Ф-ия $\ell(t) = f(x_0 + te_1, y_0 + te_2)$ има производна в $t=0$

$\exists \lim_{t\to 0} \frac{\ell(t) - \ell(0)}{t} = \ell'(0)$

$\ell'(0) = \frac{\partial f}{\partial x}(x_0 y_0) e_1 + \frac{\partial f}{\partial y}(x_0 y_0) e_2$

$\left(\frac{\partial f}{\partial x}(x_0 y_0), \frac{\partial f}{\partial y}(x_0 y_0)\right) = \operatorname{grad} f(x_0 y_0)$

градиент $\Rightarrow$

!!! $\ell'(0) = \langle \operatorname{grad} f, \vec{e} \rangle$

$\langle \operatorname{grad} f(x), \vec{e} \rangle = \sum_{i=1}^{n} e_i \frac{\partial f}{\partial x_i}(x)$ $\quad \vec{e} = (e_1 \dots e_n)$

$\max \frac{\partial f}{\partial \vec{e}}(x) = \| \operatorname{grad} f(x) \|$

Лекции и упражнения

ВА Касиярян

Предмети от обхождащи
Теорема на Ойлер - Ферма и
Теорема на Уилсън

За произволно $n \in \mathbb{N}$, $n > 1$
ФП $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ на $\mathbb{Z}$ по
$n\mathbb{Z}$ (класовете по $n\mathbb{Z}$ и остатъците
при делене с n)
Представя $\mathbb{Z}_n$ като мн-во
$\mathbb{Z}_n = \{z + n\mathbb{Z} \mid 0 \le z \le n-1\}$
$\forall z = qn + r \Rightarrow z + n\mathbb{Z} = r + n\mathbb{Z}$
$r + n\mathbb{Z}$ е комутативен
представен с r-ия $r + n\mathbb{Z}$ с
r елемента
Лема
$\bar{a}$ обр в $\mathbb{Z}_n$ е тъкмо
a е взаимно от n + $n\mathbb{Z}$ за
всяко естествено делители
на n
Док

$(\mathbb{Z}_n, +)$ е циклична гр
от $\mathbb{Z}_n$ порождена от класа
на 1 - едва и $\forall$ ненулева
ПГ на $(\mathbb{Z}_n, +)$ е циклична
и порождена от $m(1+n\mathbb{Z}) =$
$m + n\mathbb{Z}$ за някой естествен
делител m на n или
Притивоположната ПГ $\{0_{\mathbb{Z}_n}\} =$
$< n + n\mathbb{Z} >$
ПГ-те на $(\mathbb{Z}_n, +)$ са
$< a + n\mathbb{Z} >$ за всеки един
делител m на n. Всички
такива циклични гр.
$< m + n\mathbb{Z} > = \{(m + n\mathbb{Z})(\varepsilon + n\mathbb{Z})$
$| 0 \leq \varepsilon \leq n - 1\}$ са чрез m в
$\mathbb{Z}_n$ и изброяват всички
$\forall < \mathbb{Z}_n, +>$

Деф:
Функцията на Ойлер
$\varphi(n)$ за $n \in \mathbb{N}$, $n > 1$ се
определя като брят
на взаимно простите с
n остатъци при делене
с n

Th.
Нека $\mathbb{Z}_n$ е пръстен от
остатъците при делене с
n и $\mathbb{Z}_n^*$ е мултиплика-
тивната група на $\mathbb{Z}_n$
Тогава
(i) $a + n\mathbb{Z}_n \in \mathbb{Z}_n^* \Leftrightarrow (a, n) = \pm 1$
(ii) $a + n\mathbb{Z}_n \in \mathbb{Z}_n^* \Leftrightarrow a + n\mathbb{Z}$
не е делител на нулата в $\mathbb{Z}_n$
(iii) $|\mathbb{Z}_n^*| = \varphi(n)$
(iv) $\mathbb{Z}_n$ е поле $\Leftrightarrow n$ е просто
число
(v) $\mathbb{Z}_n$ е област (няма делител на
нулата) $\Leftrightarrow n$ е просто число

Док
(i) $\rightarrow$ Ако $a + n\mathbb{Z} \in \mathbb{Z}_n^*$ то $\exists$
$b + n\mathbb{Z} \in \mathbb{Z}_n$ така че
$ab + n\mathbb{Z} = (a + n\mathbb{Z})(b + n\mathbb{Z}) =$
$1 + n\mathbb{Z}$

Това е равно силно на
$ab - 1 = nq \in n\mathbb{Z}$ за някое
$q \in \mathbb{Z}$
Сега $(a,n)/ab, (a,n)/nq$
откъдето $(a,n)/ab - nq = 1$
и $(a,n) = \pm 1$

(i)← ако $(a,n) = \pm 1$ то
съществува $u, v \in \mathbb{Z}$ т. ка $au + nv = 1$
Следователно $(a + n\mathbb{Z})(u + n\mathbb{Z})$
$= au + nv + n\mathbb{Z} = 1 + n\mathbb{Z}$ и
$1 (a + n\mathbb{Z})^{-1} = u + n\mathbb{Z} \in \mathbb{Z}_n$
По def това означава
че $a + n\mathbb{Z} \in \mathbb{Z}_n^*$

(ii)→ Ясно, защото обратимите
спрямо умножението
елементи не са делители на
нулата.

