
Лекция №4 (01.10.20)

---

2. Явное построение конечных полей.

2.1. Явные вычисления и арифметика.

Поскольку $E = \mathbb{F}_{p^n}$ является n-мерным векторным пространством над своим простым подполем $F = \mathbb{F}_p$, то E имеет базис $\{e_1, \ldots, e_n\}$ над F. Следовательно, сложение в E не представляет проблемы (оно осуществляется покомпонентно). Элементы в E мы можем рассматривать как наборы из n элементов над F. И, таким образом, проблема возникает именно с умножением. Мы имеем

$$(a_1e_1 + \ldots + a_ne_n)(b_1e_1 + \ldots + b_ne_n) = \sum_{i,j=1}^{n} a_ib_je_ie_j. \tag{1}$$

Соответственно, все, что нам необходимо, это знать, как перемножить два базисных элемента. Так как произведение любых двух базисных элементов можно снова выразить как линейную комбинацию через базисные элементы, то существуют n^2 уравнений следующего вида:

$$e_ie_j = \sum_{k=1}^{n} a_{ijk}e_k, \quad i, j = 1, \ldots, n. \tag{2}$$

Система $(a_{ijk})_{i,j,k=1,n}$ состоит из n^3 элементов поля $F = \mathbb{F}_p$ и называется *явными данными* для $E = \mathbb{F}_{p^n}$, причем умножение на n-мерном векторном пространстве F^n определено с помощью формул (1) и (2).

Определение явных данных для E равносильно определению унитарного неприводимого многочлена f степени n над $F = \mathbb{F}_p$, поскольку мы представляем E как $F[X]/(f) \cong F(\alpha)$ (α – корень f) и выбираем произвольный базис $\{e_1, \ldots, e_n\}$ в E. В алгебре стандартным выбором является полиномиальный базис $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Тогда коэффициенты a_{ijk}, определяющие произведение e_ie_j, получаются с помощью умножения двух многочленов $e_i, e_j \in F[X]$, и вычисляется остаток их произведения относительно деления на f. Это не представляется трудным, поскольку мы можем использовать арифметику многочленов над $F = \mathbb{F}_p$.

Лемма 1. *Число $b(n,q)$ упорядоченных базисов поля $E = \mathbb{F}_{p^n}$ над $F = \mathbb{F}_p$ равно*

$$b(n,q) = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\dots(q-1).$$

Возникает вопрос, насколько трудным является построение явных данных для E? Умножение двух многочленов степени n в обычном случае требует $\mathcal{O}(n^2)$ операций по модулю p. Таким образом, определение явных данных для E посредством многочлена f займет $\mathcal{O}(n^4)$ операций в $\mathbb{F}_p$. Формулы (1) и (2) показывают, что умножение двух элементов в E может занять до $\mathcal{O}(n^3)$ операций по модулю p. Таким образом, построение явных данных позволяет уменьшить сложность умножения в E.

2.2. Расширения степени p^k.

Пусть $F = \mathbb{F}_q$ – поле характеристики p. В этом параграфе мы покажем, как построить расширения F степени p^k. Для этого будем использовать функцию следа, чтобы найти неприводимые многочлены степени p^k над F.

Сперва рассмотрим случай, когда $k = 1$. Отметим следующий результат теории Галуа: пусть E/F – расширение Галуа простой степени p поля F характеристики p. Тогда существует элемент $b \in E$, такой, что $E = F(b)$, где $a = b^p - b \in F$. Это влечет, что минимальный многочлен элемента a есть $X^p - X - a$, который даст нам желаемый неприводимый многочлен.

Лемма 2. *Пусть a – элемент поля $F = \mathbb{F}_q$, где q – степень простого числа p. Тогда многочлен $X^p - X - a$ приводим над F тогда и только тогда, когда имеет корень в F.*

Теорема 1. *Пусть a – элемент поля $F = \mathbb{F}_q$, где q – степень простого числа p. Тогда многочлен $X^p - X - a$ неприводим над F тогда и только тогда, когда абсолютный след $\mathrm{Tr}_{\mathbb{F}_p}(a) \neq 0$.*

Таким образом, мы можем построить расширение $\mathbb{F}_p$ степени p. Если нам необходимо построить расширение степени $n = p^k$ для некоторого целого $k \geq 2$, то мы можем использовать данную теорему рекурсивно.

Теорема 2. *Пусть $F = \mathbb{F}_q$ – поле характеристики p, $a \in F$ – элемент с абсолютным следом, отличным от нуля, и пусть α – корень многочлена $f = X^p - X - a$. Тогда $a\alpha^{p-1}$ – элемент в $E = F(\alpha)$ с абсолютным следом, отличным от нуля. Следовательно, $X^p - X - a\alpha^{p-1}$ – неприводимый многочлен над E.*

Теорема 3. *Пусть* $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ *– неприводимый многочлен над* $F = \mathbb{F}_q$*, где* q *– степень простого числа* p*, пусть* b *– элемент* F*. Тогда многочлен* $g = f(X^p - X - b)$ *неприводим над* F *тогда и только тогда, когда* $\mathrm{Tr}_{\mathbb{F}_p}(nb - a_{n-1}) \neq 0$.