Aritmetika a algoritmy, otázky ke zkoušce a cvičení (7. května 2021)

Otázky

- Bezoutova věta: algoritmické aspekty (cvičení 2 a 8) a matematické důsledky (cv. 4–7).
- Komutativní monoidy, grupy a okruhy. Bezprostřední důsledky axiomů.
- Eulerovy grupy, Eulerova funkce a Eulerova (Fermatova) věta. Cvičení 9 a 10.
- Modulární reprezentace a čínská zbytková věta. Cvičení 10. Pseudoprvočísla (cv. 13, 14, 15).
- Metoda RSA. Důkaz správnosti pomocí modulárních reprezentací. Cvičení 12.

Cvičení

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

2. 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, použijte zobecněný Eukleidův algoritmus k nalezení některého řešení.

3. Zdůvodněte, že z úvah o korektnosti Eukleidova algoritmu (jak v oboru celých, tak v oboru přirozených čísel) plyne, že pro každá dvě čísla, z nichž alespoň jedno je nenulové, existuje jejich společný dělitel, který je dělitelný všemi jejich (ostatními) společnými děliteli.

4. Dokažte, že v oboru celých čísel (a také v každém oboru integrity, v němž platí Bezoutova věta) jsou pro nenulové číslo p následující podmínky ekvivalentní:
   (i) každý dělitel čísla p je buď invertibilní, nebo dělitelný číslem p (takže pokud p navíc není invertibilní, je prvočíslem),
   (ii) $\forall a \forall b (p \mid a \cdot b \rightarrow p \mid a \vee p \mid b)$.

   Návod. V důkazu implikace (i) $\Rightarrow$ (ii) užijte Bezoutovu větu na dvojici p a a, čili uvažujte čísla x a y taková, že $px + ay$ je dělitel jak čísla p, tak čísla a. Pokud $px + ay$ je invertibilní, čili je dělitelem čísla 1, pak $pxb + aby \mid b$.

Domyslete podrobně. Pak ale $p \mid b$. Druhá možnost, kdy $px + ay$ je dělitelné číslem p, je také příznivá: v tom případě máme $p \mid a$. V důkazu implikace (ii) $\Rightarrow$ (i) uvažujte dělitel d čísla p, neboli uvažujte čísla d a u taková, že $du = p$. Na d a u použijte podmínku (ii). Kde v obou důkazech se uplatní předpoklad, že $p \neq 0$?

5. S pomocí Bezoutovy věty dokažte, že celá nenulová čísla a a b jsou nesoudělná, právě když $\forall z(a \mid bz \rightarrow a \mid z)$.

6. Vyvoďte z předchozího cvičení, že když x a y jsou nesoudělní dělitelé čísla z, pak $x \cdot y \mid z$.

7. Vyvoďte z cvičení 5 ještě toto: když x je nesoudělné s každým z čísel $y_1, \ldots, y_k$, pak je nesoudělné i s jejich součinem $\prod_{i=1}^{k} y_i$.

8. V okruhu $\mathbb{Z}_{65536}$ vyřešte rovnici $7x = 100$.

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

10. Na základě znalosti čísla $\varphi(100)$ a s využitím Fermatovy 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.

11. (a) Dokažte, že když n není prvočíslo, pak $2^n - 1$ není prvočíslo.
    (b) Když n má lichý dělitel větší než 1, pak $2^n + 1$ není prvočíslo.

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

12. 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 $1\,579\,156\,340$.

13. Dokažte, že pro liché číslo $m > 2$ je v $\mathbb{Z}_m$ podmínka $2^{m-1} = 1$ ekvivalentní s podmínkou $2^m = 2$. Dokažte, že číslo $161\,038$ splňuje druhou z těchto podmínek a v tomto smyslu je pseudoprvočíslem (první podmínku ovšem splňovat nemůže, 2 není v $\mathbb{Z}_m$ invertibilní).

14. Dokažte, že čísla 341, 561, 645, 1105, 1387, 1729 a 1905 jsou pseudoprvočísla. Některá z nich v $\mathbb{Z}_m$ splňují silnější podmínku než $2^{m-1} = 1$, totiž, že pro každé s nesoudělné s m v $\mathbb{Z}_m$ platí $s^{m-1} = 1$. Která z nich to jsou? Číslům splňujícím tuto silnější podmínku se říká *absolutní pseudoprvočísla*.

15. 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.