
Лекция №1 (03.09.20)

---

1. Предварительные сведения из теории конечных полей.

1.1. Фундаментальные свойства конечных полей.

Теорема 1. *Порядок любого конечного поля есть степень простого числа. Для заданного $q = p^n$, где p – простое, существует и притом единственное поле порядка q с точностью до изоморфизма (а именно, поле разложения многочлена $X^q - X$ над $\mathbb{Z}_p$).*

Теорема 2. *Пусть q – степень простого числа, $F = \mathbb{F}_q$. Тогда расширение Галуа поля F есть $E = \mathbb{F}_{q^n}$. Группа Галуа $G = Gal(E/F)$ является циклической порядка n, порожденная автоморфизмами $\sigma : x \mapsto x^q$ поля E. Кроме того, фиксированное поле подгруппы G порождается элементом σ^m, где $m|n$, и имеет порядок q^m, соответственно изоморфно $\mathbb{F}_{q^m}$.*

Автоморфизм $\sigma : x \mapsto x^q$ называется *автоморфизмом Фробениуса* поля $\mathbb{F}_{q^n}$.

Теорема 3. *Пусть f – унитарный неприводимый многочлен степени n над полем $F = \mathbb{F}_q$, α – корень f в некотором расширении. Тогда $F(\alpha) \cong \mathbb{F}_{q^n}$ – поле разложения многочлена f:*

$$f = (X - \alpha)(X - \alpha^q) \dots (X - \alpha^{q^{n-1}}).$$

В частности, два неприводимых многочлена одной и той же степени над конечным полем имеют одно и то же поле разложения.

Теорема 4. *Мультипликативная группа конечного поля – циклическая.*

Любой порождающий элемент мультипликативной группы поля $\mathbb{F}_q^\times$ называется *примитивным элементом поля* $\mathbb{F}_q$. Унитарный неприводимый многочлен f степени n над $\mathbb{F}_q$ называется *примитивным многочленом*, если его корни являются примитивными элементами для $\mathbb{F}_{q^n}$. В общем случае неприводимый многочлен над $\mathbb{F}_q$ не является примитивным.

Следствие 1. *Пусть q – степень простого числа, $n \in \mathbb{Z}^+$. Существует примитивный многочлен степени n в $\mathbb{F}_q[X]$.*

Отметим, что не существует эффективных детерминированных алгоритмов для нахождения примитивного многочлена произвольной степени n над $\mathbb{F}_q$ или примитивного элемента в $\mathbb{F}_{q^n}$.

1.2. Неприводимые многочлены над конечными полями.

Теорема 5. *Пусть f – неприводимый многочлен степени m над $\mathbb{F}_q$ и пусть $n \in \mathbb{Z}^+$. Тогда $f|X^{q^n} - X$ тогда и только тогда, когда $m|n$. Кроме того, $f^2 \nmid X^{q^n} - X$.*

Теорема 6. *Многочлен $X^{q^n} - X \in \mathbb{F}_q[X]$ представляет собой произведение всех унитарных неприводимых многочленов над $\mathbb{F}_q$ степеней, делящих n. В частности,*

$$q^n = \sum_{d|n} dD_{d,q}, \qquad (1.2.1)$$

где $D_{d,q}$ – число унитарных неприводимых многочленов над $\mathbb{F}_q$ (дедекиндово число).

Хотелось бы получить с помощью (1.2.1) рекурсивную формулу для $D_{n,q}$. Определим *функцию Мёбиуса* $\mu : \mathbb{N} \to \mathbb{Z}$:

$$\mu(n) = \begin{cases} 1, n = 1; \\ (-1)^k, n - \text{произведение} k \text{различных простых чисел}; \\ 0, \text{иначе}. \end{cases} \qquad (1.2.2)$$

Лемма 1.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1; \\ 0, n > 1. \end{cases}$$

Теорема 7 (Формула обращения Мёбиуса)**.** *Пусть $f, F : \mathbb{N} \to G$. Тогда следующие условия эквивалентны: В случае, когда G – аддитивная группа:*

1. *$F(n) = \sum_{d|n} f(d)$ для произвольного $n \in \mathbb{N}$.*
2. *$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ для произвольного $n \in \mathbb{N}$.*

В случае, когда G – мультипликативная группа:

1. $F(n) = \prod_{d|n} f(d)$ *для произвольного* $n \in \mathbb{N}$.

2. $f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}$ *для произвольного* $n \in \mathbb{N}$.

Теорема 8. *Число* $D_{n,q}$ *неприводимых унитарных многочленов степени* n *над* $\mathbb{F}_q$ *равно*

$$D_{n,q} = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Предложение 9. *Пусть* q *– степень простого числа,* $n \in \mathbb{Z}^+$. *Тогда произведение* $I_{n,q}(X)$ *всех унитарных неприводимых многочленов степени* n *над* $\mathbb{F}_q$ *равно*

$$I_{n,q}(X) = \prod_{d|n} (X^{q^{n/d}} - X)^{\mu(d)}. \qquad (1.2.3)$$

Теорема 10. *Пусть* f *– унитарный неприводимый многочлен степени* n *над* $\mathbb{F}_q$. *Тогда* f *разлагается на* d *различных неприводимых множителей степени* n/d, *где* $d = НОД(n, k)$ *и* f *рассматривается как многочлен над* $\mathbb{F}_{q^k}$.

Следствие 2. *Пусть* f *– унитарный неприводимый многочлен степени* n *над* $\mathbb{F}_q$. *Тогда* f *неприводим над* $\mathbb{F}_{q^k}$ *тогда и только тогда, когда* $НОД(k, n) = 1$.

Следствие 3. *Пусть* f *– примитивный многочлен степени* nk *над* $\mathbb{F}_q$. *Тогда* f *разлагается на* k *различных примитивных многочленов степени* n, *если рассматривать* f *над* $\mathbb{F}_{q^k}$.