Gaussova prvočísla

Kuba Krásenský

Abstrakt. Stejně jako z reálných čísel jsou svým způsobem nejzajímavější čísla celá, i v komplexních číslech existuje pozoruhodná podmnožina. Jsou to Gaussova čísla – komplexní čísla, jejichž reálná i imaginární část jsou celé. Tato množina tvoří v Gaussově rovině čtvercovou mřížku. Ukazuje se, že i mezi těmito čísly jsou některá, která se nedají zapsat jako součin dvou jiných – Gaussova prvočísla. Na přednášce zjistíme, která to jsou, přičemž využijeme různé znalosti z teorie čísel. Na závěr nám nabyté znalosti pomohou vyřešit několik diofantických rovnic.

Komplexní čísla

V tomto odstavci shrnu základní informace o komplexních číslech. Bylo by dobré, kdyby je přibližně znal každý, kdo na přednášku půjde.

Imaginární jednotka i je „druhá odmocnina z mínus jedné“. Tím myslíme, že platí $i^2 = -1$. Imaginární jednotka není reálné číslo; je to jedno z čísel *komplexních*. Komplexní číslo je potom každé číslo tvaru $a + bi$. Koeficientům a, resp. b říkáme *reálná*, resp. *imaginární část* komplexního čísla. Můžeme je (jako každou dvojici bodů) vynášet do roviny. Na ose x budou ležet reálná čísla, na ose y čísla *ryze imaginární*. A třeba číslo $2 + 2i$ bude ležet na ose prvního kvadrantu.

Díky této geometrické představě definujeme *velikost* komplexního čísla z jako $|z| = \sqrt{a^2 + b^2}$. Vidíme, že $|z|$ odpovídá velikosti úsečky spojující bod (a, b) s nulou (počátkem souřadnic). Známe-li tuto definici, můžeme každé komplexní číslo z vyjadřit také ve tvaru $|z| \cdot (\cos\varphi + i \sin\varphi)$. Zde φ označuje úhel, který svírá spojnice počátku a bodu (a, b) s reálnou osou.

Díky tomu, že víme, kolik je i^2, už umíme násobit dvě komplexní čísla. A sčítat je, to je samozřejmě ještě snazší:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Na přednášce budeme také potřebovat pojem *komplexně sdruženého* čísla $\overline{a + bi} = a - bi$.

Tvrzení. *Pro libovolná komplexní čísla z_1, z_2, z platí:*

(i) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,

(ii) $|z|^2 = z \cdot \overline{z}$,
(iii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

Střípky z teorie čísel

Abychom dokázali některá tvrzení o Gaussových číslech, musíme ovládat určité postupy z teorie čísel. Tady budeme mít potřebné znalosti pěkně pohromadě.

Definice. Říkáme, že celá čísla a a b jsou kongruentní modulo d, pokud dávají stejný zbytek po dělení d. To znamená $d \mid (a - b)$. Kongruenci zapisujeme $a \equiv b \pmod{d}$.

Poznámka. S kongruencemi se stejným modulem lze počítat prakticky stejně jako s rovnicemi.

Tvrzení. *Pro každé celé číslo a platí $a^2 \equiv 0$ nebo $a^2 \equiv 1 \pmod{4}$.*

Předchozí tvrzení se často formuluje slovy „nula a jednička jsou *kvadratické zbytky* modulo čtyři“. Je jednoduché jej dokázat – stačí postupně umocnit na druhou výrazy $4k$, $4k + 1$, $4k + 2$ a $4k + 3$.

Věta. (Wilsonova) *Jestliže je p prvočíslo, pak platí*

$$(p - 1)! \equiv -1 \pmod{p}.$$

Důkaz rád předvedu na konzultaci nebo v jakékoliv volné chvíli. Na přednášce na něj nebude čas.

Gaussova čísla

Definice. Komplexní číslo, jehož reálná i imaginární část jsou celá čísla, nazveme *Gaussovým celým číslem*.

Definice. *Normou* Gaussova čísla nazveme druhou mocninu jeho velikosti. Značíme $N(a + bi) = |a + bi|^2 = (a + bi) \cdot (\overline{a + bi}) = a^2 + b^2$.

Norma má tu příjemnou vlastnost, že je to vždy přirozené číslo (nebo nula). To se využívá například při důkazech matematickou indukcí. Navíc platí klíčová vlastnost, kterou si snadno dokážete:

Tvrzení. *Pro každá Gaussova čísla a, b platí*

$$N(ab) = N(a) \cdot N(b).$$

Je důležité si rozmyslet, že Gaussova čísla jsou *uzavřená na sčítání a násobení* – součet i součin dvou Gaussových čísel je Gaussovo číslo. Podobné tvrzení platí pro celá čísla. Ani jedna z těchto množin ale není uzavřená na dělení. $5/2$ není celé číslo a není to ani Gaussovo číslo. Stejně jako v obyčejných celých číslech proto definujeme dělitelnost.

