Gaussove prvočísla

Michal Szabados

Úvod

Táto prednáška bude o komplexných celých číslach. Komplexné celé číslo je jednoducho číslo tvaru $a + bi$, kde a a b sú celé. Čiže sú to akoby mrežové body roviny. Keďže komplexná rovina sa nazýva Gaussova, aj tieto čísla sa nazývajú ako Gaussove celé čísla. Nás budú zaujímať vlastnosti týkajúce sa násobenia a delenia, aby sme mohli definovať prvočísla. A nakoniec ich všetky nájdeme..

Základy

Komplexné číslo je číslo tvaru $a+bi$, kde i je imaginárna jednotka s vlastnosťou $i^2 = -1$. Taktiež sa dá zapísať v tvare $re^{i\alpha}$, kde r je jeho absolútna hodnota a α uhol, ktorý zviera s reálnou osou. Pre násobenie dvoch komplexných čísel platia nasledujúce vzťahy:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$
$$re^{i\alpha} \cdot se^{i\beta} = (rs)e^{i(\alpha+\beta)}$$

Absolútna hodnota komplexného čísla $z = a+bi$ je definovaná ako $|z| = \sqrt{a^2 + b^2}$, čo je geometricky vzdialenosť od nuly. Tiež sa používa pojem komplexne združeného čísla $\overline{z} = a - bi$.

Tvrdenie. *Pre ľubovoľné komplexné čísla z_1, z_2, z platí*

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

Úloha 1. Dostali sme štvorčekovú sieť. Aké je maximálne $n \in \mathbb{N}$, pre ktoré existuje kružnica so stredom v niektorom mrežovom bode, na ktorej leží n mrežových bodov?

Gaussove prvočísla

Definícia. (Neformálna) *Gaussove prvočíslo je také komplexné celé číslo, ktorého jediný deliteľ až na násobenie jednotkou je ono samo. Pritom jednotkou chápeme čísla* 1, i, -1 a $-i$, *ale tieto čísla spolu s nulou ako prvočísla nepočítame.*

Úloha 2. Dokážte, že ak je z prvočíslo, tak aj $\overline{z}$ je prvočíslo.

Úloha 3. Dokážte, že reálne prvočísla tvaru $4k+3$ sú aj komplexnými prvočíslami.

Ďalej sa budeme snažiť dokázať, že rozklad čísla na komplexné prvočísla je až na symetrie (násobenie jednotkami a pod.) jednoznačný. Z toho nám potom vyplynie návod, ako nájsť všetky komplexné prvočísla. Na niektoré tvrdenia budeme potrebovať malú Fermatovu vetu:

Veta. (Malá Fermatova) *Pokiaľ celé číslo a nie je deliteľné prvočíslom p, tak a^p dáva zvyšok 1 po delení p. Teda*

$$a^p \equiv 1 \pmod{p}.$$

Tvrdenie. *Súčin dvoch čísel, z ktorých sú obe súčtom dvoch štvorcov, je tiež súčet dvoch štvorcov.*

Tvrdenie. *Ak číslo $n = a^2 + b^2$ je deliteľné prvočíslom $p = x^2 + y^2$, tak $\frac{n}{p}$ je tiež súčtom dvoch štvorcov.*

Tvrdenie. *Ak číslo tvaru $a^2 + b^2$ je deliteľné číslom, ktoré nie je súčtom dvoch štvorcov, tak ich podiel je deliteľný číslom, ktoré tiež nie je súčtom dvoch štvorcov.*

Tvrdenie. *Nech a, b sú dve nesúdeliteľné čísla. Potom každý deliteľ čísla $a^2 + b^2$ je súčtom dvoch štvorcov.*

Tvrdenie. (Fermat) *Nepárne prvočíslo p sa dá zapísať ako súčet dvoch štvorcov práve vtedy, keď $p \equiv 1 \pmod{4}$.*

Úloha 4. Ak pre prvočíslo p tvaru $4k + 3$ platí $p \mid (a^2 + b^2)$, tak $p \mid a$ a zároveň $p \mid b$. Dokážte.

Zagierov dôkaz na jednu vetu

Tento dôkaz Fermatovho tvrdenia som pre zaujímavosť našiel na wikipédii.

Definícia. *Majme množinu S s konečným počtom prvkov. Involúcia je taká funkcia $f : S \mapsto S$, ktorá je samoinverzná. T.j. $f(f(x)) = x$ pre $x \in S$.*

Úloha 5. Počet pevných bodov ($x \in S$ takých, že $f(x) = x$) každej involúcie na danej množine má rovnakú paritu.

Dôkaz. (Fermatovho tvrdenia) Zostrojme množinu S usporiadaných trojíc (x, y, z) takých, že $p = x^2 + 4xy$. Tá má zrejme involúciu $(x, y, z) \mapsto (x, z, y)$. Iná menej zrejmá involúcia je

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

Tá má len jeden pevný bod $(1, 1, k)$. Keďže počet pevných bodov involúcií na tej istej množine má rovnakú paritu, prvá involúcia musí mať nejaký pevný bod. Takže p sa dá napísať ako $x^2 + 4y^2$.