Algebrou proti koronaviru IV

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)? [Chceme zjistit $B = B^1$, což nám stačí zjistit mod o díky $B < o$. Hledáme vhodné n takové, aby $Z^n = (B^v)^n = B^{vn} \equiv B^1 \pmod{o}$, přičemž dle Eulera je $B^{\varphi(o)} \equiv 1 \pmod{o}$, takže n má splňovat $vn \equiv 1 \pmod{\varphi(o)}$. Konkrétně řešíme $27o \equiv 1 \pmod{40}$, což dá $o \equiv 3 \pmod{40}$. Hodnotu B tedy zjistíme tak, že Z umocníme na třetí a zmodulíme 55, takže $B = 38$.]

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) $x^3 - 2$, [$\mathbb{C}$: $(x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, kde $\omega = \frac{1}{2}(-1 + \sqrt{3}i)$; $\mathbb{R}$: $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$; $\mathbb{Q}$: ireducibilní; $\mathbb{Z}_3$: $(x+1)^3$; $\mathbb{Z}_5$: $(x+2)(x^2+3x+4)$]

   (b) $x^4 - x^2 - 2$. [$\mathbb{C}$: $(x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$; $\mathbb{R}$: $(x^2+1)(x+\sqrt{2})(x-\sqrt{2})$; $\mathbb{Q}$: $(x^2+1)(x^2-2)$; $\mathbb{Z}_3$: $(x^2+1)^2$; $\mathbb{Z}_5$: $(x^2+3)(x+2)(x+3)$]

3. Nalezněte všechny ireducibilní polynomy nad $\mathbb{Z}_2$ stupně nejvýše 4. [x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$]

Rozklady v číselných oborech

4. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady prvků 3, 5, 6, 7, $10-6i$, $9+3i$. [$3 = 3$, $5 = (2+i)(2-i)$, $6 = 3(1+i)(1-i)$, $7 = 7$, $10-6i = -(1+i)^3(4+i)$, $9+3i = 3(1+i)(2-i)$]

5. Spočítejte v oboru $\mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady prvků 2, $3 - i\sqrt{2}$ a $5 - i\sqrt{2}$. [$2 = -(i\sqrt{2})^2$, $3 - i\sqrt{2} = 3 - i\sqrt{2}$, $5 - i\sqrt{2} = -(1 + i\sqrt{2})^3$]

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. [Čísla tvaru $a^2 - 2b^2$ nemohou dávat zbytky 3 či 5 po dělení 8, takže ani jejich absolutní hodnoty nemohou dávat zbytek 3.]

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 $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$?