(ii)← Допускаме че $a + n\mathbb{Z}$
$\in \mathbb{Z}_n$ не е делител на нулата

в $\mathbb{Z}_n$ но не обратим
относно умножението.
Тогава съгласно условие
(i) $НОК(a,n) = \pm d \neq \pm 1$ за
някое $d \in \mathbb{N}$
Ако $a_1 = \frac{a}{d} \in \mathbb{Z}$ и $n_1 = \frac{n}{d} \in \mathbb{N}$
то $(a + n\mathbb{Z})(n_1 + n\mathbb{Z}) = an_1 + n\mathbb{Z} =$
$a_1 d n_1 + n\mathbb{Z} = a_1 n + n\mathbb{Z} =$
$n\mathbb{Z} = n_1 + n\mathbb{Z} \neq n\mathbb{Z}$
Следователно $a + n\mathbb{Z}$ е
делител на нулата в $\mathbb{Z}_n$.
Противоречието доказва че
ако $a + n\mathbb{Z}$ не дели нулата
в $\mathbb{Z}_n$ то $a + n\mathbb{Z} \in \mathbb{Z}_n^*$

(iii) Съгласно условие (i)
броят на елементите
$|\mathbb{Z}_n^*| = |\{a + n\mathbb{Z} \mid a, n = \pm 1, 1 \leq a \leq n\}| =$
$= \varphi(n)$

(iv) $\mathbb{Z}_n$ е поле $\Leftrightarrow$
$\forall a+n\mathbb{Z} \in \mathbb{Z}_n \setminus \{n\mathbb{Z}\}$ е обратим
$\Leftrightarrow |\mathbb{Z}_n^*| = n-1 \overset{(iii)}{\Leftrightarrow} \ell(n) = n-1$

Ако n е просто число, то остатъците $1, 2, \ldots, n-1$ при делене с n са взаимно прости с n и $\ell(n) = n-1$

Ако $n = kl$ е $k, l \in \mathbb{N}$, $1 < k, l < n-1$ е съставно то измежду остатъците от $1, \ldots, n$ при делене с n има поне 2 остатъка k и n които не са взаимно прости с n. Следователно $\ell(n) \leq n-2$ и $\mathbb{Z}_n$ не е поле

(v) $\mathbb{Z}_n$ е област $\Leftrightarrow$
$\forall$ елемент $a+n\mathbb{Z} \in \mathbb{Z}_n \setminus \{n\mathbb{Z}\}$ е делител на нулата в $\mathbb{Z}_n \overset{(ii)}{\Leftrightarrow}$ $\forall$ елемента $a+n\mathbb{Z} \in \mathbb{Z}_n \setminus \{n\mathbb{Z}\}$ е от $\mathbb{Z}_n^* \Leftrightarrow \mathbb{Z}_n$ е поле $\overset{(iv)}{\Leftrightarrow} n$ е просто

□

$\ell\left(p_1^{a_1} \cdots p_k^{a_k}\right) = p_1^{a_1-1}(p_1-1)\, p_2^{a_2-1}(p_2-1) \cdots p_k^{a_k-1}(p_k-1)$

Лема

Ако p е просто число $n \in \mathbb{N}$ то $\ell(n) = p^{n-1}(p-1)$

Док

Остатъците $1 \leq k \leq p^n$ при делене с p^n не е взаимно прост с $p^n \Leftrightarrow p$ дели k. Тогава е в сила за $k = pm$, $1 \leq m \leq p^{n-1}$ има p^{n-1} остатъка при делене с p^n които не са взаимно прости с p^n. Оттук броят на взаимно простите с p^n остатъци при делене с p^n е $\ell(n) = p^n - p^{n-1} = p^{n-1}(p-1)$ □

Лема

Ако a и b са взаимно прости естествени числа то - числата от 1 до

ф-ята на Ойлер
$\varphi(ab) = \varphi(a)\varphi(b)$
док
Разгл таблицата

1	2	..	s	..	a-1	a
a+1	a+2	..	a+s	..	a+(a-1)	2a
ja+1	ja+2		ja+s		(j+1)a
(b-1)a+1	(b-1)a+2				(b-1)a+a-1	ba

$0 \le r \le b-1$ с a стълба и b реда
За $\forall x \in \mathbb{N}$ означаваме с $P(x)$
мн-вото на простите делители на x. Тогава $(x, ab) = \pm 1 \iff$
$P(x) \cap P(ab) = \emptyset \iff P(ab) = P(a) \cup P(b)$.
$\iff P(x) \cap [P(a) \cup P(b)] = [P(x) \cap P(a)] \cup$
$[P(x) \cap P(b)] = \emptyset \iff$
$P(x) \cap P(a) = 0$ и $P(x) \cap P(b) = \emptyset \iff$
$(x, a) = 1$ и $(x, b) = 1$
Трябва да докажем че
броят на взаимно
простите с ab и b

