mezinárodní
korespondenční
seminář

iksko.org

Diskrétní logaritmus

Matěj Doležálek

Abstrakt. Jak se chová násobení a mocnění mod n? S pomocí primitivního prvku si zadefinujeme diskrétní logaritmus a ukážeme, jak skrze grupy nahlížet na řády, kvadratické zbytky a další.

Bleskový úvod do grup

Definice. *Grupou* rozumíme množinu G s binární operací $\circ$ takovou, že

(i) G je uzavřená na $\circ$,
(ii) existuje takové $e \in G$, že $e \circ a = a \circ e = a$ pro každé $a \in G$,
(iii) pro každé $a \in G$ existuje a' takové, že $a \circ a' = a' \circ a = e$,
(iv) operace $\circ$ je asociativní.

Definice. Řekneme, že H je *podgrupou* grupy G, pokud $H \subseteq G$ a zároveň tvoří H grupu se stejnou operací jako G. Řekneme, že prvky $a_1, \ldots, a_n \in G$ *generují* H, pokud je H nejmenší podgrupa G splňující $\{a_1, \ldots, a_n\} \subseteq H$. Tuto skutečnost značíme $\langle a_1, \ldots, a_n \rangle = H$.

Definice. *Homomorfismem* mezi grupami G, H po řadě s operacemi $\circ$, $*$ rozumíme zobrazení $f : G \to H$ splňující

$$f(a \circ b) = f(a) * f(b)$$

pro každá $a, b \in G$. *Izomorfismem* rozumíme homomorfismus, který je zároveň bijekcí. Skutečnost, že G, H jsou izomorfní, značíme $G \simeq H$.

Definice. *Direktním součinem* grup G, H rozumíme grupu $G \times H$ uspořádaných dvojic (g, h), $g \in G$, $h \in H$, v níž binární operaci provádíme po složkách: v první složce operaci z G, v druhé z H.

Definice. Budiž n přirozené číslo. Znakem $\mathbb{Z}_n$ miňme množinu zbytkových tříd mod n, resp. jejich grupu se sčítáním. Znakem $\mathbb{Z}_n^*$ miňme množinu těch zbytkových tříd mod n, které jsou nesoudělné s n, resp. jejich grupu s násobením. Označme $\varphi(n) = |\mathbb{Z}_n^*|$.

Cvičení. Najdi všechny podgrupy $\mathbb{Z}_n$.

Mocnění v $\mathbb{Z}_n^*$

Definice. *Řádem* prvku $a \in \mathbb{Z}_n^*$ rozumíme mohutnost podgrupy, kterou a generuje v $\mathbb{Z}_n^*$. Značíme $\operatorname{ord}_n(a) = |\langle a \rangle|$.

Cvičení. Nejmenší přirozené k takové, že $a^k \equiv 1 \pmod{n}$, je $k = \operatorname{ord}_n(a)$.

Důsledek. Platí $a^x \equiv a^y \pmod{n}$, právě pokud $x \equiv y \pmod{\operatorname{ord}_n(a)}$.

Věta (Euler, malý Fermat). Pro $a \in \mathbb{Z}_n^*$ platí $a^{\varphi(n)} \equiv 1 \pmod{n}$. Pro prvočíslo p pak speciálně $a^{p-1} \equiv 1 \pmod{p}$.

Důsledek. Pro každé $a \in \mathbb{Z}_n^*$ platí $\operatorname{ord}_n(a) \mid \varphi(n)$. Díky tomu můžeme s exponenty ve výrazu mod n nakládat jako s prvky $\mathbb{Z}_{\varphi(n)}$.

Primitivní prvek

Definice. *Primitivním prvkem* rozumíme takové $g \in \mathbb{Z}_n^*$, že $\operatorname{ord}_n(g) = \varphi(n)$, neboli $\langle g \rangle = \mathbb{Z}_n^*$.

Lemma. Nechť $a \in \mathbb{Z}_n^*$ a $k \mid \operatorname{ord}_n(a)$. Pak v $\mathbb{Z}_n^*$ existuje prvek řádu k.

Lemma. Nechť $a, b \in \mathbb{Z}_n^*$, $\alpha = \operatorname{ord}_n(a)$, $\beta = \operatorname{ord}_n(b)$. Potom pokud jsou α, β nesoudělná, pak $\operatorname{ord}_n(ab) = \alpha\beta$.

Věta (Lagrange). Nechť je f polynom s celočíselnými koeficienty, z nichž ne všechny jsou násobky p. Pak má f nejvýše $\deg f$ různých kořenů mod p.

