$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$

$(\mathbb{Z}[\sqrt{2}])^\times = ?$

$(a + b\sqrt{2}) \in (\mathbb{Z}[\sqrt{2}])^\times \Leftrightarrow$

$a^2 - 2b^2 = \pm 1$

$\frac{1}{a+b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$

$(\mathbb{Z}[\sqrt{2}])^\times = \{\pm(1+\sqrt{2})^k,\ k \in \mathbb{Z}\}$

$a + b\sqrt{2} \in (\mathbb{Z}[\sqrt{2}])^\times \Rightarrow (a+b\sqrt{2})^{-1} = \pm(a - b\sqrt{2})$

$1 < a + b\sqrt{2} < 1 + \sqrt{2}$

$(a+b\sqrt{2})^{-1} \in (0, 1)$

$\pm(a - b\sqrt{2}) \in (0, 1)$

$-1 < a - b\sqrt{2} < 1$

$1 < a + b\sqrt{2} < 1 + \sqrt{2}$

---

$0 < 2a < 2 + \sqrt{2}$

$0 < a < 1 + \frac{\sqrt{2}}{2} \doteq 1{,}7 < 2$

Tedy nutně $a = 1$

$a^2 - 2b^2 = \pm 1$

$-2b^2 = \pm 1 - 1$

$b^2 = 0, 1 \Rightarrow b = 0, 1, -1$

Jednotky $1,\ 1+\sqrt{2},\ 1-\sqrt{2}$ - nesplňují nerovnost $1 < x < 1+\sqrt{2}$

Tedy $1+\sqrt{2}$ je nejmenší jednotka větší než 1.

Sporem dokážeme, že $\forall \alpha \in (\mathbb{Z}[\sqrt{2}])^\times$: $\alpha = \pm(1+\sqrt{2})^k$, $k \in \mathbb{Z}$. Předpokládejme naopak, že $\exists \beta \in (\mathbb{Z}[\sqrt{2}])^\times$: $\beta$ nelze napsat jako $\pm(1+\sqrt{2})^k$.

Pak umíme $x = (-1)^m \beta \cdot (1+\sqrt{2})^k$ takové, že $1 < x < (1+\sqrt{2})$, nemůže nastat.

Umíme k maximální takové, že $(1+\sqrt{2})^k < |\beta| \Rightarrow x = |\beta| \cdot (1+\sqrt{2})^{-k}$

Kdy $(\mathbb{Z}[\sqrt{2}])^{\times} = \{\pm(1+\sqrt{2})^k, k \in \mathbb{Z}\}$?

