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)?

A → 47 → B

umíme efektivně spočítat kvůli tomu, že známe rozklad

$\varphi(55) = 40$ — veřejné

$o = 55 = 5 \cdot 11$ — tajné

$v = 27$, $n = 3$

$B^{v \cdot n} = Z^n = 47^n = B$

$v \cdot n \equiv 1 \pmod{40}$

Bezout $\Rightarrow n = 3$

$B^{40} \equiv 1 \pmod{55}$ — Euler

$Z^3 = 47^3 \bmod 55 = 38$

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) $x^3 - 2$,

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

$3 = 2 + 1$

$3 = 3 + 0$

$x^3 - 2 = (x^2 \dots)(x - \dots)$

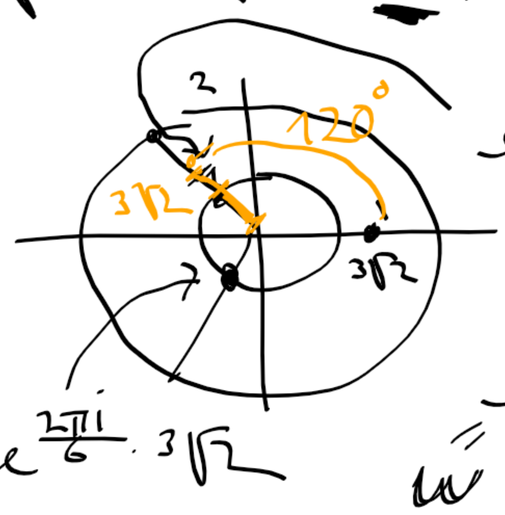
$2x + 2 = 2 \cdot (x + 1)$ v $\mathbb{Z}[x]$

a)

$\sqrt[3]{2}$

$(x^3 - 2) = (x - \sqrt[3]{2}) \cdot (x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) =$

$= (x - \sqrt[3]{2})(x - \sqrt[3]{2} \cdot \omega)(x - \sqrt[3]{2} \cdot \omega^2)$



$e^{\frac{2\pi i}{3}} \cdot \sqrt[3]{2}$

$e^{\frac{2\pi i}{6}} \cdot \sqrt[3]{2}$

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

ω

$\mathbb{R}[x]$: $(x^3 - 2) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$

$\mathbb{Q}[x]$ $\quad \sqrt[3]{2} \notin \mathbb{Q}$ $\quad x^3 - 2 = x^3 - 2$

je ired. v $\mathbb{Q}[x]$

$\mathbb{Z}_3$: $\not{0}$, $\not{1}$, 2

$(x^3 - 2) : (x + 1) = x^2 + 2x + 1$

$x^3 - 2 = x^3 + 1 = (x + 1)(x^2 + 2x + 1) = (x+1)^2$

$= (x + 1)^3$

$4 = 3 + 1$

$= 2 + 2$

$x^2 + 1$

$(x^2 + 1)^2 = x^4 + 2x^2 + 1$

→ U polynomu st. 4 se nám může stát, že nemá kořen, ale ani není ireducibilní nad tělesem

b) $x^4 - x^2 - 2$ Zkusme substituci $x^2 = y$: $y^2 - y - 2 = (y-2)(y+1)$

$\hookrightarrow$ $x^4 - x^2 - 2 = (x^2-2)(x^2+1)$

$\mathbb{C}$: $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$
$x^2 + 1 = (x+i)(x-i)$
$\Big\}$ $x^4 - x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})(x+i)(x-i)$

$\mathbb{R}$: x^2+1 je ireducibilní nad $\mathbb{R}$ (nemá v $\mathbb{R}$ kořen)

$\Rightarrow$ $x^4 - x^2 - 2 = (x^2+1)(x-\sqrt{2})(x+\sqrt{2})$

$\mathbb{Q}$: x^2+1 i x^2-2 ireducibilní nad $\mathbb{Q}$ $\Rightarrow$ $x^4 - x^2 - 2 = (x^2+1)(x^2-2)$

$\mathbb{Z}_3$: x^2+1: nemá kořen v $\mathbb{Z}_3$ $\Rightarrow$ ireducibilní

$x^2 - 2 = x^2 + 1$

$\Rightarrow$ $x^4 - x^2 - 2 = x^4 + 2x + 1 = (x^2+1)^2$

$\mathbb{Z}_5$: x^2+1: kořen 2 a 3, tedy $x^2+1 = (x-2)(x-3) =$
$= (x+3)(x+2)$

$x^2 - 2 = x^2 + 3$: nemá kořen

$\Rightarrow$ $x^4 - x^2 - 2 = x^4 + 4x^2 + 3 = (x^2+3)(x+3)(x+2)$

Rozklady v číselných oborech

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

$x = a + b\sqrt{5} \rightsquigarrow V(x) = |a^2 - 5b^2|$

$\mathbb{Z}[\sqrt{5}]$

$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$

$\Rightarrow V(a+bi) = a^2 + b^2$

invertibilní v $\mathbb{Z}[i]$: $\pm 1, \pm i$

PLATÍ?

(i) $x \mid y \Rightarrow V(x) \mid V(y)$

(ii) $x \mid y$ & $y \nmid x$ $\quad V(x) \mid V(y)$, $V(x) \neq V(y)$

(iii) $V(x) = 1 \Leftrightarrow x$ je invert.

