Teorie čísel: Cvičení 6 – výsledky a vybraná řešení

21. března 2022

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

Výsledky:

-2. $x^{15}-1 = t_1(x)t_3(x)t_5(x)t_{15}(x) = (x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1)$

-1. a) $\frac{17-7i}{13}$, b) 25, c) $7+8i$

0. a) Z tvrzení z přednášky (nebo faktu, že v $\mathbb{Z}[i]$ neexistuje prvek normy 7) je 7 prvočinitel v $\mathbb{Z}[i]$.

   b) $N(5+i) = 26$, hledáme tedy rozklad $5+i$ na prvočinitele normy 2 a 13 (platí, že $a \mid b$ implikuje $N(a) \mid N(b)$ a z charakterizace prvočinitelů na přednášce pak i tito prvočinitelé musí existovat). Prvočinitel normy 2 je až na asociovanost právě jeden (např. $i+1$) a po vydělení zjistíme, že $5+i = (1+i)(3-2i)$. Oba tyto prvky už jsou prvočinitelé, neboť mají prvočíselnou normu (cv. 3).

1. a) $x^7-1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$,

   b) $x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$.

2. Čistě z definice roznásobte oba výrazy. (Nebo použijte definici přes sdružený prvek a uvědomte si vlastnosti komplexního sdružení.)

3. Pokud je $N(\alpha) = 1$, tak $\alpha\bar{\alpha} = 1$ a $\bar{\alpha}$ je tak inverz. Naopak pokud $\alpha \parallel 1$, tak $N(\alpha) \mid N(1) = 1$, což v $\mathbb{Z}[i]$ implikuje $N(\alpha) = 1$.

4. Použijte, že prvočinitelé jsou v gaussovských oborech shodní s ireducibilními prvky. Jaké normy můžou mít dělitelé α a co to o nich říká?

5. a) $15 = 3 \cdot 5 = 3 \cdot (2+i)(2-i)$

   b)$12+21i = 3(4+7i) = 3(2+i)(3+2i)$

   c) $3+21i = 3(1+7i) = 3(1+i)(1+2i)(2-i)$

6. Implikace zleva doprava je zřejmá. Pro tu druhou to jde buď napřímo rozepsat, nebo použít, že z norem dostaneme $a^2 = N(a) \mid N(b) = b^2$, což už nad $\mathbb{Z}$ implikuje $a \mid b$ (viz první cvičení a p-valuace).

7. Prvky součinů jsou navzájem asociované, takže to není spor (v gaussovských oborech je rozklad jednoznačný až na asociovanost).

8. Rozmyslete si, jakého tvaru jsou v $\mathbb{Z}[i]$ násobky n.

9. Použijte definice.

10. Vyjde x^4+1. Jde si všimnout, že nemá racionální kořen (ireducibilita ze zadání je implicitně myšlena v $\mathbb{Q}[x]$) a například výpočtem ověřit, že neexistuje rozklad na dva polynomy stupně 2.

11. Z příkladu 5 vidíme, že NSD je 3. Euklidovým algoritmem dostaneme $3 = (3+2i)(12+21i)+(-4-1)(3+21i)$.

12. Ano, NE, ano.

13. Po chvilce výpočtů vyjde, že $1+i \mid x+yi$ právě když $2 \mid y-x$.

14. Třeba $\mathbb{Q}$.

15. Použijte tvrzení na začátku cvičení a vyjde to.

16. Vyjádřete si oba polynomy z definice pomocí odmocnin z jedničky. Všimněte si, že mají stejně velké stupně a dokažte, že množina kořenů (včetně násobností) je skutečně stejná.