1. Dokažte, že podílové těleso oboru $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ lze ztotožnit s tělesem $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ (nejprve tvrzení přesně zformulujte).

$\updownarrow$ jsou izomorfní

$\mathbb{C}$

$$\frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{ac+bd+(bc-ad)i}{c^2+d^2} = \underbrace{\frac{ac+bd}{c^2+d^2}}_{\in\mathbb{Q}} + \underbrace{\frac{bc-ad}{c^2+d^2}}_{\in\mathbb{Q}}\, i$$

φ

$c+di \neq 0$

$$a+bi = \frac{p}{q} + \frac{r}{s}i = \frac{ps+qri}{qs}$$

$p, q, r, s \in \mathbb{Z}$

- $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$
- $\varphi(a+b) = \varphi(a)+\varphi(b)$

2. Vydělte se zbytkem polynomy

(a) $x^4 + 3x^3 + 4x^2 + x + 3$ a $x^2 + 2$ v $\mathbb{Z}[x]$ a v $\mathbb{Z}_5[x]$; [$x^2 + 3x + 2$, zbytek $-5x - 1 \in \mathbb{Z}[x]$, resp. zbytek $4 \in \mathbb{Z}_5[x]$]

(b) $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x$ a $x + 1$ v $\mathbb{Z}_2[x]$. [$x^9 + x^6 + x^5 + x^2 + 1$, zbytek 1]

a) $(x^4 + 3x^3 + 4x^2 + x + 3) : (x^2+2) = x^2 + 3x + 2$

$$\begin{array}{l} -x^4 \qquad -2x^2 \\ 3x^3 + 2x^2 + x + 3 \\ -3x^3 \qquad -6x \\ 2x^2 - 5x + 3 \\ -2x^2 \qquad -4 \\ -5x - 1 \end{array}$$

$\mathbb{Z}[x]$: $x^2 + 3x + 2$ $(-5x-1)$

$\mathbb{Z}_5[x]$: $x^2 + 3x + 2$ (4)

4. Spočtěte $\mathrm{NSD}(f, g)$ a příslušné Bézoutovy koeficienty pro polynomy

(a) $f = x^3 + x^2 + x + 1$ a $g = x^2 + 2x + 2$ v oboru $\mathbb{Z}_3[x]$ a v oboru $\mathbb{Z}_5[x]$; [$2 = (2x + 1)f + (x^2 + x + 2)g$ v $\mathbb{Z}_3[x]$ a $x + 3 = f + (4x + 1)g$ v $\mathbb{Z}_5[x]$]

(b) $f = x^3 - x^2 - x - 2$ a $g = x^3 - 2x^2 + 3x - 6$ v oboru $\mathbb{Q}[x]$. [$7x - 14 = (-x - 2)f + (x + 3)g$]

$h = \mathrm{NSD}(f,g) = a\cdot f + b\cdot g$

a, b jsou polynomy

x^3+x^2+x+1	1	0
x^2+2x+2	0	1
x	1	$-x-2 = 2x+1$
2	$-x-2 = 2x+1$	$1-(2x+1)(x+2) = 1-2x^2-4x-x-2 = x^2+x+2$
0	.....	.....

$\cdot\,-(x+2)$

$(x^3+x^2+x+1):(x^2+2x+2) = \underline{x+2}$

$2x^2+2x+1$

x

$-(x+2)$

$(x^2+2x+2) : x = x+2$

$2x+2$

2

(mod 3)

$x : 2 = 2x$

$2x \cdot 2 = 4x \equiv x$

$$\boxed{\mathrm{NSD}(f,g) = 2 = (2x+1)\cdot f + (x^2+x+2)\cdot g}$$

3. Nechť $\mathbf{T}$ je těleso a $f, g \in \mathbf{T}[x]$. Ukažte, že pokud $f \mid g$ a $g \mid f$ (jinými slovy f dělí g beze zbytku a g dělí f beze zbytku), pak existuje nenulové $u \in T$ takové, že $f = ug$.

$f \mid g \Rightarrow \deg(f) \leq \deg(g) \Rightarrow \deg(f) = \deg(g)$

$g \mid f \Rightarrow \deg(g) \leq \deg(f)$

$f : g = h$

$f = g \cdot h$

$\Downarrow \deg(h) = 0$

$\Downarrow h \in T$

5. Najděte všechny kořeny polynomu $f = x^2 + x \in \mathbb{Z}_6[x]$ v okruhu $\mathbb{Z}_6$ a napište všechny rozklady (až na pořadí) tohoto f na součin kořenových činitelů, tj. na součin tvaru $(x - a)(x - b)$, kde a, b jsou kořeny.
[$0, 2, 3, 5,\ x^2 + x = x(x - 5) = (x - 3)(x - 2)$]

0 ✓
1 ✗
2 ✓
3 ✓
4 ✗
5 ✓

$(x^2 + x) = x \cdot (x - a) = x(x+1) = x \cdot (x - 5)$

$(x^2 + x) = (x - 2)(x - a) = x^2 + (-a - 2)x + 2a$

$(x-2)(x-3)$ $\quad 2a = 0 \Rightarrow a = 3$