $f : \{1, ..., p-1\} \to \{1, ..., p-1\}$ s predpisom $f(x) \equiv ax \pmod{p}$ nadobúda každú hodnotu práve raz. Naozaj, nech

$$ai \equiv aj \pmod{p}.$$

Teda $a(i-j) \equiv 0 \pmod{p}$. Ale $p \nmid a$, teda $p \mid (i-j)$. Odtiaľto dostávame $i = j$. Takže, f nadobúda každú hodnotu nanajvýš raz, a teda musí nadobudnúť každú hodnotu práve raz. Potom naozaj f je permutáciou na množine $\{1, ..., p-1\}$, a preto:

$$\begin{array}{ccccccccc} f(1) & \cdot & f(2) & \cdot & \ldots & \cdot & f(p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) & \pmod{p} \\ (a \cdot 1) & \cdot & (a \cdot 2) & \cdot & \ldots & \cdot & (a \cdot (p-1)) \equiv (p-1)! & \pmod{p} \end{array}$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$
$$a^{p-1} \equiv 1 \pmod{p}$$

□

Analogicky vieme dokázať aj zovšeobecnenú vetu, kde namiesto prvočísla p máme všeobecne celé číslo n, a namiesto množiny $\{1, 2, \ldots, p-1\}$ máme množinu všetkých kladných čísel, čo sú nesúdeliteľné s n a sú menšie ako n (aby platil argument, že z $ai \equiv aj \pmod{n}$ vyplýva $i \equiv j$, musí platiť[1] $\gcd(a, n) = 1$).

[1] gcd je „greatest common divisor“, t.j. najväčší spoločný násobok.

Veta 2 (Eulerova veta)**.** *Nech a a n sú nesúdeliteľné čísla. Potom platí*

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

kde $\varphi(n)$ je počet kladných celých čísel, menších n a nesúdeliteľných s n.

Dajme si malú rozcvičku.

Cvičenie 1 (Leningradské matematické krúžky, 10.095)**.** Dokážte, že pre rôzne prvočísla p, q platí $p^q + q^p \equiv p + q \pmod{pq}$. **Hinty**: 1

Cvičenie 2 (IMO 2005, 4)**.** Nájdite všetky prirodzené čísla, ktoré sú nesúdeliteľné so všetkými členami postupnosti $a_n = 2^n + 3^n + 6^n - 1$. **Hinty**: 2

2 Nachádzame korene

Dobre, vieme, že pre $n = p$ a $k = p-1$ (resp. $k = \varphi(n)$ vo všeobecnosti) platí $a^k \equiv 1 \pmod{n}$. Môžeme ale sa spýtať prirodzenú otázku: či vždy $k = p-1$ (resp. $k = \varphi(n)$) bude najmenším číslom takým, že $a^k \equiv 1 \pmod{n}$?

Odpoveď je, že nie je vždy. Okrem triviálneho príkladu pre všetky kladné celé čísla n: $1^1 \equiv 1 \pmod{n}$, vieme odskúšať aj niečo zaujímavejšie, napríklad:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{7} \\ 2^2 &\equiv 4 \pmod{7} \\ 2^3 &\equiv 8 \equiv 1 \pmod{7} \end{aligned}$$

Takže, najmenším takým číslom k, aby $2^k \equiv 1 \pmod{7}$ je $k = 3$. Tato situácia motivuje nás zaviesť definíciu:

Definícia 1. Rádom prvku a modulo n voláme najmenšie kladné celé číslo k také, že $a^k \equiv 1 \pmod{n}$, a značíme ho $k = \mathrm{ord}_n(a)$.

Značenie $\mathrm{ord}_n(a)$ pochádza z anglického *„order“*.
Vrátime sa ale k našej otázke. Keď namiesto 2 skúsime 3, tak máme:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{7} \\ 3^2 &\equiv 2 \pmod{7} \\ 3^3 &\equiv 6 \pmod{7} \\ 3^4 &\equiv 4 \pmod{7} \\ 3^5 &\equiv 5 \pmod{7} \\ 3^6 &\equiv 1 \pmod{7} \end{aligned}$$

Takže, mocniny 3 modulo 7 dávajú *všetky možne zvyšky*, a $\mathrm{ord}_7(3) = 6$, čo je *najväčším možným rádom* (lebo podľa vety 1 $a^6 \equiv 1 \pmod{7}$ pre všetky nesúdeliteľné so 7 čísla a). Toto nás priviedlo k definícii primitívneho prvku.

