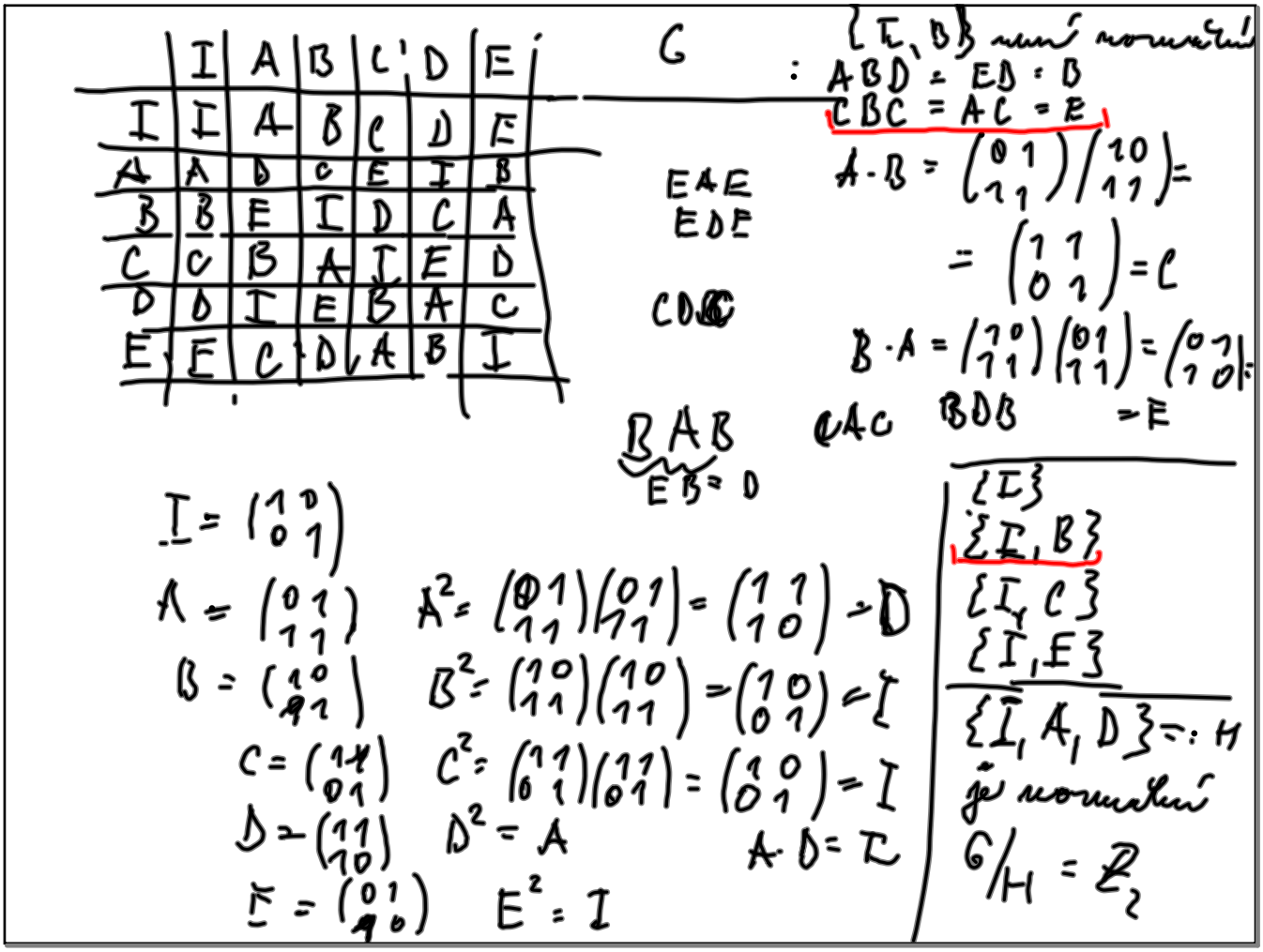

G
{I, B} není normální
ABD = ED = B
CBC = AC = E
A·B = (0 1 / 1 1)(1 0 / 1 1) =
= (1 1 / 0 1) = C
B·A = (1 0 / 1 1)(0 1 / 1 1) = (0 1 / 1 0)
BAB CAC BDB = E
EAE
EDE
CDC
BAB
EB = D
I = (1 0 / 0 1)
A = (0 1 / 1 1) A² = (0 1 / 1 1)(0 1 / 1 1) = (1 1 / 1 0) = D
B = (1 0 / 1 1) B² = (1 0 / 1 1)(1 0 / 1 1) = (1 0 / 0 1) = I
C = (1 1 / 0 1) C² = (1 1 / 0 1)(1 1 / 0 1) = (1 0 / 0 1) = I
D = (1 1 / 1 0) D² = A
A D = C
E = (0 1 / 1 0) E² = I
{I}
{I, B}
{I, C}
{I, E}
{I, A, D} =: H
je normální
G/H = Z₂

3 6-8:07

Určíme zbytek po dělení číslem 100.
Tedy je jednoznačně určen zbytky po dělení číslem 4
a číslem 25.

