Teorie čísel: Cvičení 10 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Nápovědy:

-2. Počítejte v $\mathbb{Z}[\mathrm{i}]$. Postup bude předveden; pokud takový příklad vidíte poprvé, není snadné si postup rozmyslet samostatně.

-1. Proveďte dělení v $\mathbb{Q}(\sqrt{2})$ a výsledek po složkách „zaokrouhlete“ do $\mathbb{Z}[\sqrt{2}]$. Uvědomte si, že zaokrouhlovací bordel po přenásobení dělitelem musí ležet v $\mathbb{Z}[\mathrm{i}]$, takže zbývá dokázat, že má malou normu.

0. Opět počítejte v $\mathbb{Z}[\mathrm{i}]$. Práci výrazně usnadní, když budete hledat jen řešení s nesoudělnými x, y, z (a na závěr si rozmyslíte, jak z nich získat i soudělná řešení). Navíc si před prací v $\mathbb{Z}[\mathrm{i}]$ rozmyslete, jakou paritu mohou jednotlivá čísla mít. Pak už je postup podobný jako v příkladu -2.

1. Opět pracujte v $\mathbb{Z}[\mathrm{i}]$; použijte obdobný postup a navíc pro usnadnění i velmi podobné triky jako v příkladu -2.

2. Lze použít geometrický náhled podobný důkazu eukleidovskosti $\mathbb{Z}[\mathrm{i}]$ nebo přímočarou analogii postupu předvedeného u příkladu -1.

3. Využijte normu. Část a) je triviální, část b) vede na Pellovu rovnici.

4. Rovnici lze interpretovat jako hledání prvků $\mathbb{Z}[\sqrt{D}]$ s jistou vlastností. Multiplikativita říká něco o množině pravých stran, pro něž existuje řešení.

5. Jde o zobecnění příkladu 1., postupujte obdobně. Nakonec nezapomeňte zajistit, že získaná x, y jsou skutečně nesoudělná.

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

7. Řešte v oboru $\mathbb{Z}[\sqrt{2}]$. Ten sice obsahuje nekonečně mnoho jednotek, ale větší část z nich se dá schovat do třetí mocniny; k rozebrání zbudou tři případy.

8. Postupujte obdobně jako v příkladě 6. Ve 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 nalevo jsou nesoudělné, a ukáže se, že rovnice nemá v $\mathbb{Z}$ řešení. (V tomhle příkladě se často hodí použít modulo 9.)

Výsledky:

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

-1. Lze dokázat, že jako eukleidovská norma poslouží absolutní hodnota klasické normy $\mathrm{N}(a + b\sqrt{2}) = a^2 - 2b^2$.

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 celé $c > 0$ a nesoudělná celá $a > b > 0$, z nichž je právě jedno sudé. Libovolné řešení, kdy je nějaká z proměnných záporná, dostaneme změnou znamének z už uvedených. Pokud je alespoň jedna z proměnných 0, tak si množinu řešení též rozmyslíme snadno.

1. Jediným řešením je $(0, 1)$.

2. Opět poslouží klasická norma, tentokrát ani není potřeba brát absolutní hodnotu.

3. a) Pouze ± 1.

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

4. Řešení uvedené rovnice odpovídají 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 $x^2 - Dy^2 = AB$. Krátce řečeno, množina pravých stran, pro něž existuje řešení, je uzavřená na násobení.

5. Řešení jsou právě $x = a(a^2 - 3b^2)$, $y = b(3a^2 - b^2)$, $z = a^2 + b^2$ pro $a, b \in \mathbb{Z}$ nesoudělná a opačné parity.

6. Řešení jsou $(\pm 2, 2)$ a $(\pm 11, 5)$.

7. Pouze $(\pm 1, 1)$.

8. Nemá řešení.

9. $(0, -1)$, $(\pm 1, 0)$, $(\pm 3, 2)$.

11. Rovnice nemá řešení.

Vybraná vzorová řešení:

-2.) Předpokládejme, že dvojice (x, y) řeší zadanou rovnici, a uvažme rozklad $(x + \mathrm{i})(x - \mathrm{i}) = y^5$ v gaussovském oboru $\mathbb{Z}[\mathrm{i}]$. Nejprve ukážeme, že $x + \mathrm{i}$ a $x - \mathrm{i}$ jsou v $\mathbb{Z}[\mathrm{i}]$ nesoudělná. Pokud by je pro spor nějaký prvočinitel π dělil, tak musí dělit i jejich rozdíl, tj. $\pi \mid 2\mathrm{i} \parallel 2 \parallel (1 + \mathrm{i})^2$ (neboť i je jednotka a víme, jak v $\mathbb{Z}[\mathrm{i}]$ vypadá rozklad 2). Protože jsme v gaussovském oboru, tak už nutně $\pi \parallel (1 + \mathrm{i})$ a BÚNO můžeme předpokládat $\pi = 1 + \mathrm{i}$ (v dalším postupu a při uvažování dělitelností nebude přenásobení jednotkou podstatné). Speciálně tak dostaneme v $\mathbb{Z}[\mathrm{i}]$ dělitelnost

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

Tedy 2 dělí y^5 v $\mathbb{Z}[\mathrm{i}]$. **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 $x + \mathrm{i}$ a $x - \mathrm{i}$ jsou tak skutečně nesoudělné.