числа $1 \le x \le ab$ е
$\varphi(a) \cdot \varphi(b)$
Нека $1 \le s_1 \le \dots \le s_{\varphi(a)} < a$ са
взаимно простите с a цели
числа $1 \le s \le a$. Тогава
целите стълбове $\{ka + s_t \mid$
$0 \le k \le b-1\}$ за $\forall$ кое
$1 \le t \le \varphi(a)$ са свстващи о
взаимно прости с a числа
Наистина, ако $d = (ka + s_t, a)$
то $d \mid a \Rightarrow d \mid ka \Rightarrow d \mid (ka + s_t) - ka$
$\Rightarrow d \mid s_t$ или d е общ делител
на a и s_t По предположение
$(s_t, a) = \pm 1$ т.е $d \mid 1 \Rightarrow d = \pm 1$
Тогава $\{ka + s_t \mid 0 \le k \le b-1$
$1 \le t \le \varphi(a)\}$ изчерпва $\forall$
взаимно прости с a числа
от таблицата. По-точно
ако $(a, ka + s) = \pm 1$ за $0 \le k \le b-1$
$1 \le s \le a$ то $s = (a, s)$ реда
a и s от първото $s \mid ka + s$

и b е общ делител на a и $ka+s \Rightarrow b \mid (ka+s) - ka = s$

т.е. $\delta = \pm 1$ или $(a,s) = 1$ и $s = s_t$ за някое $1 \le t \le \ell(a)$

За δ фиксирано $1 \le s \le a$ т.в.т. s се среща в $\{ka+s \mid 0 \le k \le b-1\}$ на s образува цяла система остатъци при делене с b.

Нанасяне, допускането $k_1 a + s \equiv k_2 a + s \pmod b$ за $0 \le k_1 < k_2 \le b-1$ води до $b \mid k_1 a - k_2 a \equiv (k_1 - k_2)a$. Но $(b,a) = 1$ т.е. $b \mid k_1 - k_2$ за $-(b-1) \le k_1 - k_2 < 0$

Но в интервала $(-(b-1), 0)$ няма цели кратни на b т.е. $\{ka+s \mid 0 \le k \le b-1\}$ е цяла система остатъци при делене с b

Следователно за $\forall 1 \le t \le \ell(a)$ съществува $\{ka+s_t \mid 0 \le k \le b-1\}$ съдържа $\ell(b)$ взаимно прости с b остатъци по модул b които са взаимно прости с a. Оттук в таблицата има $\ell(a)\ell(b)$ взаимно прости с ab числа, които са разположени в стълбовете на

$s_{T_1} \dots s_{T_{\ell(a)}}$

$\uparrow, h$

За произволно естествено $n = p_1^{a_1} \dots p_k^{a_k}$ с $\ell(n) = \ell(p_1^{a_1} \dots p_k^{a_k}) = p_1^{a_1-1}(p_1-1) \dots p_k^{a_k-1}(p_k-1)$

Док

По предположение $p_1 \dots p_k$ са различни прости числа т.че $(p_1^{a_1} \dots p_k^{a_k}) = 1$ и $\ell(p_1^{a_1} \dots p_k^{a_k}) = \ell(p_1^{a_1}) \ell(p_2^{a_2} \dots p_k^{a_k}) = p_1^{a_1-1}(p_1-1)\ell(p_2^{a_2} \dots p_k^{a_k})$.

Продължаваме по същия начин нагоре

пример $\varphi(63) = \varphi(3^2 \cdot 7) = 3^{2-1}(3-1)(7-1) = 3 \cdot 2 \cdot 6 = 36$

Th на Ойлер

За произволно $n \in \mathbb{N}$ и произволно $a \in \mathbb{Z}$, $(a,n)=1$ е в сила $a^{\varphi(n)} \equiv 1 \pmod n$

Док

На единица на пръстена $\mathbb{Z}_n$ трябва да докажем че $(a+n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$

Но за a и n взаимно прости $\Rightarrow a + n\mathbb{Z} \in \mathbb{Z}_n^*$

$\Rightarrow$ редът е на $a+n\mathbb{Z} \in \mathbb{Z}_n^*$ дели реда $\varphi(n)$ на $\mathbb{Z}_n^*$

Така че $(a+n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$

$\mathbb{Z}_{63}^* = \{a + 63\mathbb{Z} \mid (a, 63) = \pm 1\}$

Например

$(25, 63) = \pm 1 \Rightarrow 25^{\varphi(63)} \equiv 1 \pmod{63}$

$25^{36} \equiv 1 \pmod{63}$

$25^{2013} \equiv ? \pmod{63}$

$2013 = 36 \cdot 55 + 33$

180

213

180

33

$25^{2013} = 25^{36 \cdot 55} \cdot 25^{33} =$

$(25^{36})^{55} \cdot 25^{33} \pmod{63} \equiv 1^{55} 25^{33} \pmod{63}$

$25^{33} \pmod{63} = ?$

$25^2 = 625 \equiv -5 \pmod{63}$

$625 = 63 \cdot 9 + 58$

$25^{33} \equiv (-5) 25 \pmod{63}$

$25^3 \equiv -125 \pmod{63} \equiv 1 \pmod{63}$

$25^{33} = 25^{3 \cdot 55} = (25^3)^{11} \pmod{63} \equiv$

$1^{11} \pmod{63} \equiv 1 \pmod{63}$

Редът на $25 + 63\mathbb{Z} \in \mathbb{Z}_{63}^*$ дели $\varphi(63) = 36$

редът е сбъдност е 3

Следствие от Th на Ойлер
Малка Th на Ферма

Ако p е просто число, неделящо цялото число a, то $a^{p-1} \equiv 1 \pmod p$

Док
Ако простото число p не дели $a \in \mathbb{Z}$, то $(p,a) = \pm 1$ по Th на Ойлер $a^{\varphi(p)} = 1 \pmod p$
Но за просто p, φ-ята на Ойлер $\varphi(p) = p-1$, откъдето $a^{p-1} \equiv 1 \pmod p$ Π

