2.3. Корни из единицы. Круговые многочлены

<u>Теорема</u> (признак Эйзенштейна): $f \in \mathbb{Z}[x]$
$f = a_0 + a_1 x + \ldots + a_n x^n$, p — простое.
Если $\forall\ 0 \le i \le n-1$ $\ p \mid a_i$, $\ p^2 \nmid a_0$, то
f — неприводим в $\mathbb{Z}$. $\quad p \nmid a_n$

<u>Д</u>: Предположим $\exists\ g, h \in \mathbb{Z}[x]: f = gh$
mod p: $\quad f(x) \equiv a_n x^n \ (p)$ или
$\bar{f} = a_n x^n$ в $\mathbb{F}_p[x]$.
$\bar{f} = \bar{g} \cdot \bar{h}$, т.е. $a_n x^n = \bar{g} \cdot \bar{h}$
$\mathbb{F}_p[x]$ — одн. разл. на множ. $\Rightarrow$
$\bar{g} = b_m x^m$, $\bar{h} = c_\ell x^\ell$, $\quad m + \ell = n$.

$g = \sum_{i=0}^{m} b_i x^i, \quad h = \sum_{i=0}^{l} c_i x^i \in \mathbb{Z}[x]$

$\bar{g} = b_m x^m \quad \bar{h} = c_l x^l \in \mathbb{F}_p[x]$

$\Rightarrow \quad p \mid b_i \quad 0 \le i \le m-1, \quad p \mid c_j \quad 0 \le j \le l-1$

$\Rightarrow \quad p \mid b_0 \quad p \mid c_0 \quad \Rightarrow \quad p^2 \mid b_0 c_0 = a_0$ — $><$ ∎

Теорема (Лемма Гаусса): $f \in \mathbb{Z}[x]$

f — непр. $/ \mathbb{Z} \Leftrightarrow f$ непр $/ \mathbb{Q}$

□ Пусть $f = gh, \quad g, h \in \mathbb{Q}[x]$

$\exists\ a, b \in \mathbb{Q} \quad a g(x), b h(x) \in \mathbb{Z}[x]$ — примитивн

(прим $\Leftrightarrow$ НОД коэфф. $= 1$)

$f_1(x) = ab f(x) = \underbrace{a g(x)}_{g_1(x)} \cdot \underbrace{b h(x)}_{h_1(x)}$

Пусть $p \mid ab$, тогда

в $\mathbb{F}_p[x]$ $\quad 0 = \bar{f}_1 = \bar{g}_1 \cdot \bar{h}_1 \Rightarrow \bar{g}_1 = 0$ или $\bar{h}_1 = 0$

$\Rightarrow p \mid$ коэфф. $g_1(x)$ или $p \mid$ коэфф. $h_1(x)$

$g_1 = ag$, $\quad h_1 = bh$ — примитивные

$\Rightarrow \neg\exists$ таких p — пр. $\Rightarrow ab = 1$

$\Rightarrow f = g_1 h_1 \in \mathbb{Z}[x]$ ∎

<u>Следствие</u>: p — пр. $\quad f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$

$f(x)$ — неприв. $/\ \mathbb{Q}$

□ Рассм. $f(x+1)$

т.к. $f(x) = \dfrac{x^p - 1}{x - 1}$ $\quad f(x+1) = \dfrac{(x+1)^p - 1}{x} =$

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

$p \mid$ $\qquad p^2 \nmid p$

Призн. Эйзенш. $\Rightarrow f(x+1)$ — неприв. $\Rightarrow f(x)$ — неприв. ∎

Опр: $f \in K[x]$ форм. производная:

$f(x) = a_n x^n + \dots + a_0$, $\quad f'(x) = n a_n x^{n-1} + \dots + a_1$.

Лемма: Св-ва:

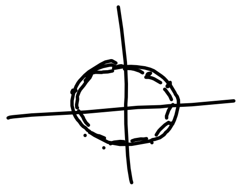
1) $(f+g)' = f' + g'$

2) $(fg)' = f'g + fg'$

□ ... ∎

Лемма: $f \in K[x]$, K - произв. $\alpha \in K$ - кратн. ($(x-\alpha)^a \mid f(x)$, $a \geq 2$) $\Leftrightarrow f'(\alpha) = 0$

□ ... ∎



Теор.