$f = x^3 + 3x^2 + 5x + 5$

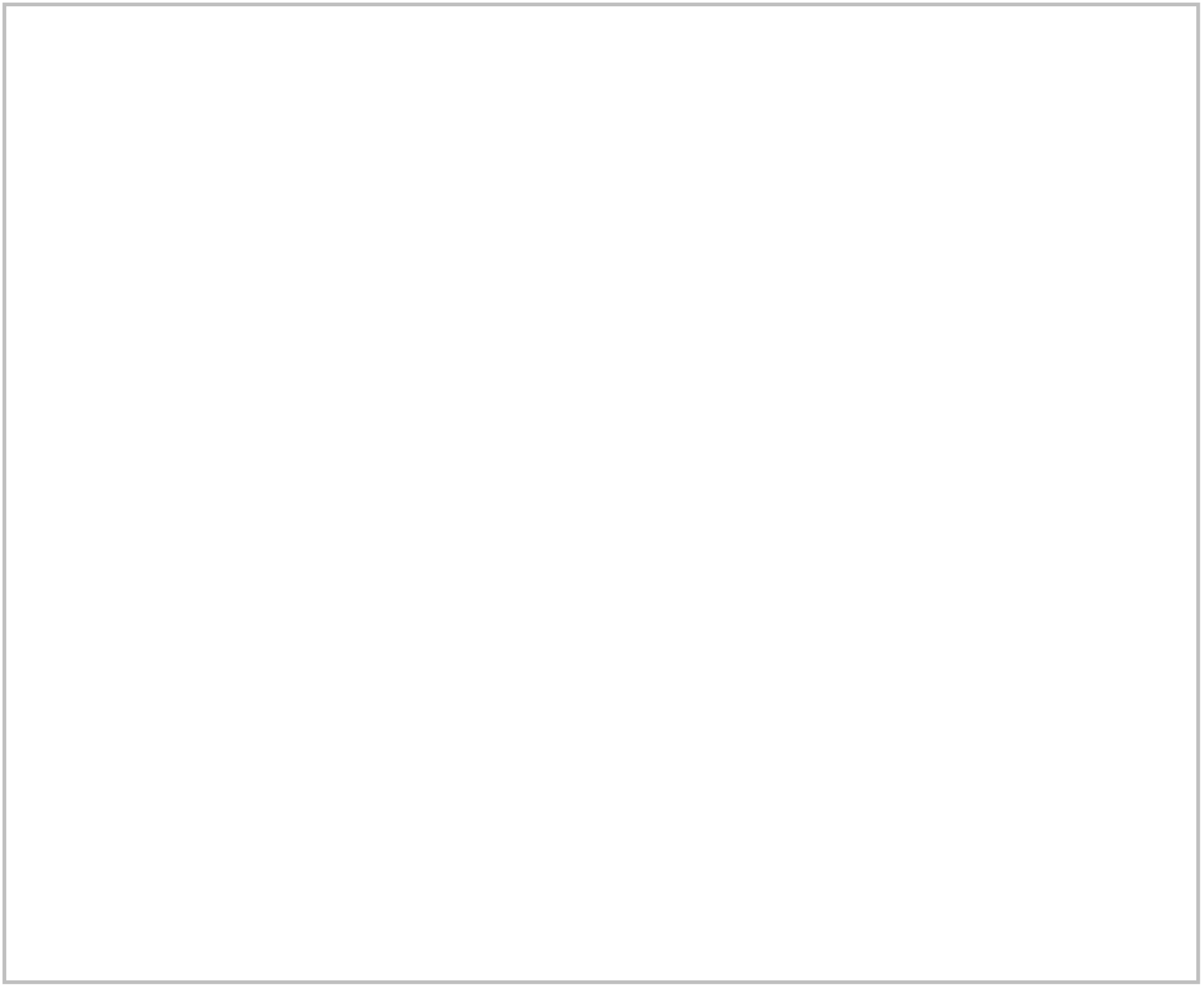
uvažme $x = y + 1$

$g = (y+1)^3 + 3(y+1)^2 + 5(y+1) + 5 =$

$= y^3 + 3y^2 + 3y + 1 + 3(y^2 + 2y + 1) + 5y +$

$+ 5 + 5 = y^3 + 6y^2 + 14y + 14$

je Eisensteinovo vzhledem 2 $\Rightarrow$ $g$ je ireducibilní $\Rightarrow$ $f$ je ireducibilní



Název: III 26-8:34 (4 z 9)

$$f = x^4 + x^3 + x^2 + x + 1$$

$$x = y + 1$$

$$g = (y+1)^4 + (y+1)^3 + (y+1)^2 + y +$$

$$+ 1 + 1 = (y^4 + 4y^3 + 6y^2 + 4y + 1) +$$

$$+ (y^3 + 3y^2 + 3y + 1) + (y^2 + 2y + 1) + y + 2 =$$

$$= y^4 + 5y^3 + 10y^2 + 10y + 5$$

$g$ je Eisensteinův vzhledem k 5 $\Rightarrow$ $f$ je ireduk.

$g_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$

$(a^n - b^n) = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$

substituujme $x = y + 1$

$h_p = (y+1)^{p-1} + (y+1)^{p-2} + \dots + (y+1) + 1 =$

$= y^{p-1} + \left(\binom{p-1}{p-2} + \binom{p-2}{p-2}\right) y^{p-2} +$

$+ \left(\binom{p-1}{p-3} + \binom{p-2}{p-3} + \binom{p-3}{p-3}\right) y^{p-3} + \dots$

$\dots + \left(\binom{p-1}{i} + \binom{p-2}{i} + \dots + \binom{i}{i}\right) y^i + \dots + p$

Chceme $p \mid \binom{p-1}{i} + \binom{p-2}{i} + \dots + \binom{i}{i}$ pro každé $i \in \{1, \dots p-2\}$

Platí $\binom{p-1}{i} + \binom{p-2}{i} + \dots + \binom{i}{i} = \binom{p}{i+1}$?

počet $i$-prvkových podmnožin $\{2, 3, \dots p\}$

počet $i$-prvkových podmnožin $\{3, 4, \dots p\}$

počet $i$-prvkových podmnožin $\{1, \dots p\}$ s nejmenším prvkem 1

počet $(i+1)$-prvkových podmnožin $\{1, \dots p\}$ s nejmenším prvkem 2

Tedy identita platí. Proto

$h_p = y^{p-1} + \binom{p}{p-1} y^{p-2} + \binom{p}{p-2} y^{p-3} + \dots$
$+ \binom{p}{2} y + \binom{p}{1}$

Když je $p$ prvočíslo, pak $p \mid \binom{p}{i}$ pro $i \in \{1, \dots p-1\} \Rightarrow h_p$ je Eis. vzhl. $p$ $\Rightarrow$ $h_p$ je ired. $\Rightarrow g_p$ je ired.