Следствие
Всеки елемент $\alpha \in \mathbb{Z}_p$ на полето $\mathbb{Z}_p$ се остатъци при делението с просто p удовлетворява равенството
$\alpha^p = \alpha$
Док
Ако $\alpha = 0 \mathbb{Z}_p = p\mathbb{Z}$, то нулевият елемент $0^p \mathbb{Z}_p = 0\mathbb{Z}_p$
Ако $\alpha \in \mathbb{Z}_p \setminus \{p\mathbb{Z}\}$, то $\alpha \in \mathbb{Z}_p^*$ т.е α е остатъка на някакво число a, т.е. $\alpha = a + p\mathbb{Z}$ за $a \in \mathbb{Z}$, $(a,p) = 1$. От М Th на Ферма $(a+p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$. Почленното умножение с $\alpha = a + p\mathbb{Z}$ дава $\alpha^p = \alpha(a+p\mathbb{Z})^{p-1} = (a+p\mathbb{Z})(1+p\mathbb{Z}) = a + p\mathbb{Z} = \alpha$ Π

Th на Уилсън
Нека $n \in \mathbb{N}$, $n > 1$. В такъв случай $(n-1)! \equiv -1 \pmod n \Leftrightarrow$ n е просто число
Док
Ако $n = kl$ с $k, l \in \mathbb{N}$, $1 < k, l < n$ е съставно число и допуснем че $(n-1)! \equiv -1 \pmod n$, то $\exists q \in \mathbb{Z}$, т.е. $(n-1)! + 1 = nq$

Сега $k \in \mathbb{N}$, $k < n$ реч $(n-1)!$ и n, откъдето $n \nmid 1$. Противоречието доказва че $(n-1)! \not\equiv -1 \pmod n$ за съставно n.

Остава да установим че за всяко просто p е в сила $(p-1)! \equiv -1 \pmod p$. Това сравнение е равносилно на $(p-1)! + p\mathbb{Z} = -1 + p\mathbb{Z}$ в $\mathbb{Z}_p$ или на $\prod_{i=1}^{p-1}(i+p\mathbb{Z}) = -1+p\mathbb{Z}$

Вземайки предвид че $\mathbb{Z}_p^* = \{i+p\mathbb{Z} \mid 1 \le i \le p-1\}$ трябва да докажем че (1) $\Pi(a+p\mathbb{Z}^*) = -1+p\mathbb{Z}$. Но $(a+p\mathbb{Z})^{-1} = b+p\mathbb{Z} \neq a+p\mathbb{Z}$ за $a+p\mathbb{Z} \in \mathbb{Z}_p^*$, то в (1) участие вземат по двама взаимно обратни елементи, които при умножение дават $1+p\mathbb{Z}$. Следователно (1) се свежда или (2) $\Pi(a+p\mathbb{Z}) = 1+p\mathbb{Z}$. Но $(a+p\mathbb{Z})^{-1} = (a+p\mathbb{Z}) \Leftrightarrow$ $1+p\mathbb{Z} = (a+p\mathbb{Z})^2 = a^2+p\mathbb{Z}$ след почленно умножение с $a+p\mathbb{Z} \in \mathbb{Z}_p^*$ за $\Rightarrow$ или с $(a+p\mathbb{Z})^{-1} \in \mathbb{Z}_p$ за $\Leftarrow$. Непосредствено се вижда че $1+p\mathbb{Z} = a^2+p\mathbb{Z}$ точно когато $a^2-1 = (a-1)(a+1) \in p\mathbb{Z}$. Простото число p реди $(a-1)(a+1)$ точно когато $p \mid a-1$ или $p \mid a+1$. Следователно $(a+p\mathbb{Z})^{-1} = a+p\mathbb{Z} \Leftrightarrow$ $p \mid a-1$ или $p \mid a+1 \Leftrightarrow$ $a+p\mathbb{Z} = 1+p\mathbb{Z}$ или $a+p\mathbb{Z} = -1+p\mathbb{Z}$. За $p=2$ имаме $1+p\mathbb{Z} = -1+p\mathbb{Z}$ и (2) е изпълнено. За всяко p от вида $4k+3$ в (3) $\Pi(a+2\mathbb{Z}) = 1+2\mathbb{Z}$ за всяко просто p доказахме че $\Pi(a+p\mathbb{Z}) = (1+p\mathbb{Z})(-1+p\mathbb{Z}) = -1+p\mathbb{Z}$ и $a+p\mathbb{Z} \in \mathbb{Z}_p^*$. $\square$

$11^{2014} \equiv ? \pmod{100}$

$(11, 100) = 1$ (11 не дели 100)

Th Ойлер $\varphi(100)$

$11 \equiv 1 \pmod{100}$

$\varphi(100) = \varphi(2^2)\varphi(5^2) =$

$\varphi(p^\alpha) = p^{\alpha-1}(p-1) \Rightarrow$

$2^{2-1}(2-1)\,5^{2-1}(5-1) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$