$12^{12^{12}} \equiv 0 \ (4)$ & $12^{12^{12}} \equiv 16 \ (25) \Rightarrow 12^{12^{12}} \equiv 16 \ (100)$

$12^{12^{12}} \equiv ? \ (25)$

$12^{20} \equiv 1 \ (25)$

Chceme zjistit zbytek exponentu, tj: čísla $12^{12^{12}}$ po dělení číslem 20

$12^{12^{12}} \equiv 0 \ (4)$ $\qquad$ $2^5 \equiv 1 \ (5)$

$12^{12^{12}} \equiv 2^{12^{12}} \equiv 2^{42} \equiv 1 \ (5) \Rightarrow 12^{12^{12}} \equiv 16 \ (20)$

$12^{12^{12}} = 12^{20k+16} \equiv 12^{20k} \cdot 12^{16} \equiv 12^{16} \equiv (-6)^8 \equiv 11^4 \equiv (-4)^2 \equiv 16 \ (25)$

V oboru $(R, +, \cdot)$ řekneme, že $a \mid b$, existuje-li $c \in R$:
$ac = b$ | $3 = (-1)\cdot(-3)$

Okruhy jsou obory $(R[x], +, \cdot)$, kde $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$\mathbb{R}[x]$ ... ireducibilní polynomy: lineární
kvadratické se záporným diskriminantem
$(x - 1 = \frac{1}{2}(2x - 2))$
↑ jednotka

$\mathbb{C}[x]$, ireducibilní polynomy: pouze lineární
(základní věta algebry)

$x^3+2x^2-5x-8 = (x-2)(x^2+4x+5) = (x-2)(x+2)^2$

	1	2	-4	-8
2	1	4	4	0

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

$= (x+1)(x^2-x+1)\left(x-\frac{-3+\sqrt{3}}{2}\right)\left(x-\frac{-3-\sqrt{3}}{2}\right)$

$= (x+1)\left(x-\frac{1+i\sqrt{3}}{2}\right)\left(x-\frac{1-i\sqrt{3}}{2}\right)(x-\quad)(x-\dots)$

	1	3	1	1	3	1
-1	1	2	-1	2	1	0

$x^4+2x^3-x^2+2x+1=0 \quad /\frac{1}{x^2}$

$x^2+2x-1+\frac{2}{x}+\frac{1}{x^2}=0$

$x+\frac{1}{x}=1 \quad x^2-x+1=0$

$x_{1/2}=\frac{1\pm i\sqrt{3}}{2}$

$(u^2-2)+2u-1=0 \qquad u=x+\frac{1}{x}$

$u^2+2u-3=0 \qquad u^2=x^2+2+\frac{1}{x^2}$

$x+\frac{1}{x}=-3 \Rightarrow x^2+3x+1=0, x_{3/4}=\frac{-3\pm\sqrt{5}}{2} \qquad (u+3)(u-1)=0 \qquad u_1=1, u_2=-3$

3 6-8:52

$x^4 + 2x^2 + 2 = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$

$(x^2-(x_1+x_2)x + x_1x_2)\cdot(x^2-(x_3+x_4)x+x_3x_4)$

Podle Eisensteinova kritéria ireducibility pro $p=2$ je tento polynom ireducibilní nad $\mathbb{Q}$ (i $\mathbb{Z}$)

$t := x^2$

$t^2+2t+2=0$

$t_{1,2} = \frac{-2 \pm i\sqrt{4}}{2} = -1 \pm i$

$x^2 = -1+i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$

$x_1 = \sqrt[4]{2}\left(\cos\frac{3\pi}{8} + i\sin\frac{3\pi}{8}\right)$

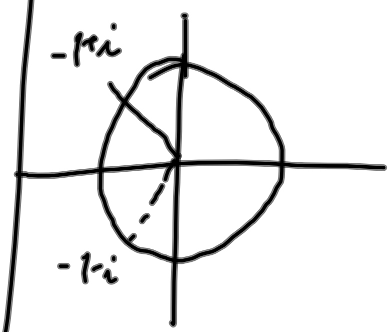
$x_2 = \sqrt[4]{2}\left(\cos\frac{11\pi}{8} + i\sin\frac{11\pi}{8}\right)$

$-1-i$

$x^2 = \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right)$

$x_3 = \sqrt[4]{2}\left(\cos\frac{5\pi}{8} + i\sin\frac{5\pi}{8}\right)$

$x_4 = \sqrt[4]{2}\left(\cos\frac{13\pi}{8} + i\sin\frac{13\pi}{8}\right)$



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

mod $\mathbb{Z}_5$:

	1	0	2	0	2
1	1	1	3	3	

	1	1	3	3
-1	1	0	-3	

	1	-2	1	-2
2	1	0	1	

$x^{10} \equiv 1 \quad (11)$

$x^{10} - 1 = (x-1)(x^9 + x^8 + x^2 + \dots + x + 1) = \vdots \ \mathbb{Z}_{11}$

$= (x-1)(x-2)(x-3)\cdots(x-10)$

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

ireducibilní mod $\mathbb{Z}_{11}$

⇒ nejvyšší pol. dělitele je polynom $(x-2)$