$p$ není prvočíslo $\Rightarrow p = a \cdot b$, $a, b > 1$

$g_p = \frac{x^p - 1}{x - 1} = \frac{x^{ab} - 1}{x - 1} = \frac{(x^a)^b - 1}{x - 1} =$

$= \frac{(x^a - 1)(x^{a(b-1)} + x^{a(b-2)} + \dots + x^a + 1)}{x - 1} =$

$= (x^{a-1} + x^{a-2} + \dots + 1)(x^{a(b-1)} + \dots + 1)$

$\Rightarrow g$ je rozložitelný

$f = x^4 + 4x^3 + x^2 + 5 = (x^2 + Ax + B) \cdot (x^2 + Cx + D) = x^4 + (A+C)x^3 + (B+D+AC)x^2 + (AD+BC)x + BD$ ; $A, B, C, D \in \mathbb{Z}$

$x^3$: $A + C = 4$

$x^2$: $B + D + AC = 1$

$x$: $AD + BC = 0$

$x^0$: $BD = 5$

1) $B = 1$ ; $D = 5$

2) $B = 5$, $D = 1$ je stejná dvojice jako 1)

i) $A + C = 4$

ii) $6 + AC = 1$

iii) $5 \cdot A + C = 0$

iii) − i) $4A = -4 \Rightarrow A = -1 \Rightarrow C = 5$

dosazením do ii) $6 + (-1) \cdot 5 = 1$ platí

3) $B = -1$, $D = -5$

i) $A + C = 4$

ii) $-6 + AC = 1$

iii) $-5A - C = 0$

4) $B = -5$, $D = -1$ symetrický

i) + iii) $-4A = 4 \Rightarrow A = -1 \Rightarrow C = 5$

pak ii) $-6 + (-1) \cdot 5 = 1$ neplatí $\Rightarrow$ není řešení

$f = (x^2 - x + 1)(x^2 + 5x + 5)$.

Postupně generujeme ireduk. polynomy rostoucího stupně; jen s vedoucím koeficientem 1

st 1: $x$, $x+1$, $x+2$ ireduk

st 2: ~~$x^2$~~, $x^2+1$, ~~$x^2+2$~~, ~~$x^2+x$~~, ~~$x^2+x+1$~~,
$x^2+x+2$, ~~$x^2+2x$~~, ~~$x^2+2x+1$~~, $x^2+2x+2$

st 3: ~~$x^3+1$~~, ~~$x^3+2$~~, ~~$x^3+x+1$~~, ~~$x^3+x+2$~~,
$x^3+2x+1$, $x^3+2x+2$, ~~$x^3+x^2+1$~~, $x^3+x^2+2$,
~~$x^3+x^2+x+1$~~, $x^3+x^2+x+2$, $x^3+x^2+2x+1$,
~~$x^3+x^2+2x+2$~~, $x^3+2x^2+1$, ~~$x^3+2x^2+2$~~, $x^3+2x^2+x+1$,
~~$x^3+2x^2+x+2$~~, ~~$x^3+2x^2+2x+1$~~, $x^3+2x^2+2x+2$

$f = x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + x + 2$

| | 1 | 2 | 2 | 2 | 2 | 0 | 1 | 2 |
|---|---|---|---|---|---|---|---|---|
| (-1) | 1 | 0 | 2 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 2 | × |
| (-2) | 1 | 2 | 0 | 1 | 2 | 1 | 0 | |
| 2 | 1 | 1 | 2 | 2 | 0 | 1 | × | |

$f = (x+2)(x+1)(x^5 + 2x^4 + x^2 + 2x + 1)$

irod $x^2+1,\ x^2+x+2,\ x^2+2x+2$

1) $x^5 + 2x^4 + x^2 + 2x + 1 = (x^2+1)(x^3+2x^2+2x+2) + 2$

$-(x^5 + x^3)$

$2x^4 + 2x^3 + x^2 + 2x + 1$

$-(2x^4 + 2x^2)$

$2x^3 + 2x^2 + 2x + 1$

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

$2x^2 + 1$

$-(2x^2 + 2)$

$2$

2) $x^5 + 2x^4 + x^2 + 2x + 1 = (x^2+x+2)(x^3+x^2+2) + 0$

$-(x^5 + x^4 + 2x^3)$

$x^4 + x^3 + x^2 + 2x + 1$

$-(x^4 + x^3 + 2x^2)$

$0 + 0 + 2x^2 + 2x + 1$

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

$0$

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