Definícia 2. Primitívnym prvkom (alebo primitívnym koreňom) modulo n voláme také číslo g, že pre všetky nesúdeliteľné s n čísla a existuje celé číslo k, že $g^k \equiv a \pmod{n}$.

Analogicky, dá sa povedať, že všetky mocniny primitívneho koreňa „vygenerujú“ všetky zvyšky modulo n.

Teraz ale zamyslime sa nad vlastnosťami primitívnych koreňov. Začneme tým, že vidíme, že ak g je primitívny koreň, tak $\mathrm{ord}_p(g)$ je najväčší možný, lebo inak by nám mocniny g sa skončili skôr, a tým pádom by sme nevygenerovali všetky možné zvyšky. Platí ale opačná implikácia? Objaví sa, že áno, ale na dôkaz tohto (aj ďalších) tvrdení budeme využívať nasledujúcu lemu.

Lema 3. *Pre kladné celé a, m, n platí $a^m \equiv 1 \pmod n$ práve vtedy keď platí $\mathrm{ord}_n(a) \mid m$.*

Dôkaz. $\implies$ Sporom. Nech $k = \mathrm{ord}_n(a)$, $k \nmid m$. Nech teda $m = kt + r$, $0 < r < k$. Teda: $a^k \equiv 1 \pmod p$ a $a^m \equiv 1 \pmod p$. Teda:

$$1 \equiv a^m \equiv a^{kt+r} \equiv a^{kt} \cdot a^r \equiv (a^k)^t \cdot a^r \equiv 1^t \cdot a^r \equiv a^r \pmod n$$

T.j. $a^r \equiv 1 \pmod n$ a zároveň $r < k = \mathrm{ord}_n(a)$, čo je spor s definíciou rádu.

$\impliedby$ Priamo. Nech $m = k\,\mathrm{ord}_n(a)$, $k \in \mathbb{N}$, potom $a^m = a^{k\,\mathrm{ord}_n(a)} \equiv 1^k \equiv 1 \pmod n$. □

Dôsledok 3.1. *Pre prvočíslo p máme $\mathrm{ord}_p(a) \mid p-1$. Navyše, pre celé n platí $\mathrm{ord}_n(a) \mid \varphi(n)$.*

Dôkaz. Aplikujeme vetu 1, resp. vetu 2 na lemu 3. □

Dôsledok 3.2. *Pre kladné celé r, s také, že $a^r \equiv 1 \pmod n$ a $a^s \equiv 1 \pmod n$ platí $a^{\gcd(r,s)} \equiv 1 \pmod n$.*

Dôkaz. Podľa lemy 3 platí $\mathrm{ord}_n(a) \mid r$ a $\mathrm{ord}_n(a) \mid s$, čo implikuje $\mathrm{ord}_n(a) \mid \gcd(r, s)$, takže podľa lemy 3 platí $a^{\gcd(r,s)} \equiv 1 \pmod n$. □

Teraz už môžeme dokázať nasledujúcu vetu.

Veta 4. *Číslo a nesúdeliteľne s n má najväčší možný rád modulo n (t.j. $\varphi(n)$) práve vtedy, keď a je primitívny koreň modulo n.*

Dôkaz. Dokážeme 2 implikácie.

Implikácia „a je primitívny koreň $\implies$ $\mathrm{ord}_n(a) = \varphi(n)$“ sa dokazuje pomerne triviálne. Naozaj, ak by platilo $\mathrm{ord}_n(a) < \varphi(n)$, tak počet prvkov v množine $\{a^i \pmod n \mid i \in \mathbb{N}\}$ by bol ostro menší ako $\varphi(n)$. Platí to, keďže pre $i = \mathrm{ord}_n(a)k + b$ platí

$$a^i \equiv a^{\mathrm{ord}_n(a)k+b} \equiv a^{\mathrm{ord}_n(a)k} a^b \equiv 1^k a^b = a^b \pmod n;$$

takže stačí uvažovať len také b: $0 \leq b < \mathrm{ord}_n(a) < \varphi(n)$. To znamená, že a negeneroval by všetky prvky.

