Seminar 7

1) K corp finit $\Rightarrow |K| = p^n$, p-prim, $n \in \mathbb{N}^*$
2) $\forall$ p prim, $\forall$ $n \in \mathbb{N}^* \Rightarrow \exists$ K corp a.î. $|K| = p^n$
3) K corp finit $\Rightarrow$ comutativ
4) K, L corpuri finite, $|K| = |L| \Rightarrow K \simeq L$

Din curs 13:
a) Calcul inversului
1) $\frac{\mathbb{Z}[i]}{(5)}$ este corp cu 25 elemente

Găsiți inversul lui $\overline{7+2i}$

În general $\frac{\mathbb{Z}[i]}{a+bi} \simeq \mathbb{Z}_{|a^2+b^2|}$, $a, b \in \mathbb{Z}$

Ex: $\left|\frac{\mathbb{Z}[i]}{(2+5i)}\right| = 29$

Caut $a+bi \in \mathbb{Z}[i]$ a.î. $(7+2i)(a+bi) = \bar{1} \pmod 5$

$7a + 7bi + 2ai - 2b - 1 \equiv \bar{0} \pmod 5$

$\Rightarrow 7a - 2b - 1 + (7b + 2a)i \equiv \bar{5}(m+ni)$ — multiplu de 5 din $\mathbb{Z}[i]$

$= 5m + 5ni$

$$\begin{cases} 7a - 2b - 1 = 5m \\ 7b + 2a = 5n \end{cases} \overset{\mathbb{Z}[i]}{\Rightarrow} \begin{cases} \hat{2}a - \hat{2}b - 1 = \hat{0} \\ \hat{2}b + \hat{2}a = \hat{0} \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} 4a = \hat{1} \pmod 5 \\ b = -a \pmod 5 \end{cases} \Leftrightarrow \begin{cases} a = 4^{-1} \pmod 5 \Rightarrow a = \bar{4} \\ b = \bar{1} \end{cases}$$

Deci inversul lui $\overline{7+2i}$ este $\overline{4+i}$

2) Câte elemente $x \in \mathbb{Z}_{561}$ au prop că $x^2 = x$?
$\Leftrightarrow |\mathcal{I}dem(\mathbb{Z}_{561})| = ?$

$561 = 3 \cdot 17 \cdot 11$

$\mathbb{Z}_{561} \cong \mathbb{Z}_3 \times \mathbb{Z}_{17} \times \mathbb{Z}_{11}$ (Lema chineză a resturilor)

$\mathbb{Z}_n$, cu $n = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \Rightarrow \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$

$|\mathcal{I}dem(561)| \leftrightarrow |\mathcal{I}dem(\mathbb{Z}_3)| \cdot |\mathcal{I}dem(\mathbb{Z}_{17})| \; \mathcal{I}dem(\mathbb{Z}_{11})|$

$(\mathcal{I}dem\, \mathbb{Z}_p)$, p - prim $\Leftrightarrow$ a găsi idempotenții din $(\mathbb{Z}_p, +, \cdot)$ e totuna de a rezolva ecuația $x^2 = \bar{x}$ în $\mathbb{Z}_p$

$x^2 = x$ în $\mathbb{Z}_p \Leftrightarrow x^2 - x \equiv 0 \pmod p \Rightarrow$

$\Rightarrow p \mid x^2 - x \Rightarrow p \mid x(x-1) \Rightarrow p \mid x$ sau $p \mid x-1$
(p-prim)

$p \mid \bar{x} \Rightarrow \bar{x} = \bar{0}$

$p \mid \bar{x-1} \Rightarrow \bar{x} = \bar{1}$

Deci $\mathcal{I}dem(\mathbb{Z}_p) = \{\bar{0}, \bar{1}\}$, p = prim

$\mathcal{I}dem(\mathbb{Z}_{p^k}) = \{\bar{0}, \bar{1}\}$, p-prim, $k \geq 1$

$\Rightarrow |\mathcal{I}dem\, \mathbb{Z}_{p^k}| = 2$, p = # prim, $k \geq 1$

$|\mathcal{I}dem(\mathbb{Z}_{561})| = 2 \cdot 2 \cdot 2 = 2^3 = 8$

Mai general $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} \Rightarrow |\mathcal{I}dem(\mathbb{Z}_n)| = 2^k$

