Лекция 18.11.2021

ТЕМА: Квадратичные вычеты и вычетно-квадратичные коды.

Квадраты в конечных полях.

Пусть $\mathbb{F}_q = \mathbb{F}_{p^m}$ конечное поле

$q \equiv p \equiv 1 \mod 2$

Определение. $0 \neq a \in \mathbb{F}_q^\times$ называется квадратом, если $\exists\, b \in \mathbb{F}_q^\times : a = b^2$.

Лемма. 1) $\mathbb{F}_q^\times$ содержит ровно $\frac{q-1}{2}$ квадратов.

2) a есть квадрат $\Leftrightarrow a^{\frac{q-1}{2}} = 1$

a неквадрат $\Leftrightarrow a^{\frac{q-1}{2}} = -1$.

Д-во. 1) Рассмотрим гомоморфизм

$s : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $s(b) = b^2$

$\operatorname{Ker} s = \{ b \in \mathbb{F}_q^\times \mid s(b) = b^2 = 1 \} = \{ \pm 1 \}$

⚠ $1 = -1$, т.к. q – нечётное

$$|S(\mathbb{F}_q^\times)| = |\mathbb{F}_q^\times / \{\pm 1\}| = (q-1)/2. \quad (2)$$

2) $\mathbb{F}_q^\times$ — циклическая группа порядка $q-1$.

$\forall\, a \in \mathbb{F}_q^\times \quad a^{q-1} = 1 \Rightarrow a^{\frac{q-1}{2}} = \pm 1$.

Уравнение $x^{\frac{q-1}{2}} = 1 \ (-1)$ имеет не более $(q-1)/2$ корней.

Если $a = b^2 \Rightarrow a^{\frac{q-1}{2}} = b^{q-1} = 1$, и имеет $(q-1)/2$ квадратов. Следовательно, решения ур-ния $x^{\frac{q-1}{2}} = 1$ — это все ненулевые квадраты поля $\mathbb{F}_q$.

Для любого неквадрата имеем, следов., $a^{\frac{q-1}{2}} = -1$

∎

Упражнение. Пусть d делит $q-1$, где $\mathbb{F}_q$ — конечное поле. Описать все ненулевые d-степени поля $\mathbb{F}_q$.

Квадратичные вычеты и невычеты

Пусть p — нечётное простое число.

Пусть $n \not\equiv 0 \bmod p$. Тогда определим символ Лежандра $\left(\frac{n}{p}\right)$:

$\left(\frac{n}{p}\right) = \left(\frac{n \bmod p}{p}\right) = 1$, если $n \bmod p$ квадрат в поле $\mathbb{F}_p$

$= -1$, если $n \bmod p$ не есть квадрат в $\mathbb{F}_p$.

$n \equiv 0 \bmod p$ $\quad \left(\frac{n}{p}\right) = \left(\frac{0}{p}\right) = 0$.

$\left(\frac{n}{p}\right) = \pm 1$, если $n \bmod p$ квадрат/неквадрат в $\mathbb{Z}/p\mathbb{Z}$.

$\left(\frac{0}{p}\right) = 0$.

Лемма 2. 1) $\forall\ n_1, n_2 \in \mathbb{Z}_{\geq 0}$

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right) \cdot \left(\frac{n_2}{p}\right)$$

2) $\left(\frac{n}{p}\right) \overset{\text{лемма 1}}{=} n^{\frac{p-1}{2}} \bmod p$, $\forall n \not\equiv 0 \bmod p$

$n \bmod p$ - квадрат $\Leftrightarrow n^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$

1) (д-во) $\left(\frac{n_1 n_2}{p}\right) \equiv (n_1 n_2)^{\frac{p-1}{2}} \bmod p \equiv$

$\equiv n_1^{\frac{p-1}{2}} \cdot n_2^{\frac{p-1}{2}} \bmod p \equiv$

$\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{если } p \equiv 1 \bmod 4 \\ -1, & \text{если } p \equiv 3 \bmod 4 \end{cases}$

Упражнение

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$

+1 бал к оценке тому, кто придумает несколько доказательств этого с-ба.

