- Rozšíření $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$
- Sdružené číslo $\bar{\alpha} := a - b\sqrt{d}$, kde $\alpha = a + b\sqrt{d}$
- Norma $\mathbf{N}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$
- Gaussova celá čísla: $\mathbb{Z}[i]$, tj. $d = -1$.

Pozorování.

$$\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta).$$

Věta. $\mathbb{Z}[i]$ je Eukleidův obor.

Pozorování. Komplexní sdružení $\alpha \mapsto \bar{\alpha}$ je automorfismus okruhu $\mathbb{C}$. Tedy speciálně je to automorfismus $\mathbb{Z}[i]$.

0.1. **Prvočísla v $\mathbb{Z}[i]$.**

- Norma v $\mathbb{Z}[i]$ je druhá mocnina absolutní hodnoty.
- Je to tedy zobrazení do $\mathbb{N}$, přičemž $\mathbf{N}(\alpha) = 0$, právě když $\alpha = 0$.

Pozorování. $\alpha \in \mathbb{Z}[i]$ je invertibilní, právě když $\mathbf{N}(\alpha) = 1$.
(Tedy $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.)

Důkaz. Je-li $\alpha\beta = 1$, pak i $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(1) = 1$ a tedy $\mathbf{N}(\alpha) = \mathbf{N}(\beta) = 1$.
Naopak, je-li $\mathbf{N}(\alpha) = 1$, je $\bar{\alpha} = \alpha^{-1}$. □

$\mathbb{Z}[i]$ je Eukleidův, tedy také Gaussův (jednoznačné rozklady na prvočinitele). Speciálně je tedy každý ireducibilní prvek prvočinitelem. Prvočinitelé $\mathbb{Z}[i]$ se nazývají Gaussova prvočísla.

Podívejme se, jaká Gaussova prvočísla existují. Pro jejich analýzu je užitečným nástrojem postřeh, že rozkladům prvků v $\mathbb{Z}[i]$ odpovídají rozklady jejich norem v $\mathbb{Z}$.

- Nechť je α Gaussovo prvočíslo, které neleží v $\mathbb{Z}$. Pak je i $\bar{\alpha}$ prvočíslo a $\alpha\bar{\alpha}$ je prvočíselný rozklad $\mathbf{N}(\alpha)$ v $\mathbb{Z}[i]$. Gaussova prvočísla, která neleží v $\mathbb{Z}$, jsou tedy tvaru $a + bi$, kde $a, b \in \mathbb{Z}$ a $a^2 + b^2$ je prvočíslo.
- Naopak, je-li nějaké prvočíslo v $\mathbb{Z}$ tvaru $a^2 + b^2$, pak $\alpha = a + bi$ a $\bar{\alpha} = a - bi$ jsou prvočísla, protože pokud by α bylo reducibilní v $\mathbb{Z}[i]$, bylo by $\mathbf{N}(\alpha)$ reducibilní v $\mathbb{Z}$.
- Zbývá ověřit, zda nějaká prvočísla v $\mathbb{Z}$ jsou zároveň Gaussovými prvočísly, případně, která to jsou.

Věta. Celočíselné prvočíslo p je Gaussovým prvočíslem, právě když $p \equiv 3 \mod 4$.

Důkaz. Platí $2 = (1 + i)(1 - i)$. Uvažujme tedy lichá prvočísla.

Z výše uvedeného rozboru plyne, že p je rozložitelné, právě když je rovno $\alpha\bar{\alpha}$, je tedy $a^2 + b^2$. Čtverec sudého celého čísla je $0 \mod 4$ a čtverec lichého je $1 \mod 4$, protože $(2k + 1)^2 = 4k^2 + 4k + 1$. Je-li tedy liché prvočíslo součtem čtverců, je $1 \mod 4$. Tím je ukázáno, že prvočísla tvaru $4k + 3$ jsou Gaussovými prvočísly.

Zbývá ukázat, že prvočísla tvaru $p = 4k + 1$ jsou součtem čtverců. K tomu stačí vzít prvek h, který je primitivní čtvrtou odmocninou z jedné v tělese $\mathbb{Z}_p$. Taková odmocnina existuje, stačí položit

$$h = \alpha^k = \alpha^{\frac{p-1}{4}},$$

kde α je primitivní prvek tělesa. Platí

$$h^2 \equiv -1 \mod p,$$

protože $\alpha^{\frac{p-1}{2}}$ je involuce. Tedy p dělí $h^2+1=(h+i)(h-i)$. Kdyby p bylo Gaussovo prvočíslo, muselo by dělit buď $h+i$ nebo $h-i$, což zjevně nedělí.

Číslo h můžeme také získat bez znalosti primitivního prvku jako

$$h=\frac{(p-1)}{2}!$$

Ukážeme, že $h^2=(p-1)!$ a vztah $h^2\equiv -1 \mod p$ pak je obsahem Wilsonovy věty. Máme

$$h^2=\left(\prod_{a=1}^{\frac{(p-1)}{2}} a\right)\cdot\left(\prod_{a=1}^{\frac{(p-1)}{2}} a\right)=(-1)^{\frac{p-1}{2}}\left(\prod_{a=1}^{\frac{(p-1)}{2}} -a\right)\cdot\left(\prod_{a=1}^{\frac{(p-1)}{2}} a\right)=(-1)^{\frac{p-1}{2}}(p-1)!$$

Tím je důkaz hotov, protože $\frac{p-1}{2}=2k$ je sudé. □

Pozorování. Rozklad prvočísla $4k+1$ na součet čtverců je jednoznačný.