Věta. Pro liché prvočíslo p existuje primitivní prvek mod p.

Lemma. Pro liché prvočíslo p a přirozené $k \geq 2$ platí $\operatorname{ord}_{p^k}(1+p) = p^{k-1}$.

Věta. Primitivní prvek mod n existuje, právě pokud je n rovno 2, 4, p^k nebo $2p^k$ pro liché prvočíslo p a $k \in \mathbb{N}$.

Diskrétní logaritmus

Definice. Nechť je n jedno z čísel z předchozí věty. Pevně zvolme primitivní prvek g mod n. Potom *diskrétním logaritmem* prvku $a \in \mathbb{Z}_n^*$ míníme ten prvek $b \in \mathbb{Z}_{\varphi(n)}$, který splňuje $g^b \equiv a \pmod{n}$, a značíme jej $\log a$.

Cvičení. Nahlédni, že pro $x, y \in \mathbb{Z}_n^*$, $a \in \mathbb{Z}_{\varphi(n)}$ platí

$$\log(xy) \equiv \log x + \log y \pmod{\varphi(n)}, \qquad \log(x^a) \equiv a \log x \pmod{\varphi(n)}.$$

Pozorování. Diskrétní logaritmus je izomorfismem ze $\mathbb{Z}_n^*$ do $\mathbb{Z}_{\varphi(n)}$.

Cvičení (Wilsonova věta). Kongruence $(p-1)! \equiv -1 \pmod{p}$ platí právě tehdy, když je p prvočíslo.

Cvičení. Pokud existuje primitivní prvek mod n, pak už existuje přesně $\varphi(\varphi(n))$ navzájem nekongruentních primitivních prvků mod n.

Cvičení. Pokud $n > 2$ a existuje primitivní prvek, pak $\log(-1) \equiv \frac{\varphi(n)}{2} \pmod{\varphi(n)}$.

Cvičení. Nechť existuje primitivní prvek mod n. Potom:

(i) Kongruence $x^m \equiv 1 \pmod{n}$ má právě $\gcd(m, \varphi(n))$ řešení.
(ii) Výraz $x^m \pmod{n}$ nabývá právě $\frac{\varphi(n)}{\gcd(m,\varphi(n))}$ různých hodnot.

Cvičení. Budiž p prvočíslo a nechť je $H \neq \{1\}$ podgrupou $\mathbb{Z}_p^*$. Potom nutně platí $\sum_{a \in H} a \equiv 0 \pmod{p}$.

Co složené moduly?

Cvičení. Pro nesoudělná a, b platí $\varphi(ab) = \varphi(a)\varphi(b)$. Následně

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

kde součin jde přes prvočísla p, která dělí n.

Věta (Čínská zbytková). Nechť jsou a, b nesoudělná přirozená čísla. Potom platí

$$\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b, \qquad \mathbb{Z}_{ab}^* \simeq \mathbb{Z}_a^* \times \mathbb{Z}_b^*.$$

Cvičení. Pro $k \geq 2$ je $\mathbb{Z}_{2^k}^*$ izomorfní direktnímu součinu $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$.

Věta (Dirichlet). Nechť $a \in \mathbb{Z}_n^*$. Potom existuje nekonečně mnoho prvočísel p splňujících $p \equiv a \pmod{n}$.

Kvadratické zbytky

Definice. Prvek $a \in \mathbb{Z}_n^*$ nazvěme *kvadratickým zbytkem*, pokud $x^2 \equiv a \pmod{n}$ má řešení. V opačném případě jej zvěme *kvadratickým nezbytkem.*

Pozorování. Nenulové kvadratické zbytky mod p jsou právě prvky se sudým diskrétním logaritmem.

Důsledek. Pro liché prvočíslo p leží v $\mathbb{Z}_p^*$ právě $\frac{p-1}{2}$ kvadratických zbytků a $\frac{p-1}{2}$ kvadratických nezbytků.

Cvičení. Nechť je p prvočíslo a n přirozené číslo. Charakterizuj v $\mathbb{Z}_p^*$ zbytky tvaru x^n pomocí diskrétního logaritmu.

Cvičení. Pokud má n dva různé liché prvočíselné dělitele, pak neexistuje primitivní prvek mod n.