$((2k+1)^2 - 1 = 4k^2 + 4k = 4k(k+1) \equiv 0 \bmod 8)$

Новое описание кода Голея G_{23}

$23 \equiv 7 \bmod 8$
$3 \bmod 4$ $\Rightarrow$ $\left(\frac{2}{23}\right) = 1$

$\Rightarrow$ $\left(\frac{-1}{23}\right) = -1$

$C_{23} = C_{f_+^{(11)}} = C_{\ell_+}$

$\ell_+(x) = \sum x^k$

$R_+ = \{ 2^n \bmod 23 \quad 1 \le n \le 11 \}$

$\left(\frac{2}{23}\right) = 1$, имеется ровно 11 квадратичных вычетов mod 23

$\left(\frac{2^n}{23}\right) = \left(\frac{2}{23}\right)^n = 1.$

$\ell_+(x) = \sum x^k$

k пробегает все квадратичные вычеты по mod 23

$\ell_-(x) = \sum x^\ell$

$\left(\frac{\ell}{23}\right) = -1$, т.к. $\left(\frac{-1}{23}\right) = -1.$

Квадратично-вычетные коды:

Циклический бинарный код Элиаса р.

Пусть $p \equiv 7 \bmod 8$, простое число.

$\left(\frac{-1}{p}\right) = -1$, $\left(\frac{2}{p}\right) = 1$.

$p = 7, 23, 31, 47, \ldots$ – бесконечная последовательность

$$e_+(x) = \sum_{\substack{k \bmod p \\ \left(\frac{k}{p}\right)=1}} x^k \in \mathbb{F}_2[x]$$

$$e_-(x) = \sum_{\left(\frac{l}{p}\right)=-1} x^l \in \mathbb{F}_2[x].$$

R_+ = мн-во квадратичных вычетов $\bmod p$

R_- = невычетов

<u>С-во:</u> Пусть c – квадратичный вычет.

Тогда $cR_+ = R_+$, $cR_- = R_-$.

$$\left(\frac{cr}{p}\right) = \left(\frac{c}{p}\right)\cdot\left(\frac{r}{p}\right) = 1\cdot\left(\frac{r}{p}\right) = \pm 1 \quad \begin{matrix} r\text{-вычет} \\ r\text{-невыч} \end{matrix}$$

$\left(\frac{2}{p}\right) = 1 \Rightarrow$

$$e_+(x)^2 \overset{\mathbb{F}_2}{=} \sum_{\left(\frac{k}{p}\right)=1} x^{2k} \equiv \sum_{\left(\frac{k}{p}\right)=1} x^{k} \mod (x^p-1)$$

$$e_-(x)^2 \equiv e_-(x) \mod (x^p-1)$$

Мы установили, что $e_\pm(x)$ являются идемпотентами в кольце $\mathbb{F}_2[x]/(x^p-1)$.

$$C_{QR}(p) = C_{e_+(x)} \subset \mathbb{F}_2[x]/(x^p-1).$$

<u>С-ва</u> <u>идемпотента</u> $e_+(x)$

1) $1 + e_+(x) + e_-(x) = \sum_{m=0}^{p-1} x^m = \frac{x^p-1}{x-1}$.

2) $e_\pm(x)^2 \equiv e_\pm(x) \mod x^p-1$

3) Пусть $\alpha^p = 1$ — примитивный корень степени p из 1 над $\mathbb{F}_2$.

$d = \operatorname{ord}^{\times}_{\mathrm{mod}\,p} 2 \qquad \alpha \in \mathbb{F}_{2^d} \supset \mathbb{F}_2.$

$$e_\pm(\alpha)^2 \overset{2)}{=} e_\pm(\alpha) \Rightarrow e_+(\alpha) \in \mathbb{F}_2.$$

4) 1) $\Rightarrow$ $1 + \ell_+(\alpha) + \ell_-(\alpha) = 0$ $\Rightarrow$

$$\left[\begin{array}{l} \ell_+(\alpha) = 1, \ \ell_-(\alpha) = 0 \\ \ell_+(\alpha) = 0, \ \ell_-(\alpha) = 1, \end{array}\right.$$

5) $\ell_+(\alpha^{-1}) = \sum_{\left(\frac{k}{p}\right)=1} \alpha^{-k \bmod p} = \sum_{\left(\frac{-k}{p}\right)=1} \alpha^{(-k)} =$

