Algebra — cvičení 4

(příklady cihlovou barvou jsme dělali on-line, na doma jsou ty ostatní bez hvězdiček)

Trocha RSA

1. Alžběta chce sdělit Bedřichovi svou velikost bot B, ale nechce, aby se tento údaj dozvěděl někdo další. Vzala tedy Bedřichovo oblíbené číslo $o = 55$ (které každý zná, ale jen Bedřich ho umí rozložit na $5 \cdot 11$) a jeho věk $v = 27$ (který taky každý zná) a Bedřichovi zaslala hodnotu

$$Z = B^v \bmod o = 47.$$

   Co má nyní Bedřich provést, aby zjistil Alžbětinu velikost bot (a kolik to teda je)?

Rozklady v oborech polynomů

2. Spočítejte v oborech $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}_3[x], \mathbb{Z}_5[x]$ ireducibilní rozklady polynomů

   (a) $x^3 - 2$,

   (b) $x^4 - x^2 - 2$.

3. Nalezněte všechny ireducibilní polynomy nad $\mathbb{Z}_2$ stupně nejvýše 4.

Rozklady v číselných oborech

4. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady prvků 3, 5, 6, 7, $10 - 6i$, $9 + 3i$.

5. Spočítejte v oboru $\mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady prvků 2, $3 - i\sqrt{2}$ a $5 - i\sqrt{2}$.

6. Dokažte, že každé prvočíslo p splňující $p \equiv 3 \pmod 4$ je ireducibilním prvkem oboru $\mathbb{Z}[i]$.

7. Ukažte, že 2 je ireducibilním prvkem $\mathbb{Z}[i\sqrt{3}]$, ale není v tomto oboru prvočinitelem.

Extra úlohy

8.⋆ Ukažte, že v oboru $\mathbb{Z}[\sqrt{2}]$ neexistuje prvek s normou 23.

9.⋆ Nalezněte nějaký prvek nějakého oboru, který bude mít alespoň *tři* různé rozklady na ireducibilní prvky.

10.⋆ Jsou $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ a $\mathbb{Z}[\sqrt{2} + \sqrt{3}]$ tytéž okruhy? A co $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ a $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$?