Algebrou proti koronaviru IV

(cvičení cihlovou barvou jsme udělali na cvičení, a tak je můžete vynechat)

Trocha RSA

Promyslete si důležitou aplikaci Eulerovy věty, kterou je algoritmus RSA, na příkladu ze života (princip algoritmu najdete na str. 26 ve skriptech):

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 $B^v \bmod o$, která vyšla 47, což je – nečekaně – počet Bedřichových prstů plus jeh věk (opět! Náhoda? Nezdá se mi!).

   (a) 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 $B = 38$.]

   (b) Kolik dalších čísel menších než 53 by bylo použitelných namísto Bedřichova věku? [$\varphi(40) + 5$ (čísla $41, 43, 47, 49, 51$), tedy kromě 27 ještě 20 dalších.]

   (c) Mohla by za stejných podmínek Alžběta Bedřicha informovat, že jí náhle vyrostla noha a že má rázem nohu pětačtyřicítku? [ano, $45^{81} = 45 \bmod 55$]

Rozklady v oborech polynomů

2. Spočítejte v uvedených oborech ireducibilní rozklady polynomů $x^3 - 2$, resp. $x^4 - x^2 - 2$:

	$\mathbb{C}[x]$	$\mathbb{R}[x]$	$\mathbb{Q}[x]$	$\mathbb{Z}_3[x]$	$\mathbb{Z}_5[x]$
$x^3 - 2$	$\prod_{i=0}^{2}(x - \omega^i \sqrt[3]{2})$	$(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$	ireducibilní	$(x+1)^3$	$(x+2)(x^2+3x+4)$
$x^4 - x^2 - 2$	$(x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$	$(x^2+1)(x+\sqrt{2})(x-\sqrt{2})$	$(x^2+1)(x^2-2)$	$(x^2+1)^2$	$(x^2+3)(x+2)(x+3)$

kde $\omega = \frac{1}{2}(-1 + \sqrt{3}i) = e^{\frac{2\pi i}{3}}$

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

Rozklady na ireducibilní prvky úzce souvisejí s dělením, podobně pak ireducibilita s invertibilitou, proto se v kvadratických rozšířeních tvaru $\mathbb{Z}[\sqrt{s}]$ často hodí uvažovat normu definovanou jako

$$a + b\sqrt{s} \mapsto |a^2 - sb^2|$$

(více o vlastnostech této normy a jejich důsledcích najdete v oddílu 3.2, resp. v Příkladech v oddílech 5.1, 5.3 ve skriptech).

4. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady prvků

   (a) 3 (b) 5 (c) 6 (d) 7 (e) $10 - 6i$ (f) $9 + 3i$.

   [(a) $3 = 3$ (b) $5 = (2+i)(2-i)$, $6 = 3(1+i)(1-i)$ (c) $7 = 7$, $10 - 6i = -(1+i)^3(4+i)$ (d) $9 + 3i = 3(1+i)(2-i)$]

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

   (a) 2 (b) $3 - i\sqrt{2}$ (c) $5 - i\sqrt{2}$

   [(a) $2 = -(i\sqrt{2})^2$ (b) $3 - i\sqrt{2} = 3 - i\sqrt{2}$ (c) $5 - i\sqrt{2} = -(1 + i\sqrt{2})^3$]

6. Dokažte tvrzení Příkladu ze str. 31 skript, které v principu říká, že

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

   (Nápověda: zkuste sporem uvažovat nějaký rozklad, pak se podívejte na normu, využijte faktu, že prvočísla jsou v $\mathbb{Z}$ prvočinitelé, a nakonec si rozmyslete něco o čtvercích $\bmod 4$.)

7. Ukažte, že 2 je ireducibilním prvkem $\mathbb{Z}[i\sqrt{3}]$, ale není v tomto oboru prvočinitelem. [$2 \cdot 2 = 4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, ale 2 nedělí ani jednu ze závorek]

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

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 $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$? [Ne. Ano: položme $a = \sqrt{2} + \sqrt{3}$, pak $\sqrt{2} = \frac{a^2-5}{2} \cdot a - 2a$, podobně pro $\sqrt{3}$.]