$= \ell_-(\alpha)$,

6) $\ell_+(\alpha^t)$ $\left(\frac{t}{p}\right)=1$ $= \sum_{\left(\frac{k}{p}\right)=1} \alpha^{kt \bmod p} = \ell_+(\alpha)$

$t > 0, \ t \not\equiv 0 \bmod p$

$\left(\frac{t}{p}\right)=-1$ $= \sum_{\left(\frac{\ell}{p}\right)=-1} \alpha^{\ell} = \ell_-(\alpha) = \ell_+(\alpha^{-1})$

7) $f_+(x) = \prod_{\left(\frac{k}{p}\right)=1} (x - \alpha^k)$ $\rightarrow$ Вести вычисления в $\mathbb{F}_{2^d}$

$f_-(x) = \prod_{\left(\frac{\ell}{p}\right)=-1} (x - \alpha^{\ell})$ $\in \mathbb{F}_2[x]$

Это многочлен над полем $\mathbb{F}_2$, так как их коэффициенты являются 2-циклотомическими множествами:

2. $R_{\pm} \equiv R_{\pm} \mod p \mid \left(\frac{2}{p}\right) = 1.$ (9)

3) Вывод:

Если $e_+(2) = 0$ (=), то $e_+(2^k) = 0$, $\left(\frac{k}{p}\right) = 1$

$e_-(2) = 1 \Rightarrow e_-(2^{-1}) = e_+(2) = 0 \Rightarrow$

$e_-(2^{-k}) = 0 \quad \forall \left(\frac{k}{p}\right) = 1 \Rightarrow$

$e_+(x)$ делится на $f_+(x)$ |

$e_-(x)$ $f_-(x)$. °

Если $e_+(2) = 1 \Rightarrow e_+(2^{-1}) = 0$

В этом случае заменим 2 на 2^{-1}

Вывод. Можно считать, что

$e_\pm(x)$ делится на $f_I(x)$.

$C_{QR}(p) = C_{f_+(x)} \overset{?}{=} C_{e_+(x)}$

$(x-1) f_+(x) f_-(x) = x^p - 1$. над F_2.

$1 + \ell_+(x) + \ell_-(x) = \frac{x^p - 1}{x - 1}$

$\text{НОД}\left(\ell_+(x), x^p - 1\right) = \prod (x - \alpha^k) = f_+(x)$

$\left(\frac{k}{p}\right) = 1$

$\ell_+(\alpha^k) = \ell_+(\alpha) = 0$

$\ell_+(\alpha^\ell) = \ell_+(\alpha^{-1}) = \ell_-(\alpha) = 1.$

$\left(\frac{\ell}{p}\right) = -1$

Следовательно, $C_{f_+} = C_{\ell_+}$

Анализ: 1) $f_+(x)$ – образующий многочлен циклического кода $C_{QR}(p)$.

$\deg f_+(x) = \frac{p-1}{2} \Rightarrow \dim C_{QR}(p) = p - \frac{p+1}{2} = \frac{p+1}{2}.$

2) $\ell_+(x)$ – проверочный код, образующий.

Нам известно всё начальное подмножество $\ell_+(x)$. $w(\ell_+(x)) = \frac{p-1}{2}$.

Бинарный код $C_{QR}(p)$ порождается

циклической перестановкой квадра-
тичных вычетов.

Пример $p = 7 \equiv 7 \bmod 8$.

$\pm n$	± 1	± 2	± 3	$\bmod 7$
$(\pm n)^2$	1	4	2	$\bmod 7$

$C_{QR}(7) \subset \mathbb{F}_2^7$

$\bmod 7$	1	2	3	4	5	6	7	$\bmod 7$
$\ell_+(x)$	1	1	0	1	0	0	0	порождающая
	0	1	1	0	1	0	0	матрица
	0	0	1	1	0	1	0	$C_{QR}(7)$
	0	0	0	1	1	0	1	

Это код Хэмминга $H_7^{(4)}$.

Теорема $C_{QR}(p)$ – нечётный код.

$$\frac{p-1}{2} = \frac{8k+7-1}{2} = 4k+3$$

Пусть $\overline{C_{QR}}$ – чётное расширение.

$$\overline{C_{QR}}^{\perp} = \overline{C_{QR}}$$

$H_8^{(4)}$!