# Teorie čísel: Cvičení 7 – výsledky a vybraná řešení

28. března 2022

**Web:** https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
**Email:** raska.martin@gmail.com

## Výsledky:

-2. Jediné řešení je $(0, 1)$. Podrobné řešení je popsáno níže.

0. Až na záměnu $x, y$ jsou všechna kladná různá řešení tvaru $x = (a^2 - b^2)c$, $y = 2abc$, $z = (a^2 + b^2)c$ pro libovolné celé $c > 0$ a libovolná celá $a > b > 0$, která jsou nesoudělná a opačné parity. Libovolné řešení, kdy je nějaká z proměnných záporná dostaneme změnou znamének z těchto. Pokud je alespoň jedna z proměnných 0, tak si množinu řešení též rozmyslíme snadno. Podrobné řešení je popsáno níže.

1. Jediným řešením je $(0, 1)$, postup je velmi podobný příkladu -2.

3. a) $\pm 1$

   b) Jednotky jsou přesně všechna řešení Pellových rovnic $x^2 - 2y^2 = \pm 1$. Jdou tak souhrně zapsat jako $\pm(1 + \sqrt(2))^n$, $n \in \mathbb{Z}$, neboť $1 + \sqrt{2}$ je minimálním řešením rcex $x^2 - 2y^2 = -1$.

4. Řešení uvedené rovnice odpovídají přesně právě prvkům s normou $A$. Multiplikativita normy nám v řeči Pellových rovnic říká, že pokud máme řešení $x_1 + y_1\sqrt{D}$ rovnice $x^2 - Dy^2 = A$ a řešení $x_2 + y_2\sqrt{D}$ rovnice $x^2 - Dy^2 = B$, tak číslo $(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D})$ je řešením rovnice $x^2 - Dy^2 = AB$.

5. $x = a(a^2 - 3b^2)$, $y = b(3a^2 - b^2)$, $z = a^2 + b^2$, pro $a, b \in \mathbb{Z}$ nesoudělná a opačné parity. Postup je velmi podobný příkladu 0.

6. Řešení jsou $(\pm 2, 2)$ a $(\pm 11, 5)$. Oproti předchozím příkladům se zde může stát, že jsou činitelé nalevo v $(x + 2i)(x - 2i) = y^3$ soudělní, pokud jsou $x$ a $y$ obě sudé. V takovém případě se rovnice po substituci $x = 2x_1$, $y = 2y_1$ převede do tvaru $(x_1 + i)(x_1 - i) = x_1^2 + 1 = 2y_1^3$ pro lichá $x_1, y_1$. Není těžké ukázat, že největší společný dělitel závorek nalevo je právě $1 + i$ s pomocí čehož už jde úloha vyřešit ($\frac{x_1+i}{1+i}$ musí být v důsledku třetí mocninou nějakého prvku $\mathbb{Z}[i]$).

7. $(\pm 1, 1)$. Řešte v oboru $\mathbb{Z}[\sqrt{2}]$. Ten sice obsahuje nekonečně jednotek pro $\varepsilon = \pm(1 + \sqrt{2})^n, n \in \mathbb{Z}$ stačí u výrazu $\varepsilon(a + b\sqrt{2})^3$ uvažovat pouze $\varepsilon = (1 + \sqrt{2})^k$, $k \in \{0, 1, 2\}$, zbytek se schová do třetí mocniny.

8. Nemá řešení. Postupujte obdobně jako v příkladě 6. V druhém kroku je třeba rozlišit, ke kterému faktoru nalevo se přidá prvočinitel 3, který na pravé straně přibyl.

9. $(0, -1)$, $(\pm 1, 0)$, $(\pm 3, 2)$. Rovnice jde s trochou snahy a trpělivosti vyřešit přímo nad celými čísly.

10. Zkuste např. 4 rozložit na součin.

11. Zmíněný obor se nazývá Eisensteinova celá čísla. Důkaz Eukleidovskosti jde provést například typickým geometrickým argumentem (a jde dohledat např. na anglické Wikipedii). K samotné rovnici se pak na začátek hodí rozebrat paritu a uvážit rozklad nad tímto oborem. Dá se ukázat, že závorky nalevou jsou nesoudělné a ukáže se, že rovnice nemá v $\mathbb{Z}$ řešení. (V tomhle příkladě se často hodí použít modulo 9.)