Definice. Říkáme, že a *je dělitelné* b, pokud existuje k takové, že $a = b \cdot k$. Také čteme „b dělí a“ a značíme $b \mid a$.

Cvičení. Dokažte, že pokud $a \mid b$, pak i $N(a) \mid N(b)$.

Cvičení. Jak poznáme, že je reálné celé číslo a dělitelné $1+i$? Jak poznáme, že je tímto číslem dělitelné $a+bi$?

Definice. *Jednotkami* nazveme Gaussova čísla normy jedna, tedy $\pm 1, \pm i$.

Úloha. (Na dlouhé zimní večery)

(i) Rozmyslete si, jak by se v Gaussových číslech dalo definovat dělení se zbytkem, a zkuste si ujasnit, proč dělení se zbytkem bude fungovat. Nápověda: Použijte normu zbytku po dělení. Pro důkaz využijte názorné geometrické představy.
(ii) Přeformulujte Eukleidův algoritmus pro Gaussova čísla a dokažte, že funguje.
(iii) Dokažte Bézoutovu větu.
(iv) Použijte předchozí výsledky k dokázání *klíčového tvrzení* z následující kapitoly.
(v) A pak už si snadno dorozmyslete, jak dokázat jednoznačnost rozkladu na prvočísla.

Prvočísla

Definice. Číslo p nazveme *Gaussovým prvočíslem*, pokud platí: Kdykoliv $p = a \cdot b$, pak buď a, nebo b je jednotka.

Tato definice sice zní trochu krkolomně, ale říká totéž jako běžná definice prvočísla. Existuje ale ještě druhý způsob, jak prvočíslo definovat:

Tvrzení. (Klíčové) *Číslo p je prvočíslo právě tehdy, když platí: Kdykoliv $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.*

Cvičení. Zkuste rozložit čísla 2, $2+2i$, 3, $3+i$ a 5 na Gaussova prvočísla.

Chtěli bychom umět rozhodnout, zda je dané číslo Gaussovým prvočíslem. K tomu nám poslouží následující série tvrzení:

Tvrzení. *Každé Gaussovo prvočíslo má reálný násobek.*

Tvrzení. *Číslo z je Gaussovo prvočíslo právě tehdy, když $\overline{z}$ je Gaussovo prvočíslo.*

Tvrzení. *Reálné prvočíslo se v Gaussově oboru rozkládá právě tehdy, lze-li jej zapsat jako součet dvou čtverců.*

Věta. (Fermatova) *Existují (až na přenásobení jednotkou) právě tato Gaussova prvočísla:*

(i) *Čísla tvaru $a+bi$, kde $N(a+bi)$ je dvojka nebo reálné prvočíslo tvaru $4k+1$.*
(ii) *Reálná prvočísla tvaru $4k+3$.*

Na přednášce větu dokážeme pomocí znalostí, které jsme postupně nasbírali. Pro zájemce přidávám jiný, trikový důkaz prvního bodu:

Definice. Mějme množinu S s konečným počtem prvků. *Involuce* je taková funkce $f\colon S \to S$, která je inverzní sama k sobě.

Lemma. *Počet pevných bodů každé involuce na dané množině má stejnou paritu.*

Důkaz. (Fermatovy věty) Sestrojme množinu S uspořádaných trojic (x, y, z) takových, že $p = x^2 + 4yz$. Ta má zřejmě involuci $(x, y, z) \mapsto (x, z, y)$. Jiná méně zřejmá involuce je

$$(x,\ y,\ z) \longmapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{pro } x < y - z, \\ (2y - x,\ y,\ x - y + z) & \text{pro } y - z < x < 2y, \\ (x - 2y,\ x - y + z,\ y) & \text{pro } x > 2y. \end{cases}$$

Ta má jen jeden pevný bod $(1, 1, k)$. Jelikož počet pevných bodů obou involucí musí mít stejnou paritu, první involuce musí mít nějaký pevný bod. Tudíž se p dá zapsat jako $x^2 + 4y^2$.

Využití

Občas se teorie kolem Gaussových čísel dá využít i v příkladech olympiádního typu.

Úloha. Řešte v celých číslech rovnici $x^2 + y^2 = 2009$. (MKS 30. ročník, seriál)

Úloha. Vyřešte diofantickou rovnici $x^2 + y^2 = 2005(x - y)$.

Úloha. (Těžká) Vyřešte obecnou diofantickou rovnici tvaru

$$\alpha x^2 + \beta x + \alpha y^2 + \gamma y + \delta = 0.$$

Tvrzení. *Jsou-li a, b nesoudělná čísla splňující $ab = y^k$, pak a i b jsou k-té mocniny (až na přenásobení jednotkou).*

Úloha. Které dvojice celých čísel splňují rovnici $x^2 + 1 = y^3$?

Úloha. Nalezněte všechny pythagorejské trojice, tj. vyřešte diofantickou rovnici

$$x^2 + y^2 = z^2.$$