Лекция №2 Конечные поля

Критерий Эйзенштейна

Пусть $P(x) \in \mathbb{Z}[x]$

$a_0 + a_1 x + \dots + a_n x^n$, $\exists p$:

$a_n \not\vdots p$, $a_0, a_1, \dots, a_{n-1} \vdots p$, $a_0 \not\vdots p^2$

Тогда P неприводим в $\mathbb{Z}[x]$ ($\Leftrightarrow$ в $\mathbb{Q}[x]$)

Д-во: если $P = QR$, $\deg Q, \deg R = n$, то $\mathrm{mod}\, p$ $\bar{P} = \bar{Q}\bar{R}$

$\mathbb{F}_p[x] \ni a_n x^n$ $a_k x^k \cdot x^l$

Лучший вариант: k или $l = 0$, тогда l или $k = n$

$\Rightarrow \deg Q$ или $\deg R = n$

$0 < k$, $l < n$

$Q = b_k x^k + \dots + b_0$

$R = c_l x^l + \dots + c_0$

$b_0 \vdots p$, $c_0 \vdots p$

$a_0 = b_0 c_0 \vdots p^2$ - противоречие

Классификация конечных полей

$\mathbb{F}_p$, где p - простое, $\mathbb{Z}/p\mathbb{Z}$

если $P \in \mathbb{F}_p(t)$ - неприводимый многочлен, то (и $\deg P = n$),

$\mathbb{F}_p[t]/P = \mathbb{F} \supset \mathbb{F}_p$

$\mathbb{F}$ - векторное пространство над $\mathbb{F}_p$ с базисом $\underbrace{1, z, z^2, \dots, z^{n-1}}_{n}$

$\deg_{\mathbb{F}_p} \mathbb{F} = n$, $\#\mathbb{F} = p^n$ $(a_1, \dots, a_n)$, $a_i \in \mathbb{F}_p$

$\mathbb{F}$ - конечное поле $\ni \underbrace{1, 2, 3, \dots, 10, \dots}_{m}$ 0 $m = 0$ $m = p \cdot q$

Утверждение если $\mathbb{F}$ - конечное поле, а p - минимальное, такое что $p \cdot 1 = 0$, то

p - простое число $\mathbb{F}_p \subset \mathbb{F}$ - простое подполе в $\mathbb{F}$

p - характеристика $\mathbb{F}$

$\dim_{\mathbb{F}_p} \mathbb{F} = n$

$\#\mathbb{F} = p^n$

Группа $\mathbb{F}$ по сложению $\mathbb{F}_p^n = \underbrace{\mathbb{F}_p \oplus \mathbb{F}_p \oplus \dots \oplus \mathbb{F}_p}_{n \text{ раз}}$

$\mathbb{Z}/p\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/p^n\mathbb{Z}$

Группа по умножению $F^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ " x^{-1} " " x^2

Пример: F_4 таблица сложения

	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

таблица умножения

	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

F_8 таблица сложения

	1	x	x^2	x^3	x^4	x^5	x^6
1	0	x^3	x^6	x	x^5	x^4	x^2
x							
x^2							
x^3							
x^4							
x^5							
x^6							

$1+x^2 = (1+x)^2 = x^6$

$1+x^4 = (1+x)^4 = x^5$

$1+x = x^3 \Rightarrow 1+x^3 = x$

и т. д.

$1+x+x^3$

$F_8 \supset F_2$

$x^3+x+1 = 0$

Тео. $1+x+x^3$ неприводим, т.к нет корней

$F_8 \supset F_4$. тогда F_8 было бы векторным пространством над F_4, $\dim = n$

$\#F_8 = (\#F_4)^n$

$F_8^* \supset F_4^*$

$\mathbb{Z}/7\mathbb{Z} \supset \mathbb{Z}/5\mathbb{Z}$

$F_q \subset F_{q'} \Leftrightarrow q' = q^\ell$ ($F_{81} \not\subset F_{243}$)

Построение поля из q элементов $q = p^n$; F_q.