Pokud byste se o řešení diofantických rovnic chtěli dozvědět více, můžete se kouknout na diplomku Maroše Hrnčiara (většina informací v ní je přirozeně nad rámec tohoto předmětu).

## Vybraná vzorová řešení:

**-2.)** Předpokládejme, že dvojice $(x, y)$ řeší zadanou rovnici a uvažme rozklad $(x + i)(x - i) = y^5$ v gaussovském oboru $\mathbb{Z}[i]$. Nejprve ukážeme, že $x + i$ a $x - i$ jsou v $\mathbb{Z}[i]$ nesoudělná. Pokud by je pro spor nějaký prvočinitel $\pi$ dělil, tak musí dělit i jejich rozdíl, tj. $\pi \mid 2i \parallel 2 \parallel (1 + i)^2$ (neboť $i$ je jednotka a

víme, jak v $\mathbb{Z}[i]$ vypadá rozklad 2). Protože jsme v gaussovském oboru, tak už nutně $\pi \parallel (1+i)$ a BÚNO můžeme předpokládat $\pi = 1+i$ (v dalším postupu a při uvažování dělitelností nebude přenásobení jednotkou podstatné). Speciálně tak dostaneme v $\mathbb{Z}[i]$ dělitelnost

$$2 \parallel (1+i)^2 = \pi^2 \mid (x+i)(x-i) = y^5.$$

Tedy 2 dělí $y^5$ v $\mathbb{Z}[i]$. To nicméně podle příkladu 6. z minulého cvičení implikuje, že 2 dělí $y^5$ i v $\mathbb{Z}$, a nutně pak $2 \mid y$ (neboť je 2 v $\mathbb{Z}$ prvočinitel). Když se nyní podíváme na rovnici modulo 4, tak dostaneme $x^2 \equiv 3 \pmod 4$. To se nicméně nemůže stát pro žádné $x \in \mathbb{Z}$ a tak máme spor. Prvky $x+i$ a $x-i$ jsou tak skutečně nesoudělné.

Nyní uvažme rozklady na prvočinitele výrazu $(x+i)(x-i) = y^5$. Pro všechny prvočinitele $p$ jsou $p$-valuace čísla $y^5$ násobky pěti, to stejné tak musí platit i pro $(x+i)$ a $(x-i)$, neboť pokud by se mocniny nějakého prvočinitele netriviálně rozdistribuovali mezi oba prvky, tak by to byl spor s nesoudělností. Můžeme tak psát $x+i \parallel (a+bi)^5$ pro nějaké $a, b \in \mathbb{Z}$. Speciálně tedy $x+i = \varepsilon(a+bi)^5$ pro některé $\varepsilon \in \{\pm 1, \pm i\}$, což jsou všechny jednotky v $\mathbb{Z}[i]$. Abychom si nyní ulehčili práci s rozborem, tak si můžeme všimnout, že $\varepsilon^5 = \epsilon$ a tedy pokud označíme $\varepsilon(a+bi) = c+di$ pro vhodná $c, d \in \mathbb{Z}$, tak dostaneme

$$x+i = \varepsilon(a+bi)^5 = \varepsilon^5(a+bi)^5 = (\varepsilon(a+bi))^5 = (c+di)^5 = c^5 + 5c^4di - 10c^3d^2 - 10c^2d^3i + 5cd^4 + d^5i$$

.

Porovnáním reálných a imaginárních částí dostaneme $x = c^5 - 10c^3d^2 + 5cd^4$ a $1 = 5c^4d - 10c^2d^3 + d^5 = d(5c^4 - 10c^2d^2 + d^4)$. Nutně tedy musí platit $d \mid 1$, což povoluje pouze $d = \pm 1$.

