# Cvičení 27. 3. 2012 – řešení

**Příklad 1.** Doplňte následující tabulku:

| okruh | obor integrity | gaussovský | OIHI | euklidovský | noetherovský |
|---|---|---|---|---|---|
| $\mathbb{Z}$ | a | a | a | a | a |
| $\mathbb{Z}_{10}$ | n | n | n | n | a |
| $\mathbb{Z}[x]$ | a | a | n | n | a |
| $\mathbb{Z}[x,y]$ | a | a | n | n | a |
| $\mathbb{Z}[x_1,x_2,\dots]$ | a | a | n | n | n |
| $\mathbb{Z}[i]$ | a | a | a | a | a |
| $\mathbb{Z}[\sqrt{2}i]$ | a | a | a | a | a |
| $\mathbb{R}$ | a | a | a | a | a |

**Příklad 2.** Buďte $a_1,\dots,a_n,d\in\mathbb{Z}$. Dokažte, že rovnice

$$a_1x_1+\cdots+a_nx_n=d$$

má celočíselné řešení, právě když $NSD(a_1,\dots,a_n)|d$.

*Řešení: Řešení:* Rovnice má řešení, právě když $d$ leží v ideálu $(a_1,\dots,a_n)$, což je ale ideál $(NSD(a_1,\dots,a_n))$.

**Příklad 3.** Vyřešte v $\mathbb{Z}$ rovnice:

1. $x^2=27y$
2. $y^3-x^3=91$
3. $x^2+x=y^3$

*Řešení:*

1. Řešením jsou všechny dvojice $(x,y)=(9z,3z^2)$ pro $z\in\mathbb{Z}$ (což je totéž co dvojice $(3^nt,3^{2n-3}t^2)$ pro $t\in\mathbb{Z}$, $t$ není násobek 3).
2. Víme, že $(y-x)(y^2+xy+x^2)=7\cdot13$, takže by nám stačilo projít všech 8 možných rozkladů 91 na součin celých čísel. My si práci trochu ulehčíme pozorováním, že $y^3>x^3$, tedy protože $x\mapsto x^3$ je rostoucí funkce, musí být $y-x>0$. Máme proto jenom čtyři možnosti:

(a) $y - x = 1, y^2 + xy + x^2 = 91$ Dosazením první rovnice do druhé dostaneme: $(x+1)^2 + x(x+1) + x^2 = 91$, což je kvadratická rovnice $x^2 + x - 30 = 0$, která má kořeny $x = 5$ a $x = -6$. Dosazením za $y$ dostaneme řešení $(x, y) = (5, 6)$ a $(x, y) = (-6, -5)$.

(b) $y - x = 7, y^2 + xy + x^2 = 13$ Použitím postupu jako výše dostaneme řešení $(-4, -3)$ a $(3, 4)$.

(c) $y - x = 13, y^2 + xy + x^2 = 7$ Kvadratická rovnice v tomto případě nemá reálné řešení.

(d) $y - x = 91, y^2 + xy + x^2 = 1$ Kvadratická rovnice v tomto případě nemá reálné řešení.

Dostali jsme tedy řešení $(5, 6), (-6, -5), (-3, 4)$ a $(-4, -3)$.

3. Levou stranu rozložíme na $x(x+1) = y^3$. Protože $x, x+1$ jsou nesoudělná, vidíme, že $x$, $x+1$ musí být oba třetí mocniny celých čísel. Přitom pokud $n \geq 1$, tak $(n+1)^3 - n^3 = 3n^2 + 3n + 1 > 1$, podobně $n \leq -2$ implikuje $(n+1)^3 - n^3 > 1$. Nutně tedy nemůže být $x \geq 1$ ani $x \leq -2$. Zbývají tedy možnosti $x = 0$ resp. $x = -1$, pro které snadno dopočítáme $y = 0$.

**Příklad 4.** Buď $x, y \in \mathbb{Z}$ řešení rovnice $x^2 + 1 = y^3$. Dokažte, že:

1. Čísla $x + i$ a $x - i$ jsou v $\mathbb{Z}[i]$ nesoudělná.
2. Výraz $x \pm i$ je v $\mathbb{Z}[i]$ třetí mocnina nějakého prvku.
3. Jediné $x$ splňující, že $x + i$ je třetí mocnina v $\mathbb{Z}[i]$, je $x = 0$.

*Řešení:*

1. Odečtením dostaneme $(x + i, x - i) = (2i, x + i)$, přitom $2i$ a 2 jsou asociované, tedy v úvahu přichází pouze dělitelé dvojky. V $\mathbb{Z}[i]$ máme rozklad dvojky na prvočinitele $2 = -i(1 + i)^2$. Podívejme se, zda $1 + i$ dělí $x + i$. Pokud ano, tak $x$ musí být liché, protože z $(a+ib)(1+i) = x+i$ dostaneme soustavu

$$\begin{aligned} a - b &= x \\ a + b &= 1, \end{aligned}$$

z níž plyne $2a = x + 1$. Tedy $x = 2a - 1$. Dosaďme do rovnice $x^2 + 1 = y^3$. Máme $(2a - 1)^2 + 1 = y^3$, čili $4a^2 - 4a + 2 = y^3$, z čehož plyne $y^3 \equiv 2 \pmod 4$. Ovšeme žádná třetí mocnina celého čísla není modulo 4 kongruentní 2, spor.

Podobně se dokáže, že ani $1 - i$ není dělitel $x + i$. Proto $(x + i, x - i) = 1$.