Implikáciu „a je primitívny koreň $\impliedby$ $\mathrm{ord}_n(a) = \varphi(n)$“ dokážeme sporom. Nech $\mathrm{ord}_n(a) = \varphi(n)$, a zároveň a nie je primitívny koreň. Tým pádom nevygeneruje všetky zvyšky, tým pádom niektorý by sa mal zopakovať podľa Dirichletoveho princípu. T.j. existuje dvojica rôznych čísel $i, j \in \{1, 2, ..., \varphi(n)\}$ takých, že $a^i \equiv a^j \pmod n$.

BUNV predpokladajme, že $i < j$. Teda $a^i(a^{j-i} - 1) \equiv 0 \pmod n$. $\gcd(a, n) = 1 \implies \gcd(a^i, n) = 1 \implies a^{j-i} - 1 \equiv 0 \pmod n$. Teda

$$a^{j-i} \equiv 1 \pmod n$$

Z lemy 3 vieme, že $\varphi(n) \mid (j - i)$. Na inej strane, $0 < j - i < \varphi(n)$, čo je spor. □

Teraz, keď už môžeme niečo povedať o vlastnostiach primitívnych koreňov, bolo by dobre si všimnúť, že ale nemáme dokázané, že existujú. A keď skúsime overiť, či existujú pre modulo 8, tak nenájdeme také prvky: $\mathrm{ord}_8(1) = 1, \mathrm{ord}_8(3) = \mathrm{ord}_8(5) = \mathrm{ord}_8(7) = 2$.

Takže, nie pre každé modulo existuje koreň. Intuícia ale hovorí, že aspoň pre prvočísla primitívne prvky by mohli existovať. Odpoveď na to dáva nasledujúca veta.

Veta 5. *Pre prvočíslo p a každé $d \mid (p-1)$ existuje práve $\varphi(d)$ prvkov v množine $\{1, 2, ..., p-1\}$, ktoré majú rád d.*

Dôkaz. Hlavnou myšlienkou dôkazu je ukázať, že počet prvkov, ktoré majú rád d, je nulový alebo rovná sa $\varphi(d)$; a potom ukázať, že nulový prípad nie je možný.

Nech $\psi(d)$ je počet prvkov, ktoré majú rád d. Ukážeme, že ak prvok rádu d existuje, tak $\psi(d) = \varphi(d)$. Nech a je taký prvok, že $\mathrm{ord}_p(a) = d$. Teda rovnica

$$a^d \equiv 1 \pmod{p}$$

má riešenia[2] $a, a^2, ..., a^d$. A podľa Langrangovej vety[3], taký polynóm stupňa d má nanajvýš d riešení v množine $\{1, 2, ..., p\}$, takže to sú všetky riešenia.

Teraz ukážeme, že naozaj len tie a^i budu mať rád d, pre ktoré platí $\gcd(i, d) = 1$.

Nech $\gcd(i, d) = 1$, a prvok a^i má rád d'. Teda $(a^i)^{d'} \equiv 1 \pmod{p}$. Ale teda $d \mid id'$, lebo $a^{(id')} \equiv 1 \pmod{p}$. $\gcd(i, d) = 1 \implies d \mid d' \implies d \leq d'$. Zároveň platí aj $d' \leq d$, lebo $(a^i)^d \equiv 1 \pmod{n}$ a d' je rád čísla a^i. Takže $d' = d$.

Na inej strane, ak $\gcd(i, d) > 1$, tak $(a^i)^{\frac{d}{\gcd(i,d)}} = (a^d)^{\frac{i}{\gcd(i,d)}} = a^{dk} \equiv 1 \pmod{p}$ pre nejaké celé k. Takže platí nerovnosť[4] $\mathrm{ord}_p(a^i) \leq \frac{d}{\gcd(i,d)} < \frac{d}{1} = d$.

