1 Конечные поля

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = GF(p) \tag{1}$$

$$f, g \in \mathbb{F}_p[x] \tag{2}$$

$$f \in \mathbb{F}_p[x] \text{ - неприводим} \tag{3}$$

$$g|f \Rightarrow g \in \mathbb{F}_p or f = \alpha g \tag{4}$$

$$11gcd(f, g) = d = d(x) \tag{5}$$

$$I : \forall f \in \mathbb{F}_p[x]\ f = c\prod f_i^{m_i} \tag{6}$$

f_i - неприводимый унитарный

$$\mathbb{F}_p[x] - \text{кольцо главных идеалов } \forall \text{идеала } I \exists \text{неприводимый } f : I = (f) \tag{7}$$

Теорема 1. *$f \in \mathbb{F}_p[x]$ - неприводимый. $F_p[x]/f$ - поле из p^n элементов, $n = deg(f)$. Тогда $\mathbb{F}_p[x]/f$, $\mathbb{Z}/(p) = \mathbb{F}_p$*

Доказательство. $a(x) \in \mathbb{F}_p[x]$ $\exists! r(x) \in \mathbb{F}_p[x] : a \equiv r(f) \leftrightarrow f|a - r$ $\exists!$ доказательство Пусть $\exists r_1, r_2$ $r_1 \equiv a(f), r_e \equiv a(f) \Rightarrow$ вы стёрли.........

$r(x) = a_1x^{n-1} + ... + a_0$ $a_1 \in \mathbb{F}_p$ есть p^n штук вот таких многочленов $|\mathbb{F}_p(x)/(f)| = p^n$ Обозначим $O = (f)$

$$E = \{f \in \mathbb{F}_p[x] : g \equiv 1(f) \tag{8}$$

$A \neq O$ $a(x) \in A \Leftrightarrow f\ x\ a \Leftrightarrow (f, a) = (1) = \mathbb{F}_p[x] \Leftrightarrow \exists u, v \in \mathbb{F}_p[x]$ $fu + av = 1 \Rightarrow av = 1(f)$ то есть $V = [v(x)]$ класс в $\mathbb{F}_p[x]$

Докажем единсвтенность

$AW = E, W \neq V$ $\exists w(x), w \not\equiv v()$ $aw = 1(f); av = 1(f)$ $a(w - v) = 0(f)$ $fxa \Rightarrow f|w - v$ □

Отсюда $q = p^n, \mathbb{F}_q = \mathbb{F}_p[x]/(f)$. $def(f) = r, f-$ неприводим

Теорема 2.

$$\forall n \geq 1 \exists f \in \mathbb{F}_p[x] \tag{9}$$

неприводимый. $deg(f) = 1$

Введём $N(g) = Ng = p(deg(g))$ для $g \in \mathbb{F}_p[x]$ Эта функция мультипликативна. $N(fg) = Nf\ Ng$ Аналог дзета функции. $\zeta(s) = \prod_p^*(1 - \frac{1}{(Nf)^s})^{-1}$ $\prod^*$ - произвдение по всем неприводимым унитарным многочленам из кольца Область сходимости $\zeta(s) = \sum_{n=1}^{\inf} \frac{1}{n^3} = \prod_{p-\text{простые}}(1 - \frac{1}{p^3})^{-1}$ при $Re(s) > 1$

$$\zeta = \prod_p^*(1 + \sum_{m=1}^{\inf} \frac{1}{(Nf)^{ms}})^{-1} = 1 + \sum_g^* \frac{1}{(Nf)^s} \tag{10}$$

$$\sum^* - \text{сумма по унитарным } g \in \mathbb{F}_p[x] \tag{11}$$

$$= 1\sum_{n=1}^{\text{inf}} \sum_{g, deg(g)=n} = \frac{1}{(Ng)^s} \tag{12}$$

$$= 1 + \sum_{n=1}^{\text{inf}} p^n \frac{1}{p^{ns}} \tag{13}$$

$$= (1 - \frac{p}{p^s})^{-1} \tag{14}$$

Количество неприводимых унитарных мночленов где $deg(g) = n$ - $\nu(n)$

$$\prod_{n=1}^{\text{inf}} (1 - \frac{1}{p^{ns}})^{-\nu(n)} = \prod_{f}^{*} = (1 - \frac{1}{(Nf)^s})^{-1} \tag{15}$$