2. Protože $(x+i)(x-i)$ je třetí mocnina a oba činitelé jsou nesoudělní, musí být každý z nich třetí mocnina.

3. Hledáme $a, b \in \mathbb{Z}$, že $x + i = (a + ib)^3$, vyčíslením imaginární části dostaneme diofantickou rovnici

$$1 = 3ba^2 - b^3$$
$$1 = b(3a^2 - b^2)$$

Nutně $b = \pm 1$, tedy $3a^2 - 1 = \pm 1$, čili $3a^2 = 0$ nebo $3a^2 = 2$. Z těchto možností má celočíselné řešení jenom ta první, tedy $a = 0$, načež dosazením do původní rovnice dostaneme $x = 0$.

Vidíme, že pokud je $(x, y) \in \mathbb{Z}^2$ řešení rovnice $x^2 + 1 = y^3$, tak $x = 0$ a nutně pak $y = 1$.

**Příklad 5.** Vyřešte v $\mathbb{Z}$ rovnice $x^2 + 2 = y^3$ a $x^2 + 4 = y^3$.

*Řešení:* První rovnici budeme řešit přechodem do $\mathbb{Z}[\sqrt{2}i]$, což je euklidovský obor integrity. Máme $(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3$. Spočtěme $(x + \sqrt{2}i, x - \sqrt{2}i) = (x + \sqrt{2}i, 2\sqrt{2}i)$. V úvahu přicházejí prvočinitel v rozkladu $2\sqrt{2}i = -(\sqrt{2}i)^3$, tedy $\sqrt{2}i$. Nechť tedy $\sqrt{2}i(a + ib) = x + \sqrt{2}i$. Pak $x = -\sqrt{2}b$ není celé číslo.

Vidíme tedy, že $x + \sqrt{2}i$ je třetí mocnina v $\mathbb{Z}[\sqrt{2}i]$. Kolik je takových třetích mocnin? Buď $x + \sqrt{2}i = (a + i\sqrt{2}b)^3$, potom snadno dopočítáme:

$$1 = 3ba^2 - 2b^3 = b(3a^2 - 2b^2)$$

z čehož $b = \pm 1$, tedy $3a^2 - 2 = \pm 1$, což má celočíselné řešení $a = \pm 1$, které už implikuje $x = a^3 - 6ab^2 = \pm 5$. Řešení jsou tedy dvě: $(x, y) = (5, 3)$ a $(-5, 3)$.

Druhou rovnici prozkoumáme opět v $\mathbb{Z}[i]$. Máme $(x+2i)(x-2i) = y^3$. Přitom $(x + 2i, x - 2i) = (x + 2i, 4)$. V úvahu tedy přicházejí opět mocniny $1 + i$. Pokud jsou $x \pm 2i$ nesoudělná, tak nutně obě čísla musí být třetí mocniny. Ukážeme, že pokud $1 + i | x + 2i$, tak $(x \pm 2i)/(1 + i)^3$ leží v $\mathbb{Z}[i]$ a jsou nesoudělná. I v tomto případě proto budou $x \pm 2i$ třetí mocniny v $\mathbb{Z}[i]$.

Nechť $x + 2i = (a + bi)(1 + i) = a - b + i(b + a)$. Potom je $x$ sudé, tedy $y$ musí být také sudé. Pišme $x = 2x', y = 2y'$. Máme rovnici $4x'^2 + 4 = 8y'^3$, čili

$$x'^2 + 1 = 2y'^3.$$

Počítáním modulo 2 zjistíme, že $x'$ musí být liché. Podívejme se na $(x' + i, x' - i) = (x + i, 2)$. V úvahu proto přicházejí pouze dělitelé 2, tedy mocniny $(1 + i)$. Rozmyslete si, že protože $x'$ je liché, tak $1 + i | x' \pm i$, ale $2 \nmid x' + i$. Tedy $(x' + i, x' - i) = 1 + i$. Potom budeme mít dvě nesoudělná čísla v $\mathbb{Z}[i]$:

$$\frac{x' \pm i}{(1 + i)} = \frac{x \pm 2i}{2(1 + i)} = i\frac{x \pm 2i}{(1 + i)^3}.$$

Pokud $x \pm 2i$ jsou třetí mocniny, tak $x + 2i = (a + ib)^3$, tedy nutně

$$x = a^3 - 3ab^2 2 = 3a^2 b - b^3$$

Z druhé rovnice opět dostaneme dvě možnosti $b = \pm 1$ a $b = \pm 2$. V prvním případě dopočítáme řešení $(x, y) = (\pm 2, 2)$, ve druhém $(\pm 11, 5)$.

Poznámka: Ne všechny diofantické rovnice jsou takto pěkně řešitelné (protipříklad: Velká Fermatova věta). Obecná rovnice $x^2 = y^3 + k$ je známá jako Mordellova (nebo také Bachetova) rovnice.

**Příklad 6** (Obecná Pellova rovnice)**.** Buď $d > 0$ nečtvercové celé číslo. Označme $G$ množinu všech kladných čísel $a + \sqrt{d}b$, že $a, b \in \mathbb{Z}$ a platí $a^2 - db^2 = 1$. Předpokládejme, že $G$ obsahuje aspoň jeden prvek různý od 1 (tak tomu vždy je). Dokažte:

1. $G$ s násobením zděděným z $\mathbb{R}$ tvoří grupu
2. $G$ je nekonečná cyklická grupa

*Řešení:* Celý problém je elementárně vyřešený ve skriptech prof. Klazara „Úvod do teorie čísel“ na adrese

`http://kam.mff.cuni.cz/~klazar/ln_utc.pdf`

My si zde jenom všimneme, že $G$ je „polovina“ množiny všech invertibilních prvků okruhu $\mathbb{Z}[\sqrt{d}]$ (ta druhá jsou prvky $a+\sqrt{d}b < 0$, grupa $\mathbb{Z}[\sqrt{d}]^\star$ je isomorfní $\mathbb{Z}_2 \times \mathbb{Z}$).