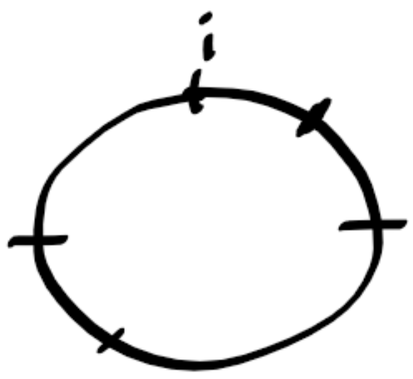
1. Nalezněte ireducibilní rozklad polynomu $x^4 + 1$ nad tělesy $\mathbb{C}$, $\mathbb{R}$ a $\mathbb{Z}_5$.
2. Nalezněte (nějaký) ireducibilní rozklad prvku $16 + i\sqrt{5}$ v oboru $\mathbb{Z}[i\sqrt{5}]$.
3. Nalezněte největšího společného dělitele čísel $4 + 6i$ a $3 - 7i$ v oboru $\mathbb{Z}[i]$.
4. Zvolme pevné $z \in \mathbb{C}$. Ukažte, že množina $\{f \in \mathbb{Q}[x] \mid f(z) = 0\}$ tvoří ideál okruhu $\mathbb{Q}[x]$.

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



$x^2 = i$

$(a+bi)^2 = i$

porovnat reálnou a imaginární část

$f \in I$

$g \in \mathbb{Q}[x]$

$g \in \mathbb{Q}$

2+2

$x^4 + 1 = f_1 \cdot f_2 \cdot f_3 \cdot f_4$

(x^2+i) (x^2-i)

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

---

1. Najděte všechny racionální kořeny daných polynomů z $\mathbb{Z}[x]$:
   (a) $2x^3 - x^2 + 3$
   (b) $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$.

a)

$\frac{r}{s} \in \mathbb{Q}$, $r, s \in \mathbb{Z}$

$s \mid 2 \rightarrow s = \pm 1, \pm 2$

$r \mid 3 \rightarrow r = \pm 1, \pm 3$

$\pm 1, \pm \frac{1}{2}, \pm 3, \pm \frac{3}{2}$

→ vyhovuje pouze 1

R gaussovský

Q jeho podílové těleso

$f \in R[x]$

$f = \sum_{i=0}^{m} a_i x^i$

$\frac{r}{s} \in Q$, konec f

$\Rightarrow s \mid a_m$

$r \mid a_0$

2. Rozmyslete si, proč je polynom $f(x) = 2x + 6$ ireducibilní v $\mathbb{Q}[x]$, ale je rozložitelný v $\mathbb{Z}[x]$. Najděte k němu v $\mathbb{Q}[x]$ asociovaný primitivní polynom.

$2x + 6 = 2(x + 3)$

$NSD(2,6) = 2$

f primitivní $\Rightarrow$
$f \in R[x]$, R gauss.
$\rightarrow$ f je ired. v $R[x]$
$\Leftrightarrow$
v $\mathbb{Q}[x]$
i pod. tzl.

- 3. Rozmyslete si, proč jsou následující polynomy v příslušných oborech ireducibilní:

(a) $x^3 + x^2 + x + 3$ v $\mathbb{Z}[x]$
(b) $x^4 + x^3 - x + 1$ v $\mathbb{Z}[x]$
(c) $4x^3 - 15x^2 + 60x + 180$ v $\mathbb{Z}[x]$
(d) $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v $\mathbb{Q}[x]$

a) je primitivní
$\rightarrow$ možný rozklad v $\mathbb{Q}[x]$

$\frac{r}{s}$	$r \mid 3$	$\rightarrow \pm 1, \pm 3$
	$s \mid 1$	$\rightarrow \pm 1$

$\frac{r}{s}$ ..... $\pm 1, \pm 3$

$\rightarrow$ nemá kořen v $\mathbb{Q}$ $\rightarrow$ ired. v $\mathbb{Q}[x]$ $\rightarrow$

je primitivní $\Rightarrow$ je ireduc. v $\mathbb{Z}[x]$

b) je primitivní $\rightarrow$ ired. vyšetřovat v $\mathbb{Q}[x]$
1 + 3 $\rightarrow$ nejde, nemá kořen v $\mathbb{Q}$
2 + 2 $\rightarrow$ upočítat

R obor integrity,
$f = \sum_{i=0}^{n} a_i x^i$, f primitivní

c)
Pokud $\exists p$ prvočíslo t.ž.
$p \mid a_0, \dots, p \mid a_{n-1}$
&
$p \nmid a_0^2$

$\Rightarrow$ f je ireducibilní

~~$3 \mid 15, 3 \mid 60, 3 \mid 180$~~ / $3^2 = 9 \mid 180$ $\Rightarrow$ je ired.
$5 \mid 15, 5 \mid 60, 5 \mid 180$, $5^2 = 25 \nmid 180$

Čínská věta o zbytcích pro polynomy

6. Vyřešte rovnice:

   (a) $(x^3 + x + 1)f(x) \equiv 1 \pmod{x^4 + x + 1}$ v $\mathbb{Z}_2[x]$

   (b) $(2x + 1)f(x) \equiv x^3 \pmod{x^2 + 1}$ v $\mathbb{Z}_3[x]$

a) Chceme $g(x)$ t.ž. $g(x)\cdot(x^3+x+1) \equiv 1 \pmod{x^4+x+1}$

Najít pomocí Bezouta

$f(x) \equiv (1+x^2)\cdot 1 \pmod{x^4+x+1}$

$NSD(x^3+x+1,\ x^4+x+1) =$

$= \boxed{1 = a(x)\cdot(x^3+x+1) + b(x)\cdot(x^4+x+1)}$

$b(x)\cdot(x^4+x+1) \equiv 0 \pmod{x^4+x+1}$

$a(x) \equiv 1+x^2$

$f(x) = (x^4+x+1)\cdot h(x) + (1+x^2)$

8. Najděte polynom $f \in \mathbb{Z}_5[x]$ co nejmenšího stupně, který splňuje

$$\begin{cases} f \equiv x+1 \pmod{x^2+1} \\ f \equiv x \pmod{x^3+1} \end{cases}$$

$f = h\cdot(x^3+1) + x$

$h\cdot(x^3+1) + x \equiv x+1 \pmod{x^2+1}$

$h(x^3+1) \equiv 1 \pmod{x^2+1}$

$\rightarrow (x^3+1) : (x^2+1) \equiv x \quad (4x+1)$

$4x+1$

$h(4x+1) \equiv 1 \pmod{x^2+1}$ / $\cdot(4x+1)^{-1}$

$h \equiv h' \rightarrow$ vyjádřím si h

7. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující $f(0) = 1, f(1) = 0, f(2) = 2$ pomocí

   (a) jako Lagrangeův interpolační polynom

   (b) pomocí Čínské věty o zbytcích

b) • $f \equiv f(a) \pmod{x-a}$

$a \in \mathbb{Q}$

$f \in \mathbb{Q}[x]$

$f = q \cdot (x-a) + r$

$\downarrow$

$f(a) = q(a)\underbrace{(a-a)}_{=0} + r \Rightarrow f(a) = r$

- $f(x) \equiv 1 \pmod{x}$
- $f(x) \equiv 0 \pmod{x-1}$
- $f(x) \equiv 2 \pmod{x-2}$