Sedmá sada domácích úloh

Termín odevzdání 22./23. 11. 18:00

Příklad 1. Rozložte v $\mathbb{Z}[i]$ na součin ireducibilních prvků:

a) 17

b) 5+i

c) 12+3i

Příklad 2. Dokažte, že pokud v gaussovském oboru R platí $x^2 = y^3$, tak je x tvaru az^3 pro nějaké $a, z \in R$, kde a je invertibilní.

Příklad 3. Dokažte, že pokud je p prvočíslo, tak platí:

a) $x^{p-1} - 1 = \prod_{n=1}^{p-1}(x - n)$ v oboru $\mathbb{Z}_p[x]$

b) pokud je p tvaru $4k + 1$ pro $k \in \mathbb{N}$, tak rovnice $x^{2k} + 1$ má v $\mathbb{Z}_p$ vždy řešení

c) pokud je p tvaru $4k + 1$ pro $k \in \mathbb{N}$, tak v $\mathbb{Z}_p$ existuje druhá odmocnina z -1.

Svůj postup podrobně zdůvodněte. Můžete bez důkazu použít fakta, že pokud a je kořen polynomu $f(x)$, tak $x - a | f$ a že $\mathbb{Z}_p[x]$ je gaussovský.