$F_q^* = \mathbb{Z}/(q-1)\mathbb{Z}$ $\quad x^{q-1} = 1$

$x^q = x$

$P(x) = x^q - x \Rightarrow$ поле разложения, K - конечное расширение F_p

$x^8 - x = x(x^3+x+1)(x^3+x^2+1)(x-1)$

$F_q = \{a \in K,\ т.ч.\ a^2 = a\}$

Остаюсь проверить, что $\#\{a^q = a\} = q$

и они образуют подполе $(a+b)^q = a^q + b^q = a+b$

$(ab)^q = a^q b^q = ab$

корней многочлена a^2-a не больше q, если их нет, то корни кратные,

т.е. $(p, p') \neq 1$

$p = x^q - x, \quad p' = -1$

$(p, p') = 1 \Rightarrow$ кратных корней нет

На самом деле, из цикличности мультипликативной группы $\Rightarrow$

$\Rightarrow \mathbb{F}_q = \mathbb{F}_p(\zeta)$, ζ – первообразный корень $(q-1)$-степени из 1

$\exists P$, $\deg P = n$

$P(\zeta) = 0$

$\mathbb{F}_8 = \mathbb{F}_p[x]/(P)$

$\mathbb{F}_4 \simeq \mathbb{F}_2[x]/_{1+x+x^2}$

$\mathbb{F}_4 \simeq \mathbb{F}_2[x]/_{1+x+x^3}$

$\mathbb{F}_q$ = минимальное поле разложения $x^q - x$

Лемма: любые два минимальных поля разложения многочлена

$P(x) \in K[x]$ изоморфны

$L_2 \supset K \supset L_1$

$L_2[x] \ni P \in L_1[x]$

Д-во: индукция по числу неприводимых неравных множителей P

и их степени $P(x) = P_1(x) \; P_2(x)$

(неприводимы над K)

Пусть α – корень P_1 в L_1

β – корень P_2 в L_2

$L_1 \supset K_1' \supset K \subset K_2' \subset L_2$

$K' := K''[\alpha] \simeq K''[\beta]$

$K[x]/_{P_1(x)}$

$P(\bar{x}) = 0$.

$L_1 \supset K' \subset L_2$

P над K' раскладывается в произведение линейных

$P = (x-\alpha)(x-\alpha')\ldots(x-\beta)$

и нелинейных $P_1'(x)$ $P_2'(x)$

L_1 и L_2 - минимальные поля разложения ▨

Автоморфизмы конечных полей

$a: \mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_q$ $\quad a(x+y) = a(x)+a(y)$

$a(xy) = a(x)\,a(y)$

Пример: $\mathbb{F}_4$ $\quad a(x) = x^2$

$\mathbb{F}_8$ $\quad a(x) = x^2$

$b(x) = x^4$

$b = a \circ a$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ $\quad y^3+y+1$

$a(x) = y = x^2$

$a: \mathbb{F}_q \circlearrowleft$ $\quad a(x) = x^p$ - автоморфизм Фробениуса (Галуа)

$a \cdot a = a^2$ $\quad : x \to (x^p)^p = x^{p^2}$

$a \cdot a \cdot a = a^3$ $: x \to (x)^{p^3}$

$\vdots$

a^{n-1} $\quad : x \to x^{p^{n-1}}$

$Id = a^n$ $\quad : x \to x^{p^n} = x^q = x$

Всего получилось n автоморфизмов, которые образуют циклическую группу

$\mathbb{Z}/n\mathbb{Z}$ с образующей $a = Frob = Fr$

$\shortparallel$ Aut $\mathbb{F}_q$ = Gal($\mathbb{F}_q$) - группа Галуа

Утверждение: все автоморфизмы $\mathbb{F}_q$ - это степени Fr

Д-во: ξ - образующая $\mathbb{F}_q^*$, $P(\xi)=0$, $\deg P = n$

$\forall$ автоморфизм переводит ξ в другой корень P и этим автоморфизм

однозначно задается $\quad b(\xi^e) = (b(\xi))^e$

корней $\leq n \Rightarrow$ автоморф. $\leq n$