Eisensteinovo kritérium:

$f(x) \in \mathbb{Z}[x]$ je rozložitelný?

$f(x) = a_n x^n + \dots + a_1 x + a_0$

Jestliže ex. prvočíslo $p \in \mathbb{Z}$

t. ž. $p | a_{n-1}, \dots, p | a_n, p | a_0$

a nedělí $p^2 \nmid a_0$

pak $f(x)$ je ireducibilní nad $\mathbb{Z}$.

Dk: Sporem – předp.

$f(x) = g(x) h(x)$ nad $\mathbb{Z}$

$f(x) \equiv a_n x^n \mod p$

$\parallel$

$g(x) h(x) \equiv a_n x^n \mod p$

$\Downarrow$ v $\mathbb{Z}_p$

jednoznačný rozklad (až na násobení jednotkou)

$g(x) \equiv b_\ell x^\ell \mod p$ | $n = k + \ell$

$h(x) \equiv c_k x^k \mod p$ |

$\Rightarrow g(x) = b_\ell x^\ell + \quad + b_0$

$p \mid b_0$

$h(x) = c_k x^k + \dots + c_0$

$p \mid c_0$

$$g(x)h(x) = \dots\dots \underbrace{b_0 c_0}_{= a_0}$$

$p^2 \mid b_0 c_0$

spor $\square$

<u>Pr 81</u> (ii) koreň $\sqrt[2007]{2}$

kandidát $f(x) = x^{2007} - 2$

Nech $s(x)$ je pol. nejnižšího stupne s koreňom $\sqrt[2007]{2}$

$\rightsquigarrow$ dělení se zbytkem

$$f(x) = h(x)\, s(x) + r(x) \qquad \text{mod } \mathbb{Q}$$

kde $\operatorname{st} r(x) < \operatorname{st} s(x)$

$$\Rightarrow r(x) = 0$$

$$\Rightarrow f(x) = h(x)\, s(x)$$

Ale $f(x)$ je nerozložitelný dle E. kritéria. $\square$

<u>Př 8.2.</u> (i) p lib. prvočíslo

$$p(x) = x^{p-2} + x^{p-3} + \dots + x + 2$$

v $\mathbb{Z}_p$.

- $x^{p-1} - 1 = (x-1)\underbrace{(x^{p-2} + x^{p-3} + \dots + x + 1)}_{p(x)-1}$

$$= (x-1)(p(x)-1)$$

$$a^{\varphi(p)} \equiv 1 \mod p \qquad (a,p)=1$$

$$a^{p-1} - 1 \equiv 0 \mod p$$

$$\boxed{a \not\equiv 0 \mod p \Rightarrow a^{p-1} - 1 \equiv 0 \mod p}$$

Předp. $a \not\equiv 0 \mod p$

- $a \equiv 1 \mod p \Rightarrow a$ je kořen
- $a \not\equiv 1 \mod p \Rightarrow a$ není kořen $f(x)$

<u>Závěr:</u> 1 je jediný kořen

(ii) $g(x) = x^2 + x + 1$

v $\mathbb{Z}_5$: 0 není

$\pm 1 \rightsquigarrow$ není

$\pm 2 \rightsquigarrow$ není

nerozlož.

v $\mathbb{Z}_7$:

0 není

± 1 není

± 2 $+2$ koreň $\rightarrow$ -2 není

± 3 3 není -3 je koreň

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

Pr 8.3 (i)

$y = x^2$

$$f(x) = x^6 - x^4 - 5x^2 - 3$$

má viacnásobný koreň

$$f'(x) = 6x^5 - 4x^3 - 10x$$

$(f, f') = \ ?$ $\rightsquigarrow$ Eukl. alg.