$x^n - 1 \ / \ \mathbb{C}$ $\quad x^n - 1 = \prod_{k=1}^{n} (x - e^{2\pi i \frac{k}{n}})$

$U_n = \langle e^{2\pi i \frac{1}{n}} \rangle$ - группа корней степени n из ед.

обозн. $\sqrt[n]{1}$

$\alpha \in U_n$ наз. примитивным $\sqrt[n]{1}$, если $U_n = \langle \alpha \rangle$, т.е. α^i — разл.

$x^n - 1$ над простым K, в $\mathbb{F}_q$?

Опр: K — поле, поле разложения $x^n - 1$ наз. n-м круговым полем, обозн. $K^{(n)}$.

Мн-во корней $x^n - 1$ в $K^{(n)}$ обозн. U_n.

$\mathrm{char}\, K = p$ (допускаем $p = 0$)

Теорема: 1) если $p \nmid n$, то U_n — циклич. гр. пор. n.

2) если $p \mid n$, $n = p^e m$, $p \nmid m$, то $K^{(n)} = K^{(m)}$, $U_n = U_m$,

корни $x^n - 1$ в $K^{(n)}$ — n-элем. U_n с
примит. p^e

$\square$ $n \geq 2$. $(x^n - 1)' = n x^{n-1} = 0$ при
досл. кратн. $x = 0$ (если $p \nmid n$). в $K^{(n)}$ $x^n - 1$
не имеет кратных корней, $|U_n| = n$

Докажем, что U_n — циклич.

Пусть $n = p_1^{e_1} \dots p_t^{e_t}$.

Многоч. $x^{\frac{n}{p_i}} - 1$ имеет не более $\frac{n}{p_i}$
корней, все корни $\in U_n$.

$\frac{n}{p_i} < n \Rightarrow \exists\, \alpha_i \in U_n : \alpha_i^{n/p_i} - 1 \neq 0$

Положим $\beta_i = \alpha_i^{n/p_i^{e_i}}$.

$(\beta_i)^{p_i^{e_i}} = \alpha_i^n = 1 \Rightarrow$ пор. $\beta_i \mid p_i^{e_i}$
т.е. имеет вид $p_i^{s_i}$ $s_i \leq e_i$

Но $\beta_i^{p_i^{e_i-1}} = \alpha_i^{n/p_i} \neq 1$. т.о. пор $\beta_i = p_i^{e_i}$

Покажем, что $\beta = \beta_1 \cdots \beta_t$ — пор. n.

Допустим, что пор. $< n$, пор $\beta \mid n$

$n = p_1^{e_1} \cdots p_t^{e_t} \Rightarrow \exists i$ пор $\beta \mid \frac{n}{p_i}$

пусть это $\frac{n}{p_1}$

$$1 = \beta^{n/p_1} = \beta_1^{n/p_1} \cdots \beta_t^{n/p_1}$$

$2 \leq i \leq t$ $\quad p_i^{e_i} \mid \frac{n}{p_1} \Rightarrow \beta_i^{n/p_1} = 1$

$\Rightarrow \beta_1^{n/p_1} = 1 \Rightarrow$ пор $\beta_1 \mid \frac{n}{p_1}$ — $><$

т.к. пор $\beta_1 = p_1^{e_1}$

Т.о. $\beta \in U_n$ — пор n $\quad U_n = \langle \beta \rangle$

2) $\operatorname{char} k = p$, $p \mid n$ $\quad x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$ ■

Опр.: $\mathrm{char}\, k = p \nmid n$. Пусть U_n — мн. прим. $\sqrt[n]{1}$.