Th Ойлер

$11^{40} \equiv 1 \pmod{100}$ Делим

частното и остатъка

2014 на $\varphi(100) = 40$

$2014 = 40 \cdot 50 + 14$ =>

$11^{2014} = 11^{40 \cdot 50 + 14} = (11^{40})^{50} \cdot 11^{14} \pmod{100}$

$11^{50} \cdot 11^{14} \pmod{100} = 11^{14} \pmod{100}$

$11^2 = 121 \equiv 21 \pmod{100}$

$11^3 = 21 \cdot 11 \pmod{100} \equiv$

$231 \pmod{100} \equiv 31 \pmod{100}$

$11^4 = 11^2 \cdot 11^2 = 21 \cdot 21 \pmod{100} = 441 \pmod{100}$

$= 41 \pmod{100}$

$11^7 = 11^4 11^3 = 41 \cdot 31 \pmod{100} =$

$1271 \pmod{100} = 71 \pmod{100}$

$11^{14} = (11^7)^2 = 71 \cdot 71 \pmod{100} =$

$5041 \pmod{100} \equiv 41 \pmod{100}$

$33^{55} \pmod{40} = ?$

$(33, 40) = 1$

$33 = 3 \cdot 11$
$40 = 2^3 \cdot 5$
без прости

Th Ойлер =>

$33^{\varphi(40)} \equiv 1 \pmod{40}$, $\varphi(40) =$

$\varphi(2^3 \cdot 5) = \varphi(2^3)\varphi(5) = 2^{3-1}(2-1)(5-1) = 16$

$\Rightarrow 33^{16} \equiv 1 \pmod{40} \Rightarrow$ реда на

$33 \in \mathbb{Z}_{40}$ дели 16

$55 = 16 \cdot 3 + 7 \Rightarrow$

$33^{16 \cdot 3}\, 33^7 = (33^{16})^3\, 33^7 \pmod{40} =$

$1^3 \cdot 33^7 \pmod{40} = 33^7 \pmod{40}$

$= ?$

(4)

$33^2 = 1089 \pmod{40} \equiv 9 \pmod{40}$

$1089 = 1080 + 9 = 27 \cdot 40 + 9$

$33^3 \pmod{40} = 33^2 \cdot 33 \pmod{40} = 9 \cdot 33 \pmod{40}$

$= 297 \pmod{40} = 17 \pmod{40}$

$33^4 \pmod{40} = 33^2 \cdot 33^2 \pmod{40} =$

$9 \cdot 9 \pmod{40} = 1 \pmod{40}$

$33^{4 \cdot 33^3} \overset{(\mathrm{mod}\ 40)}{=} 1^{17} \pmod{40}$

Зад 16

$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, $T = \langle 3 + \sqrt{2} \rangle =$

$\{(3 + \sqrt{2})(x + y\sqrt{2}) \mid x + y\sqrt{2} \in R, x, y \in \mathbb{Z}\}$

Да се Дока че $T = T_0 = \{a + b\sqrt{2} \in R \mid$

$a \equiv 3b \pmod{7}\}$ и

$R/T \cong \mathbb{Z}_7$

Елементите на T са от вида

$(3 + \sqrt{2})(x + y\sqrt{2}) = (3x + 2y) + \sqrt{2}(x + 3y) =$

$a + b\sqrt{2}$ с $\begin{cases} a = 3x + 2y \\ b = x + 3y \end{cases}$

За $T \subseteq T_0$ забелязваме

че за елементи на T е в сила

$a - 3b = (3x + 2y) - 3(x + 3y) =$

$3x + 2y - 3x - 9y = -7y \in 7\mathbb{Z}$

следователно $a \equiv 3b \pmod{7}$ и $T \subseteq T_0$

За $T_0 \subseteq T$ трябва да докажем че

всеки елемент (x, y) на сис-ма

(1) с $a \equiv 3b \pmod{7}$ са в

цели коефициенти $x, y \in \mathbb{Z}$

$\left| \begin{matrix} a = 3x + 2y \\ b = x + 3y \end{matrix} \right| \begin{matrix} (-3) \\ (2) \end{matrix} \Rightarrow$ имаме

$-7x = 2b - 3a \quad x = \frac{3a - 2b}{7} \in \mathbb{Z}$

защото $3a \pmod{7} = 3 \cdot 3b \pmod{7}$

$9b \pmod{7} = 2b \pmod{7}$

$3a - 2b \in 7\mathbb{Z}$ и $x = \frac{3a - 2b}{7} \in \mathbb{Z}$

$\left|\begin{matrix} a = __ \\ b = __ \end{matrix}\right| \left\{\begin{matrix} 1 \\ (-3) \end{matrix}\right\} \Rightarrow$ имаме

от $a - 3b = 7y$ имаме

$y = -\frac{(a-3b)}{7} \in \mathbb{Z}$ т.к.