Takže, ak prvok rádu d existuje, tak takých prvkov je práve toľko, koľko nesúdeliteľných čísel s d na intervale $[0, d)$. Podľa definície je to $\varphi(d)$. Ukázali sme teda, že $\psi(d) \neq 0 \implies \psi(d) = \varphi(d)$.

Každý rád je deliteľom $p-1$ podľa dôsledku 3.1, takže teraz pôjdeme zrátať počty prvkov v množine $\{1, 2, \ldots, p-1\}$.

$$p - 1 = \sum_{d|(p-1)} \psi(d) \leq \sum_{d|(p-1)} \varphi(d)$$

Teraz ukážeme, že $\sum_{d|(p-1)} \varphi(d) = p - 1$. Všimneme si, že

$$\sum_{d|p-1} \varphi(d) = \sum_{d|p-1} \varphi\left(\frac{p-1}{d}\right),$$

lebo každý deliteľ $d \mid n$ vieme vyjadriť aj ako $d = \frac{n}{\frac{n}{d}} = \frac{n}{d'}$, t.j. cez iný deliteľ $d' \mid n$. Taktiež platí

$$\sum_{d|p-1} \varphi\left(\frac{p-1}{d}\right) = p - 1,$$

lebo $\varphi\left(\frac{p-1}{d}\right)$ je počet čísel, ktoré majú NSD d s $p-1$ (teda sú nesúdeliteľné s $\frac{p-1}{d}$).

Takže, ak pre nejaké d platí $\psi(d) = 0$, tak potom:

$$p - 1 = \sum_{d|p-1} \psi(d) < \sum_{d|p-1} \varphi(d) = p - 1$$

čo je spor. Teda pre každé $d \mid p-1$ platí $\psi(d) = \varphi(d)$. □

Dôsledok 5.1. *Pre ľubovoľné nepárne prvočíslo p existuje primitívny koreň. Navyše, v množine $\{1, 2, ..., p-1\}$ existuje práve $\varphi(p-1)$ primitívnych koreňov.*

[2] všimnite si, že $a^{d+1} \equiv a \pmod{n}$, takže pre vyššie mocniny nedostaneme nové zvyšky; zároveň je jasne, že $(a^i)^d = (a^d)^i \equiv 1 \pmod{n}$ a navyše všetky tieto čísla majú rôzne zvyšky, čo sa dá ukázať podobným argumentom, ako v dôkaze vety 4.

[3] analog základnej vety algebry pre zvyškové triedy $\pmod{p}$ (tzv. pole $\mathbb{Z}/p\mathbb{Z}$)

[4] dá sa ukázať, že v prvej nerovnosti v skutočnosti vždy sa dosiahne rovnosť

Skúsime teraz zamyslieť sa, čo sa stane, keď n je zložené číslo. Vidíme, že napr. pre $n = 9$ $g = 2$ je primitívny prvok. Ale pre $n = 8$ alebo $n = 15$ neexistuje. Dokážeme nasledujúce 2 vety:

Veta 6. *Ak celé číslo $n = ab$, kde $a, b \geq 3$ sú nesúdeliteľné čísla, tak primitívny prvok modulo n neexistuje.*

Cvičenie 3. Dokážte predchádzajúcu vetu. **Hinty**: 3

Veta 7. *Ak celé číslo $n = 2^k$, kde $k \geq 3$, tak primitívny prvok modulo n neexistuje.*

Cvičenie 4. Dokážte predchádzajúcu vetu. **Hinty**: 4

Zistime, že všetky čísla, ktoré sa nedá zapísať ako $n = ab$, $\gcd(a, b) = 1$, $a, b \geq 3$ alebo $n = 2^k$, $k \geq 3$ sú $1, 2, 4, p^k, 2p^k$, kde p – nepárne prvočíslo. O vlastnostiach týchto čísel hovorí nasledujúca veta.

