Билет 2.1:
Конечное поле как множество классов вычетов по модулю неприводимого многочлена

Неприводимый многочлен

Пусть $F[x]$ – множество всех многочленов $f(x)$ всевозможных неотрицательных степеней с коэффициентами из поля $GF(p)$:

$$F[x] = \{f(x) : f(x) = f_0 + f_1 \cdot x + f_2 \cdot x^2 + ... + f_n \cdot x^n + ..., f_i \in GF(p)$$

• *Определение:* Многочлен $p(x) = a_0 + a_1 \cdot x + ... + a_m \cdot x^m$ называется неприводимым над полем GF(p), если он не распадается на множители над этим полем.

Классы вычетов по модулю неприводимого многочлена

Разобьем множество $F[x]$ на p^m классов вычетов по модулю неприводимого многочлена $p(x)$. Для этого рассмотрим все остатки от деления многочленов из $F[x]$ на $p(x)$. Они имеют вид

$$b(x) = b_0 + b_1 \cdot x + ... + b_{m-1} \cdot x^{m-1}, b_i GF(p)$$

Два многочлена из множества $F[x]$ называются сравнимыми по модулю многочлена $p(x)$, если при делении на $p(x)$ они дают одинаковый остаток.

Таким образом, множество $F[x]$ распадается на не пересекающиеся классы многочленов, сравнимых по модулю $p(x)$. Обозначим множество этих классов символом $\frac{F[x]}{p(x)}$

Теорема (Структура $\frac{F[x]}{p(x)}$)

$\frac{F[x]}{p(x)}$ - поле, то есть множество ненулевых остатков $\frac{F'[x]}{p(x)}$ образуют мультипликативную группу.

Несколько выводов по примеру

1. Элементы поля $\frac{F[x]}{p(x)}$ и мультипликативной группы $\frac{F'[x]}{p(x)}$ не зависят от $p(x)$, а зависят только от его степени m и поля $GF(p)$. Поэтому поле вычетов по модулю $p(x)$ будет обозначать $GF(p^m)$
2. Сложение / вычитание $GF(p^m)$ зависит только от p.
3. Умножение / разбиение на обратные элементы в $GF(p^m)$ зависит от $p(x)$.
4. Сложение в $GF(p^m)$ задаётся обычным поразрядным сложением векторов / многочленов.
5. Умножение в $GF(p^m)$ сводится к умножению соответствующих многочленов по правилам поля $GF(p)$ и поиску остатка по модулю $p(x)$.

Билет 2.2:
Задание поля посредством корня неприводимого многочлена

Рассмотрим уравнение, заданное в поле действительных чисел $\mathbb{R} : x^2 + 1 = 0$

Известно, что оно не имеет корней в $\mathbb{R}$, но назначив его корнем число $i = \sqrt{-1} : i^1 + 1 = 0$, мы получим его решение с некотором другое поле $\mathbb{C}$– поле комплексных чисел. По сути, мы построили $\mathbb{C} = \{x + i \cdot y : x, y \in \mathbb{R}, i^2 = -1\}$ благодаря присоединению числа $i \notin \mathbb{R}$ к исходному полю $\mathbb{R}$. Аналогично, неприводимый многочлен $p(x)$ не имеет корней в $GF(p)$, но допустим, что он имеет корень $\alpha \in GF(p^m)$. Тогда $p(\alpha) = 0$. И есть $GF(p^m)$ есть расширение $GF(p)$ при помощи α.

Билет 2.3:
Строение конечных полей. Основные теоремы о многочленах над конечными полями.

Теорема о корнях многочленов $GF(q)$

Если $f(x)$ многочлен над $Gf(q), \beta \in GF(q^m)$ и $f(\beta) = 0,$ то $f(\beta^q) = 0$

Доказательство

Пусть $f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$, согласно теореме о биноме Ньютона над конечным полем:

$$(f(x))^q = a_0^q + a_1^q \cdot x^q + \cdots + a_n^q \cdot x^{n \cdot q} = a_0 + a_1 \cdot x^q + \cdots + a_n \cdot x^{n \cdot q} = f(x^q)$$

так как $f_i \in GF(q)$, а потому $a_i^{q-1} = 1, \quad a_i^q = a_i$

Теорема о делителях $x^{q^m} - x$

Неприводимые над $GF(q)$ многочлены $p(x)$, степени n которых делят m, и только они, являются делителями многочлена $x^{q^m} - x$. То есть многочлен x^{q^m} распадается на произведение минимальных функций всех элементов поля $GF(q^m)$.

• *Определение:* Элементы поля, являющиеся корнями одного и того же неприводимого многочлена, называются сопряженными элементами поля.

Теорема

Все корни одного и того же неприводимого многочлена имеют одинаковый порядок.

Билет 2.4: Определение минимальной функции. Свойства минимальных функций (единственность, существование, неприводимость).

• *Определение:* Минимальной функцией (минимальным многочленом) для элемента $\beta \in GF(q^m)$ называется такой нормированный многочлен $m(x)$ над $GF(q)$ минимальной степени, что $m(\beta) = 0$

Важные особенности минимальных функций

1. Это многочлены над $GF(q)$
2. Но их корни лежат в расширении $GF(q^m)$
3. Минимальные функции – важнейший класс многочленов над конечными полями
4. Все основные алгебраические коды основаны на минимальных функциях

Важнейшие свойства минимальный функций (Теорема)

1. Минимальная функция для β – неприводимый многочлен над $GF(\beta)$
2. Если многочлен $f(x)$ таков, что $f(\beta) = 0$, то $m(x)|f(x)$, где $m(x)$ – минимальная функция для β.
3. Минимальная функция для β единственна (обратное вообще говоря не верно)
4. Для каждого элемента $\beta \in GF(q^m)$ существует минимальная функция
5. Степени минимальной функции элемента $\beta \in GF(q^m)$ – делиель m

Как строить минимальные функции?(Требуемые результаты)

Теорема

Все корни $\beta, \beta^q, \ldots, \beta^{q^{m_1}} \in GF(q^m)$ неприводимого над $GF(q)$ многочлена $p(x)$ степени m различны.

Теорема

Если $f(x)$ многочлен над $GF(q)$, $\beta \in GF(q^m)$ и $f(\beta) = 0$, то f$(\beta^q) = 0$

Теорема

Степень минимальной функции элемента $\beta \in GF(q^m)$ – делитель m

Алгоритм построения минимальной функции

1. Фиксируем $\beta \in GF(q^m)$ для которого строится минимальная функция.
2. Вычисляем последовательность: $\beta, \beta^q, \ldots, \beta^{q^i}, \ldots$ до тех пор, пока не найдём такой j, что $\beta^{q^i} = \beta$.
3. Всегда получим n различных $\beta, \ldots, \beta^{q^n}$, где n – некоторый делитель m
4. Тогда $m_\beta(x) = (x - \beta) \cdot (x - \beta^q) \cdot \cdots \cdot (x - \beta^{q^n})$