Definice. Nechť je p liché prvočíslo. Pak pro $a \in \mathbb{Z}_p^*$ definujeme *Legendreův symbol* jako

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{pokud je } a \text{ kvadratický zbytek,} \\ -1, & \text{pokud je } a \text{ kvadratický nezbytek.} \end{cases}$$

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

Důsledek. Legendreův symbol je úplně multiplikativní – pro $a, b \in \mathbb{Z}_p^*$ platí

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

Věta (Zákon kvadratické reciprocity). Nechť jsou p, q různá lichá prvočísla. Potom platí

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} \text{-1}, & \text{pokud } p \equiv q \equiv 3 \pmod{4}, \\ 1, & \text{jinak.} \end{cases}$$

Věta (Druhý suplement). Pro liché prvočíslo p platí

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{pokud } p \equiv \pm 1 \pmod{8}, \\ \text{-1}, & \text{pokud } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Počítáme

Příklad 1. Jsou dána různá prvočísla p, q. Dokaž $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Příklad 2. Jsou dána prvočísla p, q splňující $q \mid 2^p - 1$. Dokaž, že $p \mid q - 1$.

Příklad 3. Najdi všechna přirozená čísla nesoudělná se všemi členy nekonečné posloupnosti $a_n = 2^n + 3^n + 6^n - 1$. (IMO 2005, 4)

Příklad 4. Nechť je p prvočíslo a b celé číslo. Dokaž, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě pokud $b^{p-1} \equiv 1 \pmod{p^2}$. (MKS 28–9–4)

Příklad 5. Nechť je $p > 3$ prvočíslo a $n = \frac{2^{2p}-1}{3}$. Dokaž, že $n \mid 2^n - 2$. (*i*KS 1, N4)

Příklad 6. Najdi všechny trojice prvočísel p, q, r splňující soustavu dělitelností

$$p \mid q^r + 1, \qquad q \mid r^p + 1, \qquad r \mid p^q + 1.$$

(USA TST 2003)

Příklad 7. Dokaž, že pro $n > 4$ je součin všech primitivních prvků mod n kongruentní 1.

Příklad 8. Nechť je p prvočíslo tvaru $3k+2$. Ukaž, že pokud $p \mid a^2+ab+b^2$, pak $p \mid a, b$.

Příklad 9. Nechť je p prvočíslo tvaru 2^k+1. Potom je každý kvadratický nezbytek mod p primitivním prvkem.

Příklad 10. Pro liché prvočíslo p urči součet všech kvadratických zbytků a součet všech kvadratických nezbytků mod p.

Příklad 11. Rozhodni, zda existuje nekonečná rostoucí posloupnost čtverců celých čísel $a_1, a_2, \ldots$ taková, že $13^n \mid a_n + 1$ pro každé $n \in \mathbb{N}$. (ELMO SL 2014)

Příklad 12. Ukaž, že 2 je primitivní prvek mod 3^n.

Příklad 13. Pro $n \in \mathbb{N}$ nemá 2^n+1 žádné prvočíselné dělitele tvaru $8k-1$. (Vietnam TST 2004)

Příklad 14. Dokaž, že neexistuje přirozené číslo a takové, že všechna tři 2^a-1, $2^{2a+1}-1$, $2^{4a+3}-1$ jsou prvočísla.

Příklad 15. Je dáno liché prvočíslo p, přirozené m, n a celé nezáporné s tak, že $p \mid m^{2^s}+n^{2^s}$. Dokaž, že $p \equiv 1 \pmod{2^{s+1}}$.

Příklad 16. Pro každé $a \in \mathbb{N}$, které není čtverec, existuje nekonečně mnoho prvočísel p takových, že $\left(\frac{a}{p}\right) = -1$.

Příklad 17. Pro $n \in \mathbb{N}$ existuje nekonečně mnoho prvočísel p takových, že každý primitivní prvek mod p je větší než n.

Příklad 18. Najdi všechna $n > 1$, pro která existuje právě jedno $0 < a \leq n!$ takové, že $n! \mid a^n + 1$. (ISL 2005 N4)

Příklad 19. Nechť je $p \geq 5$ prvočíslo. Dokaž, že existuje $1 \leq a < p-1$ takové, že ani $a^{p-1}-1$ ani $(a+1)^{p-1}-1$ není násobkem p^2. (ISL 2001 N4)

Příklad 20. Nechť je p liché prvočíslo. Najdi všechny dvojice (A, B) takové, že A, B jsou různé neprázdné podmnožiny $\mathbb{Z}_p^*$ splňující

(i) $A \cup B = \mathbb{Z}_p^*$,
(ii) pokud $a, b \in A$ nebo $a, b \in B$, pak $ab \in A$,
(iii) pokud $a \in A$, $b \in B$, pak $ab \in B$. (Indická MO)

Příklad 21. Dokaž, že existuje nekonečně mnoho přirozených n takových, že n^4+1 má prvočíselného dělitele většího než $2n$. (MKS 30–2–8)

Příklad 22 (Lifting the exponent lemma – LTE). Nechť je p liché prvočíslo a $x, y \in \mathbb{Z}$ tak, že $p \mid x-y$, $p \nmid x, y$. Potom pro $n \in \mathbb{N}$ platí

$$v_p\left(x^n - y^n\right) = v_p(x-y) + v_p(n),$$

kde $v_p(a)$ značí p-valuaci, tj. exponent největší mocniny p, jež dělí a.