Veta 8. *Primitívne korene modulo n existujú práve vtedy, keď $n = 2, 4, p^k, 2p^k$, kde p – nepárne prvočíslo.*

Dôkaz. Dôkaz nie je krátky, takže ho zatiaľ nebudeme uvádzať. Ukážeme ale plán, podľa ktorého dôkaz funguje a ponúkneme dokazovanie jednotlivých častí ako cvičenie pre čitateľa:

1. Ošetrime prípady $n = 2, 4$.
2. Ukážeme, že pre $n = p^2$ existuje primitívny koreň.
3. Ukážeme, že ak pre p^2 existuje primitívny koreň, tak existuje aj pre p^k, kde $k \geq 3$.
4. Ukážeme, že ak pre p^k existuje koreň, tak aj pre $2p^k$ existuje koreň.

□

Cvičenie 5. Dokážte, že ak g je primitívny koreň modulo nepárne prvočíslo p, tak g alebo $g + p$ je primitívny koreň modulo p^2. **Hinty**: 5

Cvičenie 6. Dokážte, že ak g je primitívny koreň modulo nepárne číslo m, tak g alebo $g + m$ je primitívny koreň modulo $2m$. **Hinty**: 6

Môžeme dokázať ešte niekoľko zaujímavých vlastnosti.

Cvičenie 7. Nech g – primitívny koreň modulo $n > 2$. Dokážte, že $g^{\frac{\varphi(n)}{2}} \equiv -1 \pmod{n}$. **Hinty**: 7

Cvičenie 8. Dokážte, že súčin všetkých primitívnych koreňov modulo prvočíslo $p > 3$ je kongruentný $1 \pmod{p}$. **Hinty**: 8

Cvičenie 9. Dokážte, že pre primitívny koreň g modulo prvočíslo p číslo $(-g)$ je tiež primitívny koreň práve vtedy, keď $p = 4k + 1$. **Hinty**: 9

3 Riešime úlohy

Hlavnou myšlienkou aplikácii primitívnych koreňov v úlohách je využitie faktu, že primitívny koreň g generuje všetky zvyšky, takže vieme vyjadriť všetky zvyšky ako g^k, kde $0 \leq k < \varphi(n)$. Pri využitie všeobecných vedomostí o rádoch budeme vedieť sa odvolať napr. na lemu 3 alebo jej dôsledky.

Úloha 1 (Hungary-Israel Math Competition 2009)**.** Pre dane nepárne prvočíslo p nájdite všetky k také, že

$$p \mid 1^k + 2^k + ... + (p-1)^k$$

Riešenie. Začnem uvedomením toho, že pre p existuje primitívny prvok g. Takže kongruenciu

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

vieme vymeniť za

$$(g^{i_1})^k + (g^{i_2})^k + \cdots + (g^{i_{p-1}})^k \equiv 0 \pmod{p}$$

kde i_j je také číslo od 0 po $p-1$ pre ktoré platí $g^{i_j} \equiv j$.

Keďže pre rôzne j dostaneme rôzne i, tak $\{i_1, i_2, \ldots, i_{p-1}\} = \{1, 2, \ldots, p-1\}$, t.j. každá mocnina sa vyskytne práve raz. Takže preusporiadaním sčítancov:

$$(g^{i_1})^k + (g^{i_2})^k + \cdots + (g^{i_{p-1}})^k \equiv (g^1)^k + (g^2)^k + \cdots + (g^{p-1})^k \pmod{p}.$$

Ďalej by nebolo ťažké si všimnúť, že je to geometrická postupnosť, takže vieme povedať, že:

$$(g^1)^k + (g^2)^k + \cdots + (g^{p-1})^k \equiv \frac{g^k(g^{(p-1)k} - 1)}{g^k - 1} \pmod{p}. \tag{1}$$

Všimneme si ale, že menovateľ vie vskutku byť 0, keďže napr. pre $k = p-1$ platí $g^{p-1} \equiv 1$. Takže rovnosť 1 nesmieme použiť ak $g^k - 1 \equiv 0$, čo ľahko nahliadneme, že to platí práve vtedy, keď $k = (p-1)m$, kde m je nejaké nezáporné celé číslo.