$a - 3b \in 7\mathbb{Z} \Rightarrow I_0 \subset I$

Търсим кер $\varphi: \mathbb{Z} \to \mathbb{Z}_7$

т.е. $\ker \varphi = \mathbb{Z}_7$, $\ker \varphi = I = I_0$

Нека $\varphi(a + b\sqrt{2}) = (a - 3b) \pmod 7$

Полиноми

Пръстенът на полиномите на една променлива

Нека R е комутативен пръстен с единица 1_R

Деф

Моном на x с коефициент $c \in R$ е $\underset{\text{краен, } n \geq 0}{cx^n} = \begin{cases} c & \text{за } n = 0 \\ \underbrace{x \cdot \ldots \cdot x}_{n} & \text{за } c = 1_R \end{cases}$

Ако $c \neq 0$ казваме, че cx^n е от степен $\deg(cx^n) = n$

Деф

Крайните суми $f(x) = \sum_{i=0}^{n} a_i x^i$ на мономи $a_i x^i$ на x с коефициенти $a_i \in R$ се наричат полиноми на x с коефициенти на R.

Мн-то на полиномите на x с коефициенти от R се бележи с $R[x]$

Деф

Старшият член на $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ е мономът от максимална степен с ненулев коефициент

$LT(f) = a_n x^n$ за $a_n \in R / \{0_R\}$
старшият коефициент на
$f(x) \neq 0_R$ е $LC(f) = a_n =$
коефициента $LT(f)$
степента $\deg LT(f) = n$
се нарича степен на
полинома $f(x) \neq 0_R$
Полагаме $\deg 0_R = -\infty$

индексация $f = \sum_i a_i x^{n-i}$ $n = \deg f$

Деф
Полиномите $f(x) = \sum_i a_i x^i$ и
$g(x) = \sum_i b_i x^i$ са равни ако
$a_i = b_i$ за $i \geq 0$
Равни полиноми $f(x)$ и $g(x)$
задават еднакви съответни
ф-ии $f: R \to R$ и $g: R \to R$
$\exists!$ т различни полиноми
f и $g \in R[x]$ задаващи
еднакви съответни ф-и
$f = g : R \to R$
Тр

Различните полиноми
x и x^p задават една и
съща ф-я $x = x^p : \mathbb{Z}_p \to \mathbb{Z}_p$

~~Принцип за съвпадение на ф-ии~~

Деф
$f(x) + g(x) = \sum_i a_i x^i + \sum_i b_i x^i =$
$\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$

Тв
$\deg(f+g) \leq \max(\deg f, \deg g)$
с равенство $\deg(f+g) = \max$
$(\deg(f), \deg(g)) \Leftrightarrow \deg f \neq \deg g$
или $\deg f = \deg g$ и
$LC(f) + LC(g) \neq 0_R$

Деф. Произведение на полиноми
$f(x) g(x) = \sum_{i=0}^{n} (a_i x^i) \sum_{i=0}^{m} (b_i x^i) =$
$\sum_{i=0}^{n+m} \left(\sum_{s=0}^{i} a_s b_{i-s} \right) x^i$!!!

ТБ.

Ако R е комутативна област, а 1 ца то за $\forall f,g \in R[x] \Rightarrow \deg(fg) = \deg(f) + \deg(g)$. За $f \neq 0$ $\in R[x]$ нарами $LT(fg) = LT(f)LT(g)$

Док

Ако $f,g \in R[x] / 0_R$ то $LT(f) = a_n x^{n+m}$ и $a_n \neq 0_R$ в областа R с $a_n \neq 0_R$ от друга страна $LT(f)LT(g) = (a_n x^n)(b_m x^m) = a_n b_m x^{n+m} \Rightarrow \deg(fg) = \deg LT(fg) = \deg LT(f)LT(g) = \deg f + \deg g$ за $f,g \in R[x] / 0_R$ Ако $f = 0_R$ то $0_R g = 0_R$ за $\forall g \in R[x] / 0_R$ $\deg 0_R = \deg(0_R g) = \deg 0_R + \deg g \Rightarrow \deg g = -\infty$ $\notin$

ВА 29.05

$\exists$ - не на корен не лежащи в подходящо разширение на полето от коефициенти.

Ф-ли на Виет

ТБ

Нека F е поле, $f(x) \in F[x] / F$ В такъв случай $\exists_{ст} E := F[x]/\langle f \rangle$ е поле $\Leftrightarrow f(x)$ е неразложим над F. В такъв случай F се влага в E чрез ПП-то $F + \langle f \rangle / \langle f \rangle$ и $\alpha = x + \langle f \rangle$ е корен на $f(x)$ от E Док $\Rightarrow$

Ако $E = F[x]/\langle f \rangle$ е поле и допуснем че $f = f_1 f_2$ е разложение с $f_1, f_2 \in F[x]$ $\deg f_1, \deg f_2 < \deg f$, $\Rightarrow (f_1 + \langle f \rangle)(f_2 + \langle f \rangle) = f_1 f_2 + \langle f \rangle = f + \langle f \rangle = \langle f \rangle = 0_E$ и полето E има делители на нулата $f_1 + \langle f \rangle \neq \langle f \rangle$