Nyní uvažme rozklady na prvočinitele výrazu $(x + \mathrm{i})(x - \mathrm{i}) = y^5$. Pro všechny prvočinitele p jsou p-valuace čísla y^5 násobky pěti. Totéž musí platit i pro $(x + \mathrm{i})$ a $(x - \mathrm{i})$, neboť pokud by se mocniny některého prvočinitele netriviálně rozdistribuovaly mezi oba prvky, nebyly by tyto prvky nesoudělné. Můžeme tak psát $x + \mathrm{i} \parallel z^5$ pro nějaké $z \in \mathbb{Z}[\mathrm{i}]$. To znamená $x + \mathrm{i} = \varepsilon z^5$ pro některé $\varepsilon \in \{\pm 1, \pm \mathrm{i}\}$, což jsou všechny jednotky v $\mathbb{Z}[\mathrm{i}]$. Abychom si nyní ulehčili práci s rozborem, všimneme si, že čtvrtá mocnina každé jednotky v $\mathbb{Z}[\mathrm{i}]$ je 1, takže $\varepsilon^5 = \varepsilon$. Proto $x + \mathrm{i} = (\varepsilon z)^5$, tj. $x + \mathrm{i}$ je pátá mocnina nějakého Gaussova celého čísla. Označme $\varepsilon z = a + b\mathrm{i}$ pro $a, b \in \mathbb{Z}$. Dostaneme

$$x + \mathrm{i} = (a + b\mathrm{i})^5 = a^5 + 5a^4b\mathrm{i} - 10a^3b^2 - 10a^2b^3\mathrm{i} + 5ab^4 + b^5\mathrm{i} = (a^5 - 10a^3b^2 + 5ab^4) + (5a^4b - 10a^2b^3 + b^5)\mathrm{i}.$$

Porovnáním reálných a imaginárních částí dostaneme $x = a^5 - 10a^3b^2 + 5ab^4$ a $1 = 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4)$. Nutně tedy $b = \pm 1$.

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

V případě $b = -1$ se snadno přesvědčíme, že rovnice $-1 = 5a^4 - 10a^2 + 1$ nemá nad $\mathbb{Z}$ řešení – nemá totiž řešení ani modulo 5.

Jediným řešením původní rovnice proto je $(x, y) = (0, 1)$. (Dosazením ověříme, že skutečně jde o řešení.)

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

1. $\pi \mid 2$. Podobně jako v případě -2 můžeme BÚNO předpokládat, že $\pi = 1 + \mathrm{i}$ a dostaneme, že $2 \mid x^2 + y^2 = z^2$ a tedy $2 \mid z^2$, jak v $\mathbb{Z}[\mathrm{i}]$, 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 mohou 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 $\mathbb{Z}[\mathrm{i}]$ nesoudělná právě tehdy, když jsou nesoudělná v $\mathbb{Z}$. Tedy opět dostáváme spor s předpokládanou nesoudělností.

Vidíme tedy, že $x + y\mathrm{i}$ a $x - y\mathrm{i}$ jsou nesoudělné a analogicky platí $x + y\mathrm{i} = \varepsilon(a + b\mathrm{i})^2$ pro nějaká $a, b \in \mathbb{Z}$ a jednotku ε. Speciálně si můžeme všimnout, že $-\varepsilon(a + b\mathrm{i})^2 = \varepsilon(\mathrm{i}(a + b\mathrm{i}))^2$. Stačí tedy uvažovat $\varepsilon \in \{1, \mathrm{i}\}$. 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. $\varepsilon = \mathrm{i}$. 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. Nepříliš 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 $\mathbb{Z}[\mathrm{i}]$, 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 $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, viz příklad 11. Často ale gaussovskost vůbec nelze zaručit a musíme si pomoct jinými sofistikovanějšími metodami. Ochutnávku můžete potkat na předmětu Algebraická teorie čísel.

- Další krok, který ne vždycky funguje, je nesoudělnost výrazů v součinu. Ne vždycky výrazy skutečně musejí 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 čtyř 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 demonstrují alespoň některé ze záludností, s nimiž 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.