V prípade, že $k = (p-1)m$ pre nejaké m, môžeme to dosadiť priamo do pôvodnej rovnosti: podľa vety 1 vieme, že $a^k \equiv 1^m \equiv 1 \pmod{p}$ pre všetky celé $a \in [1, p-1]$. Takže:

$$1^k + 2^k + \cdots + (p-1)^k \equiv \underbrace{1 + 1 + \ldots 1}_{p-1} \equiv (p-1) \not\equiv 0 \pmod{p}.$$

V prípade keď k nie je násobkom $p-1$, aplikujeme rovnosť 1:

$$\frac{g^k(g^{(p-1)k} - 1)}{g^k - 1} \equiv \frac{g^k(1^k - 1)}{g^k - 1} \equiv \frac{g^k \cdot 0}{g^k - 1} \equiv 0 \pmod{p}.$$

Takže, ukázali sme, že pre všetky k, čo sú násobky $p-1$, podmienka zo zadania neplatí, a pre všetky zvyšné k platí.

Cvičenie 10. Dokážte, že čísla $1, 2, ..., 238$ je možne usporiadať do kruhu tak, že pre ľubovoľné tri za sebou idúce čísla a, b, c, platí $239 \mid b^2 - ac$. **Hinty**: 10

Cvičenie 11. Ukážte, že 2 je primitívny prvok modulo 3^n. **Hinty**: 11

Cvičenie 12 (1993 Chinese IMO Team Selection Test)**.** Pre prvočíslo $p \geq 3$ definujeme

$$F(p) = \sum_{k=1}^{\frac{p-1}{2}} k^{120} \qquad\qquad f(p) = \frac{1}{2} - \left\{ \frac{F(p)}{p} \right\}$$

kde $\{x\} = x - \lfloor x \rfloor$. Určite hodnoty $f(p)$ pre každé p. **Hinty**: 12

Cvičenie 13. Dokážte, že 2 je primitívny prvok modulo 101. **Hinty**: 13

Cvičenie 14 (Putnam 1994)**.** Pre $a \in \mathbb{N}_0$ zadefinujeme $n_a = 100a - 101 \cdot 2^a$. Pre $0 \geq a, b, c, d \geq 99$ ukážte, že platí

$$n_a + n_b \equiv n_c + n_d \pmod{10100} \implies \{a, b\} = \{c, d\}.$$

Hinty: 14

Cvičenie 15 (Crux Mathematicorum)**.** Dokážte, že pre každé prvočíslo p existuje permutácia $(a_1, a_2, ..., a_{p-1})$ čísel $1, 2, ...p-1$ taká, že súčet $a_i + a_{i+1} + ... + a_j$ je deliteľný p iba pre dvojicu $(i, j) = (1, p-1)$. **Hinty**: 15

Cvičenie 16 (MKS 28-9-4)**.** Nech p je prvočíslo a b je celé číslo. Dokážte, že $b^{p^2-1} \equiv 1 \pmod{p^2}$ práve vtedy, keď $b^{p-1} \equiv 1 \pmod{p^2}$. **Hinty**: 16

Cvičenie 17. Dokážte, že ak $p \mid 2^{2^n} + 1$, tak $2^{n+1} \mid p - 1$. **Hinty**: 17 18

Cvičenie 18. Nájdite všetky dvojice prvočísel p, q, t.ž. $q \mid 2^p - 1$ také, že v prvočíselnóm rozklade $q - 1$ môžu byť len $2, 3, 5, 7$. **Hinty**: 19

Cvičenie 19. Nájdite všetky také n, že $n \mid 2^n - 1$. **Hinty**: 20

Cvičenie 20. Nájdite všetky nepárne n, že $n \mid 3^n + 1$. **Hinty**: 21

Cvičenie 21. Nájdite všetky také čísla n, že $n \mid 3^n - 2^n$. **Hinty**: 22

Cvičenie 22. Dokážte, že pre všetky kladné celé $a > 1$ a $n \geq 1$ platí $n \mid \varphi(a^n - 1)$. **Hinty**: 23

Cvičenie 23 (KMS 41/Z1-10)**.** Dané sú prvočísla p a q také, že $q = 2p + 1$. Dokážte, že existuje prirodzené číslo deliteľné q také, že jeho ciferný súčet v desiatkovej sústave je najviac 3. **Hinty**: 24

Cvičenie 24 (Indicka MO)**.** Nech p je nepárne prvočíslo. Nech A, B sú dve rôzne neprázdne podmnožiny množiny $\{1, 2, ..., p-1\}$ také, že platí:

1. $A \cup B = \{1, 2, ..., p-1\}$.
2. Ak $a_1, a_2 \in A$, tak $a_1 a_2 \pmod{p} \in A$. Ak $b_1, b_2 \in B$, tak $a_1 a_2 \pmod{p} \in A$.
3. Ak $a \in A, b \in B$, tak $ab \pmod{p} \in B$.