(iv) $V(x \cdot y) = V(x) \cdot V(y)$

3

$a^2 + b^2 = 3 \Rightarrow$ nemá řešení

$a, b \in \mathbb{Z}$

$\Rightarrow$ neexistuje prvek normy 3

$\Rightarrow$ 3 nejde rozložit ve "smysluplném"

$x \neq 1$

Uvažujme rozklad $3 = x \cdot y$, $y \neq 1$

$\Rightarrow V(3) = V(x \cdot y) \overset{(iv)}{=} V(x) \cdot V(y)$

$3 \cdot 3 = 9$

$\Rightarrow V(x) = 3$

$3 = 3$

5

$1+2i$
$-1-2i$
$i-2$
$-i+2$

$1-2i$
$-1+2i$
$i+2$
$-i-2$

Uvažujme rozklad $5 = x \cdot y$

Potom $V(5) = V(x \cdot y) = V(x) \cdot V(y)$

$5 \cdot 5 = 25$

$\Rightarrow V(x) = 5$

Prvky normy 5:

$1+2i$	$1-2i$
$-1-2i$	$-1+2i$
$i-2$	$i+2$
$-i+2$	$-i-2$

vzájemně asociované

Zkusme $x = 1+2i$

Potom $y = \frac{5}{1+2i} = \frac{5}{1+2i} \cdot \frac{1-2i}{1-2i} = \frac{5-10i}{5} = 1-2i$

$\Rightarrow 5 = (1+2i)(1-2i)$

10-6i:

$$10-6i = 2\cdot(5-3i)$$

$\Rightarrow$ Zvlášť rozložíme 2 a $5-3i$

2: $A\bar{A}\ 2 = x\cdot y$

$2\cdot 2 = 4 = V(2) = V(x\cdot y) = V(x)\cdot V(y) \Rightarrow V(x) = 2 = a^2+b^2$

mapr. $1+i = x$

$\Rightarrow 2 = (1+i)(1-i)$

$y = \frac{2}{x} =$

$= \frac{2}{1+i} = \frac{2}{(1+i)}\cdot\frac{1-i}{(1-i)} =$

$= 1-i$

$5-3i$: $A\bar{A}\ 5-3i = x\cdot y$

$2\cdot 17 = 34 = V(5-3i) = V(x\cdot y) = V(x)\cdot V(y) \Rightarrow V(x) = 2$

mapr. $x = 1+i$

$y = \frac{5-3i}{x} = \frac{5-3i}{1+i} = \frac{5-3i}{1+i}\cdot\frac{1-i}{1-i} =$

$= \frac{5-3i-5i+3i^2}{2} = \frac{2-8i}{2} = 1-4i$

$\Rightarrow 5-3i = (1+i)(1-4i)$

Dohromady $10-6i = (1+i)(1-i)(1+i)(1-4i) =$

$= -(1+i)^3\cdot(4+i)$

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

$x = a + bi\sqrt{2} \Rightarrow V(x) = a^2 + 2b^2$

$3 - i\sqrt{2}$: $V(3 - i\sqrt{2}) = 11$, 11 je prvočíslo $\Rightarrow$ $3 - i\sqrt{2}$ je ireducibilní

$5 - i\sqrt{2}$: $V(5 - i\sqrt{2}) = 25 + 2 = 27 = 3 \cdot 3 \cdot 3$

$a^2 + 2b^2 = 3 \Rightarrow$ např. $1 - i\sqrt{2}$

Chceme určit $\frac{5 - i\sqrt{2}}{1 - i\sqrt{2}} = \frac{5 - i\sqrt{2}}{1 - i\sqrt{2}} \cdot \frac{1 + i\sqrt{2}}{1 + i\sqrt{2}} = \frac{5 + 5i\sqrt{2} - i\sqrt{2} + 2}{1 + 2} = \frac{7 + 4i\sqrt{2}}{3}$,

ale $\frac{7 + 4i\sqrt{2}}{3} \notin \mathbb{Z}[i\sqrt{2}] \Rightarrow$ Zkusíme sem druhý prvek mocniny 3: $1 + i\sqrt{2}$

$\frac{5 - i\sqrt{2}}{1 + i\sqrt{2}} = \frac{5 - i\sqrt{2}}{1 + i\sqrt{2}} \cdot \frac{1 - i\sqrt{2}}{1 - i\sqrt{2}} = \frac{3 - 6i\sqrt{2}}{3} = 1 - 2i\sqrt{2}$

Chceme rozložit $1 - 2i\sqrt{2}$, jediná možnost je opět $1 + i\sqrt{2}$:

$\frac{1 - 2i\sqrt{2}}{1 + i\sqrt{2}} = \frac{1 - 2i\sqrt{2}}{1 + i\sqrt{2}} \cdot \frac{1 - i\sqrt{2}}{1 - i\sqrt{2}} = \frac{-3 - 3i\sqrt{2}}{3} \cdot -1 - i\sqrt{2}$

$\Rightarrow 5 - i\sqrt{2} = (1 + i\sqrt{2})^2(-1 - i\sqrt{2}) =$

$= -(1 + i\sqrt{2})^3$

$\mathbb{Z}[i\sqrt{3}]$

prvočinitel: $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$

ireducibilní: $p = a \cdot b \Rightarrow p \mid a \vee p \mid b$

norma:

$x = a + bi\sqrt{3}$

$V(x) = \boxed{a^2 + 3b^2}$

$\overset{\text{n.}}{\Rightarrow}$ prvočinitel $\Rightarrow$ ireducibilní

$2 \mid 4 = (1+i\sqrt{3})(1-i\sqrt{3}) \quad (1+i\sqrt{3})(1-i\sqrt{3}) = 4$

$2 \nmid 1+i\sqrt{3}$

$2 \nmid 1-i\sqrt{3}$ $\Rightarrow$ 2 není prvočinitel

$V(2) = 4 = 2 \cdot 2$ $\Rightarrow$ prvek normy 2 v $\mathbb{Z}[i\sqrt{3}]$ neexistuje

$\Rightarrow$ 2 je ireducibilní v $\mathbb{Z}[i\sqrt{3}]$