Aritmetika a algoritmy, otázky ke zkoušce a cvičení (19. května 2024)

Otázky

- Komutativní monoidy, grupy a okruhy. Obory integrity a tělesa. Bezprostřední důsledky axiomů: jednoznačnost neutrálního a inverzních prvků v monoidu, krácení v grupě, násobení nulou v okruhu, krácení v oboru integrity. Eulerova věta ve verzi pro komutativní grupy.
- Dělitelnost v oborech integrity: cvičení 1–3.
- Eukleidův algoritmus ve struktuře $\mathbb{Z}$ a jeho zobecněná (čtyřsloupcová) varianta. Jeho vlastnosti a důkaz korektnosti. Matematická tvrzení, která lze považovat za důsledky korektnosti Eukleidova algoritmu: cvičení 4 a Bézoutova věta ve struktuře celých čísel. Aplikace Eukleidova algoritmu (cv. 5–7).
- Matematické důsledky Bézoutovy věty: invertibilní prvky v $\mathbb{Z}_m$, ekvivalentní podmínka pro nesoudělnost v $\mathbb{Z}$, cv. 8–10, přičemž 8 je ke zkoušce povinné.
- Eulerovy grupy, Eulerova funkce a Eulerova (Fermatova) věta (cv. 11 a 12).
- Modulární reprezentace, čínská zbytková věta. Aplikace modulárních reprezentací: výpočet hodnot Eulerovy funkce, a také (hlavně) metoda RSA.
- Když m je prvočíslo a $k \mid m-1$, pak $\Phi(m)$ obsahuje přesně k prvků řádu $\varphi(k)$. Tato otázka je nepovinná, ale pokud někdo zvládá důkaz a dovede říci stručně něco o jejím významu a souvislostech, není nutné se jej ptát na nic dalšího (ani na cvičení).

Cvičení

1. Dokažte následující tvrzení z axiomů oboru integrity. (a) Když pro prvek x platí $x \mid 1$, pak x je nesoudělný s každým y. (b) Když naopak $\neg(x \mid 1)$, pak x je soudělný s nulou. (c) Když x je ireducibilní, pak x je soudělný s y, právě když $x \mid y$.
2. Dále dokažte. (d) Když x a y jsou největší společní dělitelé prvků a a b, pak $x \parallel y$. (e) Když $d \neq 0$ je největší společný dělitel prvků ad a bd, pak a a b jsou nesoudělné.

3. A dále dokažte, že když s v libovolném oboru integrity je prvočíslo a $x \mid s^k \cdot w$, pak existují prvek y a číslo i takové, že $x = s^i \cdot y$ a přitom $y \mid w$. Z toho vyvoďte, že když $x \mid s^2$, pak $x \parallel s^2$, nebo $x \parallel s$, nebo $x \mid 1$.

   Návod. Pracujte s největším $i \leq k$ takovým, že $s^i \mid x$. Pak existují v a y taková, že $x = s^i \cdot y$ a $s^i \cdot y \cdot v = s^k \cdot w$. Rozlište případy $i = k$ a $i < k$. Když $i < k$, máte $y \cdot v = s^{k-i} \cdot w$. V této situaci dokažte a použijte následucící pomocné tvrzení: když s je prvočíslo, $s^j \mid y \cdot v$ a přitom $\neg(s \mid y)$, pak $s^j \mid v$.

4. Zdůvodněte, že z úvah o korektnosti Eukleidova algoritmu (jak v oboru celých, tak v oboru přirozených čísel) plyne, že pro každá dvě čísla existuje jejich největší společný dělitel, neboli společný dělitel dělitelný všemi společnými děliteli.

5. Užijte Eukleidův algoritmus k nalezení největšího společného dělitele (a) čísel 65 975 193 a 265 927, (b) čísel 180 589 a 54 737.

6. V okruhu $\mathbb{Z}_{65536}$ vyřešte rovnici $7x = 9$.

7. O každé z rovnic $4495x + 2356y = 155$ a $4495x + 2356y = 160$ (o každé zvlášť) rozhodněte, zda má řešení v oboru $\mathbb{Z}$ celých čísel. Pokud ano, nalezněte některá řešení.