$$3f(x) : \tfrac{1}{2} f'(x) =$$

$$= (3x^6 - 3x^4 - 15x^2 - 9) : (3x^5 - 2x^3 - 5x)$$

$$-(3x^6 - 2x^4 - 5x^2)$$

$= x +$ zlomek

$$\boxed{3x^6-3x^4-15x^2-9 = x(3x^5-2x^3-5x) + (-x^4-10x^2-9)}$$

$$(3x^5-2x^3-5x):(-x^4-10x^2-9) = -3x + \ldots$$

$$-(3x^5+30x^3+27x)$$

$$\boxed{3x^5-2x^3-5x = -3x(-x^4-10x^2-9) + (-32x^3-32x)}$$

$$(-x^4-10x^2-9):(-32)(x^3+x) = \frac{1}{32}x + \ldots$$

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

$$\boxed{-x^4-10x^2-9 = -(x^3+x) - 9x^2 - 9}$$

$$-(x^3+x) = -9\cdot\frac{1}{9}x(x^2+1) + 0$$

poslední nenulový zbytek

$\Rightarrow \ (f, f') = x^2 + 1$

$\Rightarrow$ vícenásobné kořeny

$\pm i$

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

$$= (x^6 - x^4 - 5x^2 - 3) : (x^2+1) = x^4 - 2x^2 - 3$$

$$\begin{array}{l} -(x^6 + x^4) \\ \hline \quad -2x^4 - 5x^2 - 3 \\ \quad -(-2x^4 - 2x^2) \\ \hline \qquad -3x^2 - 3 \end{array}$$

$$\boxed{f(x) = (x^2+1)\underbrace{(x^4 - 2x^2 - 3)}_{(x^2-3)(x^2+1)}}$$

$y = x^2$

$$\boxed{f(x) = (x^2+1)^2 (x^2-3)}$$

rozkład nad $\mathbb{Z}$ a $\mathbb{Q}$

$$\boxed{f(x) = (x^2+1)(x+\sqrt{3})(x-\sqrt{3})}$$

nad $\mathbb{R}$

$$\boxed{f(x) = (x+i)^2 (x-i)^2 (x+\sqrt{3})(x-\sqrt{3})}$$

nad $\mathbb{C}$

nad $\mathbb{Z}_5$: $x^2+1 = (x+2)(x-2)$

$$\boxed{f(x) = (x+2)^2 (x-1)^2 (x^2-3)}$$

nad $\mathbb{Z}_5$

mod $\mathbb{Z}_7$:

- $x^2 + 1$ nerozložitelný

0 není

± 1 není

± 2 není

± 3 není

- $x^2 - 3$

0 není

± 1 není

± 2 není

± 3 není

$$\boxed{f(x) = (x^2+1)^2 (x^2-3)}$$

$\boxed{\text{mod } \mathbb{Z}_7}$

(ii) $p(x)$ má vícenásobný kořen i $\Rightarrow$ má i vícenásobný kořen $-i$ $\Rightarrow$ má faktor $(x^2+1)^2$

$$p(x) : (x^2+1)^2 =$$

$$= (x^6+x^5+4x^4+2x^3+5x^2+x+2) : (x^4+2x^2+1) = x^2+x+2$$

$$-(x^6 + 2x^4 + x^2)$$

$$x^5+2x^4+2x^3+4x^2+x+2$$

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

$$2x^4 + 4x^2 + 2$$

$$\boxed{p(x) = (x^2+1)^2(x^2+x+2)}$$

$\boxed{\text{nad } \mathbb{R}, \mathbb{Z}, \mathbb{Q}}$

nad $\mathbb{C}$:

$$x_{1,2} = \frac{-1 \pm \sqrt{1-8}}{2} = -\frac{1}{2} \pm \frac{\sqrt{7}}{2} i$$

$$\boxed{p(x) = (x+i)^2 (x-i)^2 \left(x + \frac{1}{2} + \frac{\sqrt{7}}{2} i\right)\left(x + \frac{1}{2} - \frac{\sqrt{7}}{2} i\right)}$$

$\boxed{\bmod \mathbb{C}}$

$\bmod \mathbb{Z}_2$: $x^2 + 1 = (x+1)^2$

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

$$\boxed{p(x) = x(x+1)^5}$$

$\boxed{\bmod \mathbb{Z}_2}$

$\bmod \mathbb{Z}_5, \mathbb{Z}_7 \; \ldots\ldots$

(iii) $q(x,y) = x^2y^2 + y^2 + xy + x^2y + 2y + 1$

reste
$$\boxed{\begin{aligned} p(x) &= 0 \\ q(x,y) &= 0 \end{aligned}}$$

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

$$q(x,y) = x^2(y^2+1) + xy + (y^2+2y+1)$$

$$q(x,y) = (x^2+1)(y^2+1) + xy + (2y^2+2y+2)$$

$$x = \pm i, \quad q(x,y) = 0$$

$$\Downarrow$$

$$\pm i y + (2y^2 + 2y + 2) = 0$$

$$2y^2 + (2 \pm i)y + 2 = 0$$

$$\vdots$$

$$y = -\frac{1}{1 \pm i}$$

$$q(x,y) = (x^2+x+2)(y^2+1) + x(-y^2-1+y) + (2y^2+2y+1-y^2-2)$$

$x :=$ koren x^2+x+2, dopočítame y