Следствие: число прим. $\sqrt[n]{1}$ $= \varphi(n)$

Опр.: $\mathrm{char}\, k = p \nmid n$, ε — прим. $\sqrt[n]{1}$

$\Phi_n(x) = \prod\limits_{\substack{s \bmod n \\ (s,n)=1}} (x - \varepsilon^s)$ наз. n-ым круговым многочленом $/ k$

$\deg \Phi_n = \varphi(n)$, $\Phi_n \in k^{(n)}[x]$.

Теорема: $\mathrm{char}\, k = p \nmid n$

1) $x^n - 1 = \prod\limits_{d \mid n} \Phi_d(x)$

2) $\Phi_n(x)$ опр. над простым подполем k. Если это подполе $\mathbb{Q}$, то $\Phi_n(x) \in \mathbb{Z}[x]$

□ 1) $x^n - 1 = \prod_{i=0}^{n-1}(x-\xi^i) = \prod_{d\mid n}\prod_{(i,n)=d}(x-\xi^i)$

$(i,n)=d \Rightarrow$ пор $\xi^i = \frac{n}{d}$

$\left((\xi^i)^{n/d} = (\xi^n)^{i/d} = 1\right)$

$i = ds$ $\quad (s, \frac{n}{d}) = 1 \quad \xi^i = \xi^{ds} = \zeta^s$

ζ — перв. кор. $\frac{n}{d}$

т.е. $\prod_{(i,n)=d}(x-\xi^i) = \prod_{(s,\frac{n}{d})=1}(x-\zeta^s) =$

$= \Phi_{\frac{n}{d}}(x)$

$x^n - 1 = \prod_{d\mid n}\Phi_{\frac{n}{d}}(x) = \prod_{d\mid n}\Phi_d(x)$ ■

2) по индукции. $\Phi_1(x) = x-1$

Пусть $n > 1$, $\Phi_d(x)$ $1 \le d < n$

$\Phi_n(x) = \dfrac{x^n - 1}{f(x)}$ $\quad f(x) = \prod\limits_{\substack{d \mid n \\ d < n}} \Phi_d(x) \in K[x]$ $\quad (\mathbb{Z}[x])$

Делим уголком с остат. $x^n - 1$ на $f(x)$

$x^n - 1 = f q_1 + r_1$, $\quad f = r_1 q_2 + r_2$, $\quad \dots$

$r_{n-1} = r_n q_n$, $\quad \dots$ ■

<u>Теорема</u>. $\Phi_n(x) \in \mathbb{Z}[x]$ — неприв. над $\mathbb{Q}$

□ д-во в книге Ч ■

<u>Лемма</u>: $\operatorname{char} K = p \nmid n$, 1) η перв. $\sqrt[n]{1}$ $\Rightarrow$ 2) $\Phi_n(\eta) = 0$ $\quad$ 2) если $\operatorname{char} K = 0$, т.е. $(\mathbb{Z}$

то $\Leftrightarrow$

□ 1) $x^n - 1 = \prod\limits_{d \mid n} \Phi_d(x)$

$1 = \eta^0, \eta_1, \dots, \eta^{n-1}$ — различ., $\quad \eta^m \neq 1$, $1 \le m \le n-1$

Покажем $\forall d \mid n,\ d < n \quad \Phi_d(\xi) \neq 0$

$\Phi_d(x) \mid x^d - 1$, $\quad \Phi_d(\xi) = 0 \Rightarrow \xi^d - 1 = 0$

— пр. $\xi^m \neq 1$, $\quad m < n$

Т.о. $\Phi_n(\xi) = 0$.

2) $\Leftarrow$ $\quad \Phi_n(\xi) = 0$, $\quad \Phi_n(x) \mid x^n - 1 \Rightarrow \xi^n = 1$

Предположим $\xi^m = 1$, $\quad m < n$

$\Phi_n(x)$ — неприв. $/\mathbb{Z} \Rightarrow (\Phi_n, x^m - 1) = 1 \quad (m < n)$

$\exists \quad r, s \in \mathbb{Z}[x] \quad r(x)\Phi_n(x) + s(x)(x^m - 1) = 1$

$$r(\xi)\underbrace{\Phi_n(\xi)}_{0} + s(\xi)\cdot(\xi^m - 1) = 1 \Rightarrow \xi^m - 1 \neq 0$$

