Teorie čísel: Cvičení 6

21. března 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Definice: Buď $\zeta_n = e^{\frac{2\pi i}{n}}$ primitivní n-tá odmocnina z 1. Pak n-tý *cyklotomický* (kruhový) *polynom* definujeme jako $t_n(x) = \prod_{\substack{1\leq a\leq n\\(a,n)=1}} (x - \zeta_n^a)$, kde násobíme přes všechna a, která jsou nesoudělná s n.

Tvrzení:

a) $\deg(t_n) = \varphi(n)$.

b) $x^n - 1 = \prod_{d|n} t_d(x)$, kde násobíme přes všechna přirozená čísla d, která dělí n.

-2. Rozložte polynom $x^{15} - 1$ na součin ireducibilních polynomů v $\mathbb{Q}[x]$.

-1. Určete, čemu se rovná:
   (a) $\frac{5+i}{3+2i}$;
   (b) $N(4 + 3i)$;
   (c) $\overline{7 - 8i}$.

0. V $\mathbb{Z}[i]$ rozložte na prvočinitele čísla 7 a $5 + i$.

! 1. Rozložte polynom $x^n - 1$ na součin ireducibilních polynomů v $\mathbb{Q}[x]$ pro a) $n = 7$, b) $n = 12$.

! 2. Ukažte, že pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ platí $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

! 3. Ukažte, že prvek $\alpha \in \mathbb{Z}[i]$ je invertibilní právě tehdy, když $N(\alpha) = 1$. Najděte všechny invertibilní prvky v $\mathbb{Z}[i]$.

! 4. Ukažte, že pokud je $N(\alpha)$ prvočíslo v $\mathbb{Z}$, pak je α prvočinitel v $\mathbb{Z}[i]$

! 5. V $\mathbb{Z}[i]$ rozložte na prvočinitele čísla 15, $12 + 21i$ a $3 + 21i$.

! 6. Ukažte, že pro $a, b \in \mathbb{Z}$ platí, že a dělí b v $\mathbb{Z}$ právě tehdy když a dělí b v $\mathbb{Z}[i]$.

! 7. V $\mathbb{Z}[i]$ platí $5 = (1 + 2i)(1 - 2i) = (2 + i)(2 - i)$. Rozmyslete si, proč to není spor s tím, že $\mathbb{Z}[i]$ je gaussovský obor.

Další příklady:

8. Ukažte, že pro $n \in \mathbb{Z}$ a $a + bi \in \mathbb{Z}[i]$ platí, že $n|(a + bi) \iff n|a$ a $n|b$.

9. Ukažte, že α je prvočinitel v $\mathbb{Z}[i]$ právě tehdy, když $\overline{\alpha}$ je prvočinitel.

10. Spočtěte osmý cyklotomický polynom a výpočtem ukažte, že je ireducibilní.

11. V $\mathbb{Z}[i]$ určete $NSD(12 + 21i, 3 + 21i)$:
   (a) z rozkladu na prvočinitele;
   (b) pomocí Euklidova algoritmu a určete Bézoutovy koeficienty.

12. Nechť $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. Rozhodněte o pravdivosti následujících tvrzení a své tvrzení dokažte.
   (a) Pokud $\alpha \mid \beta$, pak $N(\alpha) \mid N(\beta)$.
   (b) Pokud $N(\alpha) \mid N(\beta)$, pak $\alpha \mid \beta$.
   (c) Pokud $\gamma = \alpha^2 + \beta^2$, pak γ není prvočinitel v $\mathbb{Z}[i]$.

13. Popište, které čísla v $\mathbb{Z}[i]$ jsou dělitelné $1 + i$.

14. Najděte příklad okruhu $R \supset \mathbb{Z}$ takového, že pro některá $a, b \in \mathbb{Z}$ platí a dělí b v R, ale a nedělí b v $\mathbb{Z}$.

15. Dokažte, že $t_{p^k}(x) = \sum_{i=0}^{p-1} x^{ip^{k-1}}$ pro každé prvočíslo p a $k \in \mathbb{N}$.

16. Dokažte, že $t_{2n}(-x) = t_n(x)$ pro každé liché $n > 1$.

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.
Úlohy s ! je doporučeno řešit přednostně.
Úlohy s $*$ jsou náročnější.