Příklad 23. Najdi všechna přirozená n taková, že $n \mid 2^n - 1$.

Příklad 24. Najdi všechna přirozená n taková, že $n^2 \mid 3^n + 1$. (TR*i*KS 69)

Příklad 25. Najdi všechna přirozená n taková, že $n^2 \mid 2^n + 1$.

Příklad 26. Dokaž, že pro $n > 1$ nemůže nastat $n \mid 2^{n-1} + 1$.

Příklad 27. Nechť je p prvočíslo, které dává zbytek 3 nebo 5 mod 8. Nechť navíc platí $p = 2q + 1$, kde q je také prvočíslo. Urči

$$\omega^{2^1} + \omega^{2^2} + \cdots + \omega^{2^{p-1}},$$

kde $\omega \in \mathbb{C}$ splňuje $\omega^p = 1$, $\omega \neq 1$.

Příklad 28. Urči počet všech posloupností $\{a_n\}_{n=0}^{\infty}$ reálných čísel takových, že $a_{m \cdot n} = a_m \cdot a_n$ a zároveň $a_n = a_{n+2011}$ pro každá $m, n \in \mathbb{N}$. (MKS 30–6–8)

Příklad 29. Je dáno liché prvočíslo p. Najdi všechna k taková, že

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

(Hungary-Israel Math Competition 2009)

Příklad 30. Pro liché prvočíslo p definujme

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

kde $\{x\} = x - \lfloor x \rfloor$. Urči $f(p)$ pro každé p. (China TST 1993)

Příklad 31. Pro $a \in \mathbb{N}_0$ definujme $n_a = 101a - 100 \cdot 2^a$. Pro $0 \leq a, b, c, d \leq 99$ ukaž

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

(Putnam 1994)

Příklad 32. Najdi všechna přirozená $n > 1$, pro která

$$n \mid 1 + \prod_{a \in \mathbb{Z}_n^*} a.$$

Příklad 33. Buď p prvočíslo a $a_1, \ldots, a_n$ po dvou různá přirozená čísla menší než p. Předpokládejme, že $p \mid a_1^k + \cdots + a_n^k$ pro každé $k \in \{1, \ldots, p-2\}$. Urči $\{a_1, \ldots, a_n\}$. (Mathematical Reflections)

Příklad 34. Budiž q liché prvočíslo. Najdi všechna prvočísla p taková, že existuje celé číslo x splňující

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

(ELMO SL 2010)

Příklad 35. Budiž $p > 13$ prvočíslo takové, že $p = 2q+1$ pro nějaké prvočíslo q. Urči, kolik existuje uspořádaných dvojic (m, n) celých čísel takových, že $0 \leq m < n < p-1$ a zároveň

$$3^m + (-12)^m \equiv 3^n + (-12)^n \pmod{p}.$$

(ELMO SL 2011)

Příklad 36. Jsou dána celá čísla a, b taková, že pro všechna přirozená n platí $b^n + n \mid a^n + n$. Dokaž, že $a = b$. (ISL 2005 N6)

Příklad 37. Najdi všechny trojice (a, b, c) přirozených čísel takové, že pro každé přirozené n, které nemá žádného prvočíselného dělitele menšího než 2020, platí

$$n + c \mid a^n + b^n + n.$$

(ELMO SL 2014)

Literatura a zdroje

[1] Štěpán Šimsa; *Řády a primitivní prvek*, Sborník *i*KS, 2016
[2] Filip Bialas, Kuba Löwit; *Teorie grup*, PraSečí seriál, 2017/2018
[3] Filip Bialas; *Kvadratická reciprocita*, Zásada 2017

