Teorie čísel: Cvičení 4 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, e-mail: simonkahlavinkova@gmail.com

Nápovědy:

-1. Uhodněte nejmenší řešení a využijte větu na začátku sady příkladů.

0. Uvažte rovnici modulo 3.

1. Postupujte jako v příkladech -1 a 0.

2. Uvažte rovnici modulo 7.

3. Při důkazu alespoň jedné z implikací musíte rozložit $x^2 - my^2$ na součin.

4. Umocněte odpovídající $x + y\sqrt{m}$.

5. Využijte existenci nekonečně mnoha řešení rovnice $x^2 - my^2 = 1$.

6. Využijte příklad 5.

7. Vhodnou substitucí se úloha převede na Pellovu rovnici.

8. Úloha vede na Pellovu rovnici, a to dokonce dvěma různými způsoby.

9. Počítejte modulo 3 a modulo 4. Alternativní postup: Použijte explicitního tvaru řešení.

10–12. Využijte tvrzení o souvislosti řešení Pellovy rovnice s řetězovými zlomky.

13. Využijte tvrzení 2.14 ze skript.

Výsledky:

-1. Minimální řešení $(3, 2)$, množina všech řešení: $\{(a, b) \mid a + b\sqrt{2} = \pm(3 + 2\sqrt{2})^n, n \in \mathbb{Z}\}$. Další explicitní řešení například $(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}$, tj. $(17, 12)$.

1. a) Minimální řešení $(2, 1)$, množina všech řešení: $\{(a, b) \mid a + b\sqrt{3} = \pm(2 + \sqrt{3})^n, n \in \mathbb{Z}\}$.
   b) Minimální řešení $(9, 4)$, množina všech řešení: $\{(a, b) \mid a + b\sqrt{5} = \pm(9 + 4\sqrt{5})^n, n \in \mathbb{Z}\}$.
   c) Minimální řešení $(8, 3)$, množina všech řešení: $\{(a, b) \mid a + b\sqrt{7} = \pm(8 + 3\sqrt{7})^n, n \in \mathbb{Z}\}$.

6. Například $(1, 1)$, $(3, 5)$, $(11, 19)$, $(41, 71)$.

10. $\sqrt{41} = [6, \overline{2, 2, 12}]$, minimální řešení je $(2049, 320)$ pro $+1$ a $(32, 5)$ pro -1.

11. $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$, minimální řešení pro $+1$ je $(24, 5)$, pro -1 řešení neexistuje.
    $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$, minimální řešení $(649, 180)$ pro $+1$ a $(18, 5)$ pro -1.

12. $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$, minimální řešení je $(9801, 1820)$ pro $+1$ a $(70, 13)$ pro -1.
    $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$.
    Minimální řešení je $(1766319049, 226153980)$ pro $+1$ a $(29718, 3805)$ pro -1.

13. $\sqrt{41} = [6, \overline{2, 2, 12}]$, vyjde $\pm 1, \pm 4, \pm 5$. (Pozor, tvrzení 2.14 ze skript dává pouze řešení s nesoudělnými x, y.)

Řešení vybraných příkladů:

3) Implikace zprava doleva je jasná: $x + y\sqrt{m} \geq 1 + \sqrt{m} > 1$. K opačné implikaci nejprve z $(x + y\sqrt{m})(x - y\sqrt{m}) = 1$ odvodíme $x - y\sqrt{m} = (x + y\sqrt{m})^{-1}$, takže $0 < x - y\sqrt{m} < 1$. Sečtením nerovností $x + y\sqrt{m} > 1$ a $x - y\sqrt{m} > 0$ dostaneme $2x > 1$, takže x je kladné. Pak už je zjevné, že i y musí být kladné.

4, 5) Řešení zobecněné Pellovy rovnice s pravou stranou -1 odpovídá prvku $\alpha \in \mathbb{Z}[\sqrt{m}]$, jehož norma splňuje $\mathcal{N}(\alpha) = -1$. Díky multiplikativitě normy platí $\mathcal{N}(\alpha^2) = \mathcal{N}(\alpha)^2 = 1$, takže prvek α^2 odpovídá řešení Pellovy rovnice (a je snadné si rozmyslet, že netriviálnímu). Explicitně můžeme spočítat, že když $x^2 - my^2 = -1$, pak $\alpha^2 = (x + y\sqrt{m})^2 = (x^2 + my^2) + 2xy\sqrt{m}$, takže $(x^2 + my^2, 2xy)$ je řešením Pellovy rovnice. Obdobně lze díky existenci nekonečně mnoha prvků normy 1 v $\mathbb{Z}[\sqrt{m}]$ (neboli nekonečně mnoha řešení Pellovy rovnice) velmi snadno dokázat, že existuje-li alespoň jeden prvek normy B, pak jich existuje nekonečně mnoho.

9)

- Elegantní postup využívající kongruence (nástin): Počítání modulo 4 zaručí, že y je sudé (jinak $x^2 \equiv 3 \pmod 4$, což nelze). Podobně modulo 3 zjistíme, že z x, y je právě jedno číslo dělitelné třemi. Dohromady je součin x a y dělitelný šesti.

- Náročnější postup využívající explicitní znalost řešení: Z příkladu -1. víme, že všechna řešení jsou tvaru $\{(a, b) \mid a + b\sqrt{2} = \pm(3 + 2\sqrt{2})^n, n \in \mathbb{Z}\}$. Když uvážíme binomickou větu, tak dostaneme

$$a = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} 3^{n-2i} \cdot (2\sqrt{2})^{2i},$$

$$b\sqrt{2} = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} 3^{n-2i-1} \cdot (2\sqrt{2})^{2i+1}.$$

  Odtud vidíme, že b je vždy dělitelné 2 a pokud je n liché, tak je a dělitelné 3, a naopak pokud je n sudé, tak je b dělitelné 3.