V případě $d = 1$ z druhé rovnice dostaneme $1 = 5c^4 - 10c^2 + 1$, což implikuje $c = 0$ a z první rovnosti tak máme $x = 0$. Dosazením do zadání zjistíme, že jediný možný výsledek je v tomto případě $(0, 1)$.

V případě $d = -1$ se snadno přesvědčíme, že rovnice $1 = 5c^4d - 10c^2d^3 + d^5$ nemá nad $\mathbb{Z}$ řešení.

Jediné řešení je tak $(x, y) = (0, 1)$ (které zároveň splňuje zkoušku).

**0.)** Na začátku si uvědomme, že můžeme předpokládat, že $x, y, z$ jsou po dvou nesoudělná čísla. Pokud by totiž nějaké prvočíslo $p$ dělilo dvě z nich, tak ze zadané rovnosti musí dělit i to třetí. A můžeme si všimnout, že vedle trojice $(x, y, z)$ je pak řešením i trojice $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p}\right)$. Tedy z nesoudělných řešení můžeme nazávěr vygenerovat i všechna soudělná tak, že je jednoduše přenásobíme vhodným kladným celým číslem. Zároveň předpokládejme, že jsou $x, y, z$ nezáporná, neboť jsou proměnné v rovnici v druhé mocnině a libovolné záporné hodnoty by byly řešením taky. Pokud je jedna z proměnných nula, tak si snadno rozmyslíme, že dostáváme řešení tvaru $(0, 0, 0)$, $(a, 0, a)$ a $(0, a, a)$ pro $a > 0, a \in \mathbb{Z}$. Odteď se tedy omezme pouze na kladná nesoudělná řešení.

Nyní uvažme v $\mathbb{Z}[i]$ rozklad $(x+iy)(x-iy) = z^2$. Na začátek opět ukážeme, že jsou členy $x+iy$ a $x-iy$ nesoudělné. Pokus by je pro spor dělil nějaký prvočinitel $\pi$, tak dělí i jejich součet a rozdíl, tedy $\pi \mid 2x$ a $\pi \mid 2iy \parallel 2y$. Rozeberme dva případy:

1. $\pi \mid 2$. Podobně jako v případě $-2$ můžeme BÚNO předpokládat, že $\pi = 1+i$ a dostaneme, že $2 \mid x^2 + y^2 = z^2$ a tedy $2 \mid z^2$, jak v $\mathbb{Z}[i]$, tak v $\mathbb{Z}$. Tedy $2 \mid z$ a při pohledu na původní rovnici modulo 4 dostaneme $x^2 + y^2 \equiv 0 \pmod 4$. Ovšem vzhledem k tomu, že druhé mocniny můžou modulo 4 dávat zbytek pouze 0 nebo 1, tak to implikuje, že $x^2 \equiv y^2 \equiv 0 \pmod 4$. Tudíž jsou $x$ i $y$ sudé a dostáváme spor s jejich nesoudělností.

2. $\pi \nmid 2$ Pak z výše uvedeného $\pi \mid x$ a $\pi \mid y$. Jde si ale rozmyslet (například přes Bézoutovu rovnost nebo prvočinitele), že dvě celá čísla jsou v $\mathbb{Z}[i]$ nesoudělná právě tehdy, když jsou nesoudělná v $\mathbb{Z}$. Tedy opět dostáváme spor s předpokládanou nesoudělností.

Vidíme tedy, že $x+iy$ a $x-iy$ jsou nesoudělné a analogicky platí $x+iy = \varepsilon(a+bi)^2$ pro nějaká $a, b \in \mathbb{Z}$ a jednotku $\varepsilon$. Speciálně si můžeme všimnout, že $-\varepsilon(a+bi)^2 = \varepsilon(i(a+bi))^2$. Stačí tedy uvažovat $\varepsilon \in \{1, i\}$. Tyto případy rozeberme:

1. $\varepsilon = 1$. Pak porovnáním dostaneme $x = a^2 - b^2$ a $y = 2ab$, což po dosazení zpátky do zadání dá $z = a^2 + b^2$.

2. $\varepsilon = i$. Pak $x = -2ab$ a $y = a^2 - b^2$, což opět po dosazení dá $z = a^2 + b^2$.