т.е. ξ — прим. $\sqrt[n]{1}_n$ ∎

$k = \mathbb{F}_p$, $\quad p \nmid n$

__Теорема__: $\Phi_n(x) = F_1(x) \dots F_l(x)$,

$F_i(x) \in \mathbb{F}_p[x]$ — непр., разл., $\deg F_i = d$

$l = \frac{\varphi(n)}{d}$, $\quad$ d — пор. p в $n(\mathbb{Z}/n\mathbb{Z})$

(наим.: $p^d \equiv 1 \ (n)$)

(ПЕРЕРЫВ до 16:00)

$\square$ Пусть ζ — прим. $\sqrt[n]{1}$ / $\mathbb{F}_p$

$\zeta \in \mathbb{F}_{p^k}$ — расш. $\mathbb{F}_p$ $\quad \zeta^n - 1 = 0$

$\Leftrightarrow \zeta^{p^k} - \zeta = 0$

$\Rightarrow p^k - 1 \equiv 0 \ (n)$, пусть d — минимальное такое k.

т.е. $p^d \equiv 1 \ (n)$

$\zeta \in \mathbb{F}_{p^d} \Rightarrow \mathbb{F}_p^{(n)} \cong \mathbb{F}_{p^d}$

ζ — перв. $\sqrt[n]{1} \Rightarrow \Phi_n(\zeta)$

Тогда $F_1(X) = (X-\zeta)(X-\zeta^p)\dots(X-\zeta^{p^{d-1}})$

$(F_1(X))^p = (X^p-\zeta^p)\dots(X^p-\underbrace{\zeta^{p^d}}_{=\zeta}) = F_1(X^p)$

$(f \in \mathbb{F}_p[X] \Leftrightarrow f(X)^p = f(X^p))$

$\Rightarrow F_1(X) \in \mathbb{F}_p[X]$

Для ζ^s, $(s,n)=1$ $\quad \zeta^s$ — перв. $\sqrt[n]{1}$

$\Rightarrow \Phi_n(\zeta^s)$.

$F_s(X) = (X-\zeta^s)\dots(X-\zeta^{sp^{d-1}})$

$\zeta^{sp^i}, \zeta^{sp^j}$ — попарно разл.

$(\zeta^{sp^i} = \zeta^{sp^j} \Leftrightarrow sp^i \equiv sp^j\ (n) \Leftrightarrow$

$p^i \equiv p^j\ (n)$ — ... $><$ с опр. d $)$

$(F_s(X))^p = F_s(X^p) \Rightarrow F_s(X) \in \mathbb{F}_p[X]$

$\varphi(n)$ чисел s : $(s,n)=1$

$$\Phi_n(X) = \prod_{\substack{s \bmod n \\ (s,n)=1}} (X - \eta^s) = \prod_{(s,n)=1} F_s(X)$$

$\deg F_s = d \Rightarrow \dfrac{\varphi(n)}{d}$ сомножит.

$F_s(X)$ — непр. в $\mathbb{F}_p[X]$.

Пусть $F_s(X) = g(X)\, h(X)$

$F_s(\eta^s) = 0 \Rightarrow g(\eta^s) = 0 \vee h(\eta^s) = 0$

Допустим $g(\eta^s) = 0$. $\eta^{sp}, \dots, \eta^{sp^{d-1}}$

— корни g, разл. d штук.

$\Rightarrow g = F_s,\ h = 1$ ■

Теорема: Аналогично, для $\mathbb{F}_q$ ...

$\square$ ... $\boxtimes$

Лемма: f — непр., $\deg f = k$

$f \mid x^{2^n} - x \iff k \mid n$

$\square$ ... $\boxtimes$

Теорема: $\mathbb{F}_q$: $\prod\limits_{\substack{f \text{ - непр., унит.} \\ \deg f \mid n}} f = x^{2^n} - x$

$\square$ ... $\boxtimes$