③ TFI:

$$\frac{\mathbb{Z}[i]}{(2-i)} \simeq \mathbb{Z}_5$$

Caut $f: \mathbb{Z}[i] \to \mathbb{Z}_5$ un morfism surjectiv de inele cu nucleul

$f(a+bi) = ? \in \mathbb{Z}_5$

$f(a+bi) = f(a) + f(b) \cdot f(i)$

f morfism

$f(a) = f(\underbrace{1+\dots+1}_{a \text{ ori}}) = \underbrace{f(1)+\dots f(1)}_{a \text{ ori}} = a f(1) = \bar{a}$, $\bar{a} \in \mathbb{Z}_5$ ($f(1) = 1$)

$f(a+bi) = \hat{a} + \hat{b} \cdot f(i)$

$\ker f \supset (2-i) \Rightarrow (2-i) \Rightarrow f(2-i) = 0$

f-morfism $\Downarrow$

$f(2) - f(i) = 0 \Rightarrow \bar{2} = f(i)$

Deci $f(a+bi) = \hat{a} + \hat{b}\,\hat{2} = \overline{a+2b}$

~~$f(a+bi)(c+di) = f(ac + adi + bdi +$~~

$f(a+bi)(c+di) = f(ac - bd + (ad+bc)i) =$

$= \overline{ac - bd + 2(ad+bc)}$ (*)

$f(a+bi) \cdot f(c+di) = \overline{(a+2b)(c+2d)} =$

$= \overline{ac + 4bd + 2(ad+bc)} = *$

$4 = -1 \pmod 5$

Curs 13:

④ $f(x) = x^4 + 1 \in \mathbb{Z}_{89}[X]$

Descompunere în factori ireductibili

Idee: $(x^2)^2 + 1 \Rightarrow y^2 + 1$

Vreau să rezolv ec $y^2 + \hat{1} = \hat{0}$ în $\mathbb{Z}_{89}$

$y^2 + 1 = 0$

$\Delta = -4 \equiv 85 \pmod{89}$ Adun 89 până găsesc număr pătrat perfect

$\Delta = 85 + 89 \cdot m = 441$ p. perfect

$\sqrt{\Delta} = 21$

$245 = 90 = \hat{1} \pmod{89}$

$$y_1 = \frac{0 - 21}{2} = -\frac{21}{2} = -21 \cdot 2^{-1} = -21 \cdot 45 = -3060 = 34 \pmod{89}$$

$$y_2 = 21 \cdot 2^{-1} = 21 \cdot 45 \equiv 55 \pmod{89}$$

$\Rightarrow x^2 \in \{34, 55\}$

$x^2 \equiv 55 \pmod{89} \equiv 144 \pmod{89} \equiv (\pm 12)^2$

$55 + 89 = 144 = 12^2 \Rightarrow x = \pm 12$

$x^2 \equiv 34 \pmod{89} \equiv 1369 \equiv (\pm 37)^2$

$f(x) = (X - \hat{12})(X + \hat{12})(X - \hat{37})(X + \hat{37})$ - sunt descompunere ireductibilă în $\mathbb{Z}_{89}[X]$

⑤ $\frac{\mathbb{R}[X]}{(X^2-17X)} \simeq \mathbb{R}\times\mathbb{R}$

Vreau $f: \mathbb{R}[X] \to \mathbb{R}\times\mathbb{R}$ să fie un morfism surjectiv de inele cu nucleul ~~generat de~~ $\ker f = (X^2-17X)$

$X^2-17X = X(X-17)$

$f(P) = (P(0), P(17))$ - morfismul

↑ P polinom $\in \mathbb{R}[X]$

! Cramer, inverse de matrici

⑥ $(X^n-2)^n - X - 2 = [(X^n-2+X-X)^n] - [X] - 2$

$= [(X^n-X-2)+X]^n - X - 2$

$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ ✗

$= \sum C_n^k (X^n-X-2)^{n-k} X^k - X - 2 =$

$= (X^n-X-2)^n + \sum_{k=1}^{n-1} C_n^k (X^2-X-2)^{n-k} X^k + (X^n-X-2)$

$= (X^n-X-2)\cdot Q[X]$ $\Rightarrow P$ este reductibil în $\mathbb{Z}[X]$
$\in \mathbb{Z}[X]$