Vidíme, že oba případy se liší pouze prohozením proměnných $x$ a $y$ a záměnou znamének. Předpokládejme tedy BÚNO $x = a^2 - b^2$, $y = 2ab$ a $z = a^2 + b^2$. Zbývá rozebrat, za jakých podmínek jsou $x$ a $y$ kladné a nesoudělné. Ne příliš složitým rozborem vyjde, že se to stane právě tehdy když $a > b > 0$, $a$ a $b$ jsou nesoudělná a mají různou paritu. Zároveň jde ověřit, že pro fixní $x$ a $y$ už jsou $a$,$b$ za těchto podmínek určena jednoznačně, a tak jsou všechna tato nalezená řešení vzájemně disjunktní. Abychom dostali i soudělná řešení, tak jednoduše můžeme pronásobit všechny proměnné nějakou konstantou $c > 0$, která bude udávat jejich výsledného největšího společného dělitele.

Dohromady tak dostáváme, že všechny disjunktní kladné řešení jsou právě tvaru $x = (a^2 - b^2)c$, $y = 2abc$ a $z = (a^2 + b^2)c$ pro libovolné $c > 0$, $a > b > 0$, kde $a$, $b$ jsou nesoudělné a různé parity.

### Doplňující poznámky k předchozímu postupu:

- Zásadní věc, která umožňovala předchozí postup, byla gaussovskost oboru $\mathbb{Z}[i]$, nad kterým jsme výraz rozkládali na součin. To nám povolovalo se získanými rovnostmi a dělitelnostmi rozumně pracovat. Obecně tedy tento postup bude dobře fungovat nad obory, které jsou gaussovské (občas si vystačíme čistě se $\mathbb{Z}$). Zdaleka ne všechna kvadratická rozšíření $\mathbb{Z}[\sqrt{D}]$ to ale splňují. Občas pomůže (z dobrých důvodů, které ale v tomhle předmětu nejspíše neuvidíme) uvažovat obor $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, občas ale gaussovskost jen tak nezískáme a musíme si pomoct jinými sofistikovanějšími metodami.

- Další krok, který ne vždycky funguje, je nesoudělnost výrazů v součinu. Ne vždycky výrazy skutečně musí být nesoudělné, občas je třeba rozbor nebo další omezující podmínky. Ale pokud zvládneme největší společný dělitel nějak omezit nebo vypočítat, tak to není neřešitelný problém. Příkladem může být úloha 6. Dále se hodí poznamenat, že pro důkaz nesoudělnosti se často hodí dívat se na výrazy modulo nějakou mocninu prvočísla.

- V příkladu $-2$ výše se nám podařilo jednotku vždy umístit dovnitř páté odmocniny a ušetřit si tak práci s rozborem 4 případů. Obecně se nám to nemusí vždy povést a nějaký rozbor bude třeba udělat (viz např. úloha 0). Ale vyplatí se předem zredukovat možnosti co nejvíce, abychom si ušetřili práci :)

- Příklad 7. ukazuje další záludnost, kterou je u reálných kvadratických rozšíření ($\mathbb{Z}[\sqrt{D}], D > 0$) nekonečný počet jednotek. Ale podobně jako v příkladu 7 jde tato věc typicky vyřešit.

- V neposlední řadě se nám může stát, že při porovnání na konci dostaneme nějakou diofantickou rovnici, u které nemusí být zjevné, jak ji řešit. Jedním z příkladů může být rovnice uvedená v poznámce u úlohy 7. Pro zajímavost tato rovnice (a mnoho dalších, které v podobných situacích vznikají) patří do rodiny Thueho rovnic a jsou známy metody, jak je řešit.

  Prakticky všechny tyto poznámky jsou přirozeně nad rámec tohoto kurzu, ale prezetují alespoň některé záludnosti, se kterými se člověk může při řešení podobných diofantických rovnic potkat. Pokud byste se o řešení diofantických rovnic chtěli dozvědět více, můžete se kouknout na diplomku Maroše Hrnčiara.