Hinty

Hint 1. Dívej se zvlášť mod p a mod q.
Hint 2. $\mathrm{ord}_q(2) = p$.
Hint 3. Malý Fermat je tvůj kamarád. $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.
Hint 4. Kolik může být $\log\left(b^{p-1}\right)$?
Hint 5. Kolik může být $\mathrm{ord}_{q^\alpha}(2)$ pro prvočíselnou mocninu q^α, jež dělí n?
Hint 6. $\mathrm{ord}_p(q) \in \{2, 2r\}$. Pro lichá p, q, r vyvoď spor.
Hint 7. Co je nějak spárovat?
Hint 8. Uprav na $a^3 \equiv b^3 \pmod p$.
Hint 9. Řád dělí $p - 1$.
Hint 10. Geometrická řada s pomocí primitivního prvku.
Hint 11. Samozřejmě, že existuje. Rostoucnost nás vůbec neomezuje.
Hint 12. Kvadratické zbytky mod 3 a kubické zbytky mod 9.
Hint 13. Eulerovo kritérium a druhý suplement.
Hint 14. Kvadratické zbytky mod a, $2a + 1$, $4a + 3$.
Hint 15. -1 je 2^s-tá mocnina něčeho, přitom její diskrétní logaritmus je $\frac{p-1}{2}$.
Hint 16. Navol si správné zbytky modulo prvočinitelé čísla a. Čínská zbytkovka a Dirichlet zařídí zbytek.
Hint 17. Navol si správné zbytky modulo $1, \ldots, n$. Čínská zbytkovka a Dirichlet zařídí zbytek.
Hint 18. Řeš zvlášť v jednotlivých modulech p^α – každé řešení mod $n!$ jednoznačně odpovídá posloupnosti řešení v jednotlivých modulech p^α. Pro složené n najdi spor díky $p^2 \mid n!$ pro prvočíslo $p \mid n$.
Hint 19. Vždy $(-a)^{p-1} \equiv a^{p-1}$. Jak jsou rozmístěna řešení $x^{p-1} \equiv 1 \pmod{p^2}$? Musí tvořit podgrupu v $\mathbb{Z}_{p^2}^*$ – najdi spor.
Hint 20. Rozmysli si, že A, B musí být disjunktní. Kam patří primitivní prvek?
Hint 21. Ber prvočíslo $p = 8k + 1$.
Hint 22. Za zadaných předpokladů si rozmysli ekvivalence

$$x^p \equiv y^p \pmod{p^{k+1}} \iff x \equiv y \pmod{p^k},$$
$$x^m \equiv y^m \pmod{p^k} \iff x \equiv y \pmod{p^k}$$

pro $p \nmid m$.
Hint 23. Nechť je p nejmenší prvočinitel n. Najdi spor diskrétním logaritmem (anebo řádem) mod p.
Hint 24. Vyřeš zvlášť $2 \mid n$. Potom stejně jako předchozí příklad.
Hint 25. Bacha, tady už $n = 1$ není jediné řešení. Může se hodit LTE.
Hint 26. Předpokládej zadanou dělitelnost. Rozmysli si, že $2 \nmid n$ a že -1 i 2 jsou kvadratické zbytky modulo každé prvočíslo $p \mid n$. Poté vyvoď spor pomocí prvočísla $p \mid n$, které minimalizuje $v_2(p - 1)$.
Hint 27. 2 je primitivní prvek mod p.
Hint 28. Zjevně $a_n \in \{-1, 0, 1\}$. Vezmi primitivní prvek, dořeš nulu.
Hint 29. Vyrob geometrickou řadu s primitivním prvkem.

Hint 30. Rozliš případy podle toho, zda $p-1 \mid 120$. Vyrob geometrickou řadu s primitivním prvkem.

Hint 31. Uvažuj zvlášť mod 100 a mod 101. Využij toho, že 2 je primitivní prvek mod 101.

Hint 32. Pokud existuje primitivní prvek, je to hračka. Pro ostatní najdi spor.

Hint 33. Uvaž polynom $x^{\log a_1} + \cdots + x^{\log a_n}$. Zadání mu dává spoustu kořenů.

Hint 34. Nejdřív si najdi dostatek x takových, že levá strana má p-valuaci $q-1$. Poté dořeš tím, že nějaké z nich je mod p kořenem $x^{q-1} + \cdots + 1$, ale není kořenem $\sum_{j=1}^{q-1} j x^{j-1}$.

Hint 35. $\left(\frac{3}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = -1$, obě -4, -12 jsou primitivní prvky. Uprav s využitím $z = n - m$.

Hint 36. Ukaž, že $a-b$ má hodně prvočíselných dělitelů. Moduly p a $p-1$ jsou pro prvočíslo p nesoudělné!

Hint 37. Ukaž, že $a+b-c$ má hodně prvočíselných dělitelů. Navol si zbytky n v různých modulech dle libosti.