~~$F_k = F_1 / F$~~ $E_1 \cdot f_2$ - може

По-точно ако $f_i + \langle f \rangle = \langle f \rangle$, то $f_i \in \langle f \rangle \Rightarrow f_i = fg$.
Но $f_i \neq 0_F$, т.е. $g_i \neq 0_F$
$\deg g_i \geq 0$ и $\deg f_i = \deg f + \deg g_i \geq \deg f$ - противоречие. Това доказва неразложимостта на f над F.
Дали $\langle f \rangle$ е максимален? Ще докажем, че $\Phi_{\Pi_{\Sigma_1}} F[x]/\langle f \rangle$ на комутативния п-к с 1-ца $F[x]$ е комут. п-к с 1-ца $1_F + \langle f \rangle$.
Достатъчно е да проверим, че $\forall$-ки ненулев елемент $g + \langle f \rangle \neq \langle f \rangle$ от E има обратен относно умн. за да получим, че E е поле. От $g \notin \langle f \rangle \Rightarrow$ f не дели g и $HOД(f,g) = 1$. Съгласно неразложимостта на f над F. Тъждеството на Безу $fu + gv = 1$, дава $(g + \langle f \rangle)^{-1} = v + \langle f \rangle$, защото $(g + \langle f \rangle)(v + \langle f \rangle) = gv + \langle f \rangle = 1_F - fu + \langle f \rangle = 1_F + \langle f \rangle$.
Знаем, че за ПП-на F на $F[x]$ и $\forall$ идеала $\langle f \rangle \triangleleft F_{[x]}$ е в сила изоморфизма на пръстени $F/F \cap \langle f \rangle \cong F + \langle f \rangle / \langle f \rangle$. $\forall$ Ще докажем, че $F \cap \langle f \rangle = \{0_F\}$, за да получим, че $F = F/F \cap \langle f \rangle$ е изоморфно на $F + \langle f \rangle / \langle f \rangle \leq_{\Pi\Pi_\Phi} E_\Pi$.
Нагледно, ако допуснем, че $\exists\, c \in F^* \cap \langle f \rangle$, то $c = fg$ за $g \in F_{[x]} \setminus \{0_F\}$
Тогава $0 \leq \deg c = \deg f + \deg g \geq \deg f \in \mathbb{N}$.
Противоречието доказва $F \cap \langle f \rangle = \{0_F\}$

Остава да проверим че $\alpha = x + \langle f \rangle \in E$ е корен на $f(x) = \sum_{i=0}^{n} a_i x^i$. Трябва да е изпълнено $f(x + \langle f \rangle) = \sum_{i=0}^{n} a_i (x + \langle f \rangle)^i =$
$\sum_{i=0}^{n} (a_i + \langle f \rangle)(x + \langle f \rangle)^i =$
$\sum_{i=0}^{n} (a_i x^i + \langle f \rangle) = (\sum_{i=0}^{n} a_i x^i) + \langle f \rangle =$
$f(x) + \langle f \rangle = \langle f \rangle = 0_E$ □

Деф
Нека полето F е Поле на полето E тогава казваме че E е разширение на F

Сл 1 Нека F е поле, $f(x) \in F[x]$ F
Тогава $\exists$ разширение E_1 на F в което f има корен $\alpha_1 \in E_1$.

Док
Нека $f = f_1 \cdot \ldots \cdot f_n$ е разлагане на $f(x)$ в произведение на неразложими над F полиноми $f_i(x) \in F[x]$

Тогава $E_1 := F[x] / \langle f_1 \rangle$ е поле в което f_1 има корен $\alpha_1 = x + \langle f_1 \rangle$. Сега $f(\alpha_1) = f_1(\alpha_1) f_2(\alpha_1) \ldots f_n(\alpha_1) = 0_{E_1} \cdot f_2(\alpha_1) \ldots f_n(\alpha_1) = 0_{E_1}$ и $\alpha_1 \in E_1$ е корен на $f(x)$ □

Сл 2
Нека F е поле, $f(x) \in F[x] \setminus F$
Тогава $\exists$ разширение E на F в което $f(x)$ се разлага в линейни множители
$f(x) = LC(f)(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$
$\alpha_1, \ldots, \alpha_n \in E$ Док
С индукция по $n := \deg(f) \in \mathbb{N}$
За $n = 1$, $f(x) = a_1 x + a_0$
$\in F[x]$, $a_1 \neq 0_F$ тогава $E := F \ni -a_0 a_1^{-1}$ е единствен корен на $a_1 x + a_0 = 0_F$
В общия случай по Сл 1 $\exists$ разширение $E_1 \supseteq F$ в което $f(x)$ има корен $\alpha_1 \in E_1$

Ш

Нека $f(x) \in E_1[x]$ има разлагане $f(x) = (x-\alpha_1) f_2(x)$ с $f_2(x) \in E_1[x]$, $\deg f_2 = \deg f - 1 = n-1$. по индукция - предположение $\exists$ разширение $E \supseteq E_1$ т.ск $f_2(x) = LC(f_1)(x-\alpha_2)\dots(x-\alpha_n)$ с $LC(f_1) = LC(f)$ и $\alpha_2, \dots \alpha_n \in E$

Нека $f(x) = LC(f)(x-\alpha_2)\dots(x-\alpha_n)$ се разлага в линейни множители над E, т.е $\alpha_1, \dots \alpha_n \in E$ □

Ф-ли на Виет

Нека $F[x] \ni f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n = a_0(x-\alpha_1)\dots(x-\alpha_n)$ с $\alpha_1, \dots \alpha_n \in E$ за подходящо разширение E над F. Сравняваме коефициентите на $x^{n-1}, x^{n-2}, \dots x^1, x^0$ в двете страни

$x^{n-1}: a_1 = a_0(-\alpha_1 - \alpha_2 - \dots - \alpha_n)$

$x^{n-2}: a_2 = a_0 \sum_{1 \le i < j \le n} (-\alpha_i)(-\alpha_j) = a_0 \sum_{1 \le i < j \le n} \alpha_i \alpha_j$