8. Dokažte, že celé číslo (a také prvek libovolného oboru integrity, v němž platí Bézoutova věta) je ireducibilní, právě když je prvočíslem.

9. Ve stejné situaci dokažte, že když x a y jsou nesoudělní dělitelé čísla z, pak $x \cdot y \mid z$.

10. Navíc zdůvodněte ještě toto: když je číslo x nesoudělné s každým z $y_1, \ldots, y_k$, pak je nesoudělné i s jejich součinem $\prod_{i=1}^{k} y_i$.

11. Určete hodnoty Eulerovy funkce φ pro argumenty 48, 49, 100, 120 a 144.

12. Na základě znalosti čísla $\varphi(100)$ a s využitím Eulerovy věty (bez užití kalkulátoru) určete poslední dvě desetinné cifry čísla 7^{121}. Určete také poslední dvě desetinné cifry čísla 6^{121}, a to například počítáním s modulárními reprezentacemi vůči modulům 4 a 25.

13. Pro šifrování metodou RSA byl zvolen šifrovací klíč $r = 1\,037$, a dále jako limit pro šifrované číslo bylo zvoleno číslo $m = 2\,248\,240\,321$. To znamená, že funkce $x \mapsto x^{1037} \bmod 2\,248\,240\,321$ je příslušnou šifrovací funkcí. S pomocí vhodných prostředků (plus případně údaje uloženého v metadatech tohoto dokumentu) rozluštěte číslo 1 579 156 340.

14. (a) Dokažte, že když n není prvočíslo, pak $2^n - 1$ není prvočíslo.
(b) Když n má lichého dělitele většího než 1, pak $2^n + 1$ není prvočíslo. Všimněte si, že z (b) plyne, že $2^n + 1$ může být prvočíslem pouze tehdy, když $n = 0$ nebo když n je mocninou dvojky.

    Návod. V (a) dokažte a využijte rovnost $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + 1)$, v (b) rovnost $a^{2k+1} + 1 = (a+1)(a^{2k} - a^{2k-1} + a^{2k-2} - \ldots + 1)$.

15. Složené číslo $m > 2$ je *pseudoprvočíslo*, jestliže v $\mathbb{Z}_m$ platí $2^{m-1} = 1$. Zdůvodněte, že podmínka (i), že v $\mathbb{Z}_m$ platí $2^{m-1} = 1$, je pro *liché* $m > 2$ ekvivalentní s podmínkou (ii), že v $\mathbb{Z}_m$ platí $2^m = 2$. Dále zdůvodněte, že žádné *sudé* $m > 2$ podmínku (i) nesplňuje, a ověřte, že $m = 161\,038$ splňuje podmínku (ii).

16. Stanovte řád prvků 2 a 3 v grupách $\Phi(19)$, $\Phi(43)$, $\Phi(73)$ a $\Phi(127)$.

    Návod. Zde i v dalších cvičeních, kde je nutné určit řád nějakého prvku, užijte kalkulátor BNCalc.pdf.

17. Stanovte řád prvků 29 a 37 v grupě $\Phi(2^{61} - 1)$. Vyvoďte z toho, že $2^{61} - 1$ je prvočíslo.

    Návod. Nejprve si pomocí funkce "factoring" kalkulátoru BNCalc.pdf opatřete prvočíselný rozklad čísla $2^{61} - 2$. Z něj stanovte relevantní exponenty.

18. Když $s \in \Phi(m)$ má řád $\varphi(m)$, pak jeho umocňováním lze získat všechny prvky grupy $\Phi(m)$ (zdůvodněte). Takovému s se říká *generátor* grupy $\Phi(m)$, a když m je prvočíslo, pak také *primitivní kořen* prvočísla m. Má-li $\Phi(m)$ nějaký generátor, říká se jí *cyklická* grupa. Určete, které z grup $\Phi(9)$, $\Phi(10)$ a $\Phi(21)$ jsou cyklické. Pro každé z prvočísel 23, 31 a 41 najděte některý jeho primitivní kořen.

