
Лекция №6 (15.10.20)

---

2. Явное построение конечных полей.

2.5. Построение примитивных элементов и примитивных многочленов.

Для построения неприводимого многочлена нам необходимо найти примитивный элемент поля $\mathbb{F}_q$. Первоначально покажем процедуру нахождения порядка элемента $c \in \mathbb{F}_q$.

Алгоритм 1. *Пусть* $c \in \mathbb{F}_q^\times$.
Шаг 1: *Находим каноническое разложение* $q-1$, *а именно,* $q-1 = p_1^{e_1}...p_s^{e_s}$.
Шаг 2: *Полагаем* $m := q-1$.
Шаг 3: *Тестируем одно из уравнений* $c^{\frac{m}{p_i}} = 1$ *для* $i = 1, \ldots, s$.
Шаг 4: *Если уравнение на Шаге 3 выполняется для некоторого* i, *то* $m := \frac{m}{p_i}$ *и переходим на Шаг 3. Иначе* $ord(c) = m$.

Далее мы представим алгоритм, вычисляющий примитивный элемент $\omega \in \mathbb{F}_q^\times$. Пронумеруем элементы $\mathbb{F}_q^\times$, например, $x_1, \ldots, x_{q-1}$.

Алгоритм 2. *Пусть* $x_1, \ldots, x_{q-1}$ – *элементы* $\mathbb{F}_q^\times$.
Шаг 1: *Положим* $i := 1$, $x := x_i$ *и вычисляем* $e := ord(x)$.
Шаг 2: *Если* $e = q-1$, *полагаем* $\omega := x$ *и завершаем алгоритм.*
Шаг 3: *Положим* $y := x_{i+1}$. *Если* $y^e = 1$, *то заменяем* $i := i+1$ *и переходим на Шаг 3.*
Шаг 4: *Вычисляем* $f = ord(y)$. *Находим положительные целые* a *и* b, *такие, что* $z = x^a y^b$ *имеет порядок* $g = НОК(e, f)$. *Заменяем* $i := i+1$, $x := z$, $e := g$ *и возвращаемся на Шаг 2.*

2.6. Вычисление круговых многочленов.

В этом параграфе мы покажем, как можно эффективно вычислить круговые многочлены Φ_n.

Теорема 1. *Пусть m и n – положительные целые. Предположим, что каждый простой делитель m также делит n. Тогда $\Phi_{mn}(X) = \Phi_n(X^m)$.*

Следствие 1. *Пусть n – положительное целое. Обозначим $\sigma(n)$ – произведение всех простых чисел, делящих n. Тогда*

$$\Phi_n(X) = \Phi_{\sigma(n)}(X^{\frac{n}{\sigma(n)}}).$$

Следствие 2. *Пусть n – положительное целое и p – простой делитель n. Тогда*

$$\Phi_{np}(X) = \Phi_n(X^p).$$

Следствие 3. *Пусть p – простое, n – положительное целое. Тогда*

$$\Phi_{p^n}(X) = X^{(p-1)p^{n-1}} + X^{(p-2)p^{n-1}} + \dots X^{p^{n-1}} + 1.$$

Второе следствие показывает, как вычислить Φ_{np} с помощью Φ_n, учитывая, что p – простой делитель n. Теперь рассмотрим случай, когда p – простое число, не делящее n.

Теорема 2. *Пусть n – положительное целое и p – простое, не делящее n. Тогда*

$$\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

Представленные результаты позволяют нам рассмотреть следующий эффективный алгоритм, вычисляющий круговой многочлен Φ_n.

Алгоритм 3 (Вычисление кругового многочлена)**. Шаг 1:** *Вычисляем каноническое разложение числа $n = p_1^{e_1} \dots p_s^{e_s}$.*
Шаг 2: *Полагаем $i := 1$, $p := p_i$ и $f := X^{p-1} + \dots X + 1$.*
Шаг 3: *Если $i < s$, то заменяем i на $i + 1$, иначе переходим на Шаг 5.*
Шаг 4: *Заменяем p на p_i и f на $\frac{f(X^p)}{f(X)}$. Переходим на Шаг 3.*
Шаг 5: *Полагаем $m = \sigma(n) = p_1 \dots p_s$ и $\Phi_n := f(X^{\frac{n}{m}})$.*

Алгоритм может быть упрощен с помощью следующего результата:

Предложение 3. *Пусть $n \geq 3$ – нечетное целое. Тогда*

$$\Phi_{2n}(X) = \Phi_n(-X).$$