прологорифмируем:

$$\sum_{n=1}^{\text{inf}} (-\nu(n) log(1 - \frac{1}{p^{ns}} = -log(1 - \frac{p}{p^s}) \tag{16}$$

$$log(1 - \tau) = \sum_{m=1}^{\text{inf}} \frac{1}{m} \tau^m \tag{17}$$

У доказательства есть бонус.

$$\sum_{n=1}^{\text{inf}} \nu(n) \sum_{l=1}^{\text{inf}} \frac{1}{l} \frac{1}{p^{lns}} = \sum_{m=1}^{\text{inf}} \frac{1}{m} \frac{p^m}{p^{ms}} \tag{18}$$

$$\sum_{n=1}^{\text{inf}} \nu(n) \sum_{l=1}^{\text{inf}} \frac{1}{l} \frac{1}{p^{lns}} = \sum_{n} \sum_{l} \frac{\nu(n)}{l} \frac{1}{p^{ms}} = \sum_{m=1}^{\text{inf}} \sum_{n|m} \frac{\nu(n)}{m/n} \frac{1}{p^{ms}} = \tag{19}$$

$$= (\sum_{n|m} \nu(n) n) \frac{1}{m} \frac{1}{p^{ms}} = \tag{20}$$

$$\sum_{n|m} \nu(n) n = p^m \tag{21}$$

$$\Rightarrow \nu(n) = \frac{1}{n} \sum_{d|m} \mu(d) p^{n/d} \neq 0 \tag{22}$$

Теорема 3.

$$\forall z \in \mathbb{F}_q^*, q - p^n, \mathbb{F}_q = \mathbb{F}_p[x]/(f) \tag{23}$$

Тогда

$$z^{q-1} - 1 = 0 \tag{24}$$

Доказательство. Пусть

$$g \in \mathbb{F}_p[x], Fxf \tag{25}$$

$$\prod_r gr = \prod_r r(f) \tag{26}$$

$$(g^{q-1} - 1) \prod r \equiv 0(f) \tag{27}$$

Следовательно

$$\prod_{z \in \mathbb{F}_q} (x - z) = x^q - x \tag{28}$$

□

Лемма 1.

$$f|x^q - x, deg(f) = d \Rightarrow \tag{29}$$

f имеет d различных корней

Доказательство.

$$x^q - x = f(x)g(x) \tag{30}$$

f(x) - d корней, g(x) - q-d корней
если $< d$ корней у f $\Rightarrow d + (q^1 d) = 1$ у $x^q - x$ □

Теорема 4. *мультипликативная группа $\mathbb{F}_q^*$ циличская то содержит $\phi(q-1)$*

Доказательство.

$$m|q-1; \psi(m) - \text{число элементов поля} \tag{31}$$

Если $\psi(m) > 0$, $\alpha \in \mathbb{F}_q^*$– порядок m. $1, \alpha, ..., \alpha^{m-1}$ - различны корни $x^m - 1$ это все корни $x^m - 1$

$$\forall \beta \in \mathbb{F}_q^* - \text{порядок } |m \tag{32}$$

$$\beta = \alpha^s, r \leq s \leq m - 1 \tag{33}$$

если $(s, m) = d, \alpha^s$ - порядок m/d
Было упражнение что

$$\alpha^s \text{ порядок } m \Leftrightarrow (s, m) = 1 \tag{34}$$

Таким образом если $\psi(m) > 0$ то $\psi(m) = \phi(m)$

$$\sum_{m|q-1} \psi(m) = q - 1 \tag{35}$$

Мы знаем что

$$\sum_{m|q-1} \phi(m) = q - 1 \tag{36}$$

Тогда

$$\sum_{m|q-1} (\phi(m) - \psi(m)) = 0 \Rightarrow \psi(q-1) = \phi(q-1) \tag{37}$$

□