19. K větě, že když p je prvočíslo, pak $\Phi(p)$ je cyklická grupa, přidejte tento dodatek či zobecnění: i grupa $\Phi(p^2)$ je cyklická.

    Návod. Řád každého $r \in \Phi(p^2)$ je dělitel čísla $p \cdot (p-1)$. Když r není násobek p, pak $\mathrm{Mod}(r, p) \neq 0$, neboli $\mathrm{Mod}(r, p) \in \Phi(p)$. Eulerova věta dává $(\mathrm{Mod}(r, p))^{p-1} = 1$ v $\mathbb{Z}_p$. Takže $r \cdot (\mathrm{Mod}(r, p))^{p-1} = r$ v $\mathbb{Z}_p$. Místo umocnění zbytku, vynásobením číslem r a pak stanovením zbytku lze zbytek spočítat až na konec. Takže $\mathrm{Mod}(r^p, p) = r$. Z toho plyne že $\mathrm{Mod}(r^p, p^2)$ je jedno z čísel $r + k \cdot p$ pro $k < p$. Takže r^p není 1 v $\mathbb{Z}_{p^2}$, z čehož dále plyne, že r nemá v $\mathbb{Z}_{p^2}$ řád p. Zvolme pevně $s \in \Phi(p)$, jehož řád ve $\Phi(p)$ je $p-1$ (tj. takové s, které je primitivním kořenem prvočísla p). Zdůvodníme, že lze zvolit $r \in \{s, s+p\}$, jehož řád v $\mathbb{Z}_{p^2}$, kromě toho, že není p, není ani dělitel čísla $p-1$. Binomická věta dává $(s+p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} \cdot s^{p-1-i} \cdot p^i$. Všechny členy součtu pro $i \geq 2$ jsou dělitelné číslem p^2, takže jsou to nuly

v $\mathbb{Z}_{p^2}$. Máme tedy $(s+p)^{p-1} = s^{p-1} + (p-1) \cdot s^{p-2} \cdot p$. Prvky s^{p-1} a $(s+p)^{p-1}$ nemohou současně být jedničky v $\mathbb{Z}_{p^2}$, protože jinak by jejich rozdíl byl dělitelný číslem p^2 a platilo by $p \mid (p-1) \cdot s^{p-2}$.

20. Složené číslo $m > 2$ je *absolutní pseudoprvočíslo*, jestliže v $\mathbb{Z}_m$ platí $s^{m-1} = 1$ pro každé $s \in \Phi(m)$. Ověřte, že 341, 561, 645, 1105, 1387, 1729 a 1905 jsou pseudoprvočísla a určete, která z nich jsou absolutními pseudoprvočísly.

    Návod. Užijte větu, že když p je prvočíslo a $k \mid p-1$, pak ve $\Phi(p)$ je přesně $\varphi(k)$ prvků řádu k. Například když $s \in \Phi(341)$ má vůči modulům 11 a 31 modulární reprezentaci $[u, v]$ a v má ve $\Phi(31)$ řád třeba 30 nebo 15, což se určitě pro některá v stane, pak v^{340} není 1 v $\mathbb{Z}_{31}$, takže s^{340} není 1 v $\mathbb{Z}_{341}$. Takže 341 není absolutním pseudoprvočíslem.

21. Pro číslo $m = 341$ určete $\varphi(m)$ a stanovte počet všech prvků s grupy $\Phi(m)$ splňujících podmínku $s^{m-1} = 1 \bmod m$ a podmínku $s^m = s \bmod m$. Totéž udělejte pro $m = 561$.

Reference

[1] H. Hasse. *Number Theory.* Springer, 1980.

[2] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[3] V. R. Pratt. Every prime has a succinct certificate. *SIAM J. Comput.*, 4(3), 1975.

[4] F. Veselý. *O dělitelnosti čísel celých*, svazek 14 v *Škola mladých matematiků.* Mladá fronta, Praha, 1966.