Nájdite všetky možne A, B. **Hinty**: 25

Cvičenie 25 (Putnam 2009/B6)**.** Dokážte, že pre každé kladné celé číslo n existuje postupnosť celých čísel $a_0, a_1 \ldots, a_{2009}$ s $a_0 = 0$ a $a_{2009} = n$ tak, že každý člen a_0 je buď nejaký prechádzajúci člen plus 2^k pre nejaké nezáporné celé číslo k, alebo sa rovná $b \pmod{c}$ pre niektoré predchádzajúce kladné členy b a c. **Hinty**: 26

Referencie

[1] Kin Y. Li. „Primitive Roots Modulo Primes“. In: *Mathematical Excalibur* (máj 2010), s. 1–2.

[2] Martin Andričík. *Kvadratické zvyšky a primitívny prvok*. https://iksko.org/files/sbornik12.pdf. Strmilov. 2023.

[3] Štěpán Šimsa. *Řády a primitivní prvek*. https://iksko.org/files/sbornik5.pdf. Strmilov. 2016.

Hinty

1. Aplikovať Malú Fermatovú vetu dvakrát pre p a q.
2. Aplikovať Malú Fermatovú vetu. Ako vybrať n? Všimnite si $\frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1=0$.
3. Aplikujte Eulerovu vetu, a potom uvažujte NSN exponentov.
4. Indukciou dokážte, že $\mathrm{ord}_{2^k}(x)$ je nanajvýš 2^{k-2}.
5. Ukážte, že $\mathrm{ord}_{p^2}(g), \mathrm{ord}_{p^2}(g+p)$ vieme ohraničiť 2 možnými hodnotami. Použite binomickú vetu.
6. Eulerova veta. $\varphi(2m)=\varphi(m)$. g a $g+m$ majú rôznu paritu.
7. Aplikujte Eulerovu vetu. Uvažujte rozdiel štvorcov, prešetrite 2 možnosti.
8. Čo vieme o inverzných prvkoch ku primitívnemu koreňu?
9. Kedy $(-g)$ nie je primitívny koreň? Čo nám to hovorí o parite rádu?
10. 239 je prvočíslo. Využite podobne myšlienky, ako v úlohe 1.
11. Indukcia podľa n. Ukážte 2 jedine možne hodnoty ord_{3^n}, jednu z nich vylúčte tiež indukciou.
12. Aby spraviť to iste ako v úlohe 10, treba, aby v hornej hranice nebola ta jedna polovica. Ako sa jej vieme zbaviť? Uvažujte paritu čísla 120.
13. Aplikujte dôsledok 3.1 a prešetrite 2 menšie prípady.
14. Využite predchádzajúcu úlohu a pozrite sa na zvyšky zvlášť modulo 100 a 101.
15. Vytvorte geometrickú postupnosť pomocou primitívneho prvku.
16. Využite Eulerovu vetu pre $n=p^2$.
17. Umocnite na druhu, a zratajte rád prvku modulo p.
18. Rád prvku 2 modulo p môže byť len nejaká mocnina dvojky (prečo?). Sporom ukážte, že pre $k \leq n$ $\mathrm{ord}_p(2) \neq 2^k$.
19. Malá Fermatova veta a rád 2 modulo q.
20. Uvažujte najmenšie prvočíslo $p \mid n$.
21. Uvažujte najmenšie prvočíslo $p \mid n$.
22. Uvažujte najmenšie prvočíslo $p \mid n$. Modulo p existujú inverzné prvky.
23. Nájdite prvok ktorý má rád n modulo a^n-1.
24. Skúste analyzovať mocniny 10.
25. Skúste analyzovať $A \cap B \neq \emptyset$.
26. Využite úlohy 12. Najprv prešetrite $3 \nmid n$.