$x^{n-i}: a_i = a_0 \sum_{1 \le j_1 < \dots < j_i \le n} (-\alpha_{j_1}) \dots (-\alpha_{j_i}) = a_0 (-1)^i \sum_{1 \le j_1 < \dots < j_i \le n} \alpha_{j_1} \dots \alpha_{j_i}$

$x^0: a_n = a_0 (-1)^n \alpha_1 \dots \alpha_n$

$$\sum_{1 \le j_1 < \dots < j_i \le n} \alpha_{j_1} \dots \alpha_{j_i} = (-1)^i \frac{a_i}{a_0}, \quad 1 \le i \le n$$

Ф-ли на Виет

елементарни симетрични полиноми от лявата страна на Ф-лата

$$f(x_1, \dots x_n) = g\left(\sum_{1 \le j_1 < \dots < j_i \le n} x_{j_1} \dots x_{j_i}, \dots, x_1 \dots x_n\right)$$

$g \in F[x_1, \dots x_n]$

Зад Нека F е поле, $f(x) \in F[x]$ / F е неразложим над F полином от $\deg(f) = n \in \mathbb{N}$. Тогава полето $E = F[x]/\langle f \rangle$ съвпада с мн-то $E_0 := \{\sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \mid b_j \in F\}$ и $E = E_0$ е изоморфно на F^n като линейно пр-во над F.

Реш

Ясно е че $E_0 \subseteq E = \{g(x) + \langle f \rangle \mid g(x) \in F[x]\}$. За обратното ползваме алгоритъма за

$q(x) \in F[x]$ и нека ℓ е частно $q \in F[x]$ и остатък $r \in F[x]$ $q = \ell q + r$ $\deg r < \deg \ell = n$, тогава $q - \ell q = r = \sum_{j=0}^{n-1} c_j x^j$ тогава $q + \langle \ell \rangle = q - \ell q + \langle \ell \rangle = r + \langle \ell \rangle = \sum_j c_j x^j + \langle \ell \rangle \in E_0$

Това доказва, че $E = E_0$

Нека $\varphi_i = F^n \to E = E_0$

$\varphi(c_0 \dots c_{n-1}) = \sum_{j=0}^{n-1} c_j x^j + \langle \ell \rangle$

Твърдим, че φ е F-линейно

т.е. $\varphi((c_0 \dots c_{n-1}) + (c_0' \dots c_{n-1}')) = \varphi(c_0 + c_0', \dots, c_{n-1} + c_{n-1}') =$

$\sum_{j=0}^{n-1} (c_j + c_j') x^j + \langle \ell \rangle = \sum c_j x^j + \langle \ell \rangle +$

$\sum c_j' x^j + \langle \ell \rangle = \varphi(c_0 \dots c_{n-1}) + \varphi(c_0' \dots c_{n-1}')$

Нека $\lambda \in F$ тогава $\varphi(\lambda(c_0 \dots c_{n-1})) = \varphi(\lambda c_0 \dots \lambda c_{n-1}) = \sum_j (\lambda c_j) x^j + \langle \ell \rangle$

$= \lambda(\sum c_j x^j + \langle \ell \rangle) = \lambda \varphi(c_0 \dots c_{n-1})$

φ е еднозначно еднозначно

т.к. $\ker \varphi = E_0 = E$

Следователно $\exists q(x) \in F[x]$, т.е. $ch = \ell q$. Допуснем, че $h \neq 0_F$ тогава $q \neq 0_F$, т.е. $\deg q \geq 0$. Оттук $n-1 \geq \deg(h) = \deg(\ell q) = \deg \ell + \deg q \geq \deg \ell = n$. Противоречие. Следователно $h = 0_F$ и φ е еднозначно еднозначно $\Rightarrow$ φ е линеен изоморфизъм

Зад 4

Да се определи дали $E_i = F_i[x] / \langle f_i \rangle$ е поле и ако е поле да се намери $\dim_{F_i} E_i$?

1) $E_1 = \mathbb{Z}_5$, $f_1 = x^3 + \bar{3}x^2 - \bar{1} \in \mathbb{Z}_5[x]$

Полином f_1 от $\deg f_1 = 3$ е разложим $\overset{\text{Нар. Ф}}{\Rightarrow}$ има корен в $\mathbb{Z}_5$

	$\bar{1}$	$\bar{3}$	$\bar{0}$	$-\bar{1}$	$f_1(\bar{0}) = -\bar{1}$
$\bar{1}$	$\bar{1}$	$-\bar{1}$	$-\bar{1}$	$-\bar{2} \neq \bar{0}$	
$-\bar{1}$	$\bar{1}$	$\bar{2}$	$-\bar{2}$	$\bar{1} \neq \bar{0}$	$\mathbb{Z}_5 = \{\bar{0}, \pm\bar{1}, \pm\bar{2}\}$
$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$-\bar{1} \neq \bar{0}$	
$-\bar{2}$	$\bar{1}$	$\bar{1}$	$-\bar{2}$	$\bar{3} = -\bar{2} \neq \bar{0}$. $\Rightarrow$	

$f_1(x)$ е неразл над $\mathbb{Z}_5$ и