

Лекция 10. Построение конечных полей из p^n элементов, где p — простое число, $n \geq 1$.
Нахождение обратного элемента в конечном поле. Мультипликативная группа конечного поля. Примитивный элемент конечного поля.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <http://mk.cs.msu.ru>

Многочлены по модулю многочлена над полем

Пусть p — простое число и $f \in \mathbb{Z}_p[x]$ — **ненулевой многочлен**.

Рассмотрим множество

$$\mathbb{Z}_p[x]/(f) = \{g(x) \in \mathbb{Z}_p[x] \mid \deg(g) < \deg(f)\}.$$

Множество $\mathbb{Z}_p[x]/(f)$ назовем множеством многочленов из $\mathbb{Z}_p[x]$, **приведенных по модулю многочлена f** .

Над элементами из множества $\mathbb{Z}_p[x]/(f)$ рассмотрим **операции сложения и умножения по модулю многочлена f** .

Сумма по модулю многочлена над полем

Если $g_1, g_2 \in \mathbb{Z}_p[x]/(f)$ и $g_1(x) + g_2(x) = g(x) \in \mathbb{Z}_p[x]$, то
положим

$$g_1(x) +_f g_2(x) = g(x) \in \mathbb{Z}_p[x]/(f).$$

Произведение по модулю многочлена над полем

Если $g_1, g_2 \in \mathbb{Z}_p[x]/(f)$ и

$$g_1(x) \cdot g_2(x) = f(x) \cdot q(x) + r(x), \quad \deg(r) < \deg(f),$$

где $q, r \in \mathbb{Z}_p[x]$, то положим

$$g_1(x) \cdot_f g_2(x) = r(x) \in \mathbb{Z}_p[x]/(f).$$

Кольцо по модулю многочлена над полем

Утверждение 1. *Если p — простое число и $f(x) \in \mathbb{Z}_p[x]$ — не постоянный многочлен, то множество $\mathbb{Z}_p[x]/(f)$ с операциями сложения и умножения по модулю многочлена f является коммутативным и ассоциативным кольцом с единицей.*

Кольцо по модулю многочлена над полем

Доказательство. Проверим свойства кольца.

1) Множество $\mathbb{Z}_p[x]/(f)$ с операцией сложения является коммутативной группой.

2) Законы дистрибутивности: если для $g_1(x), g_2(x), h(x) \in \mathbb{Z}_p[x]/(f)$ выполняется

$$\begin{aligned}(g_1(x) + g_2(x)) \cdot h(x) &= f(x) \cdot q(x) + r(x), & \deg(r) < \deg(f), \\ g_1(x) \cdot h(x) &= f(x) \cdot q_1(x) + r_1(x), & \deg(r_1) < \deg(f), \\ g_2(x) \cdot h(x) &= f(x) \cdot q_2(x) + r_2(x), & \deg(r_2) < \deg(f),\end{aligned}$$

то $r(x) = r_1(x) + r_2(x)$.



Теорема о поле по модулю многочлена над полем

Теорема 1. Пусть p — простое число и $f(x) \in \mathbb{Z}_p[x]$ — непостоянный многочлен. Кольцо $\mathbb{Z}_p[x]/(f)$ с операциями сложения и умножения по модулю многочлена f является полем тогда и только тогда, когда $f(x)$ — **неприводимый многочлен над полем \mathbb{Z}_p** .

Теорема о поле по модулю многочлена над полем

Доказательство.

1. Если $f(x)$ — неприводимый многочлен, то докажем, что кольцо $\mathbb{Z}_p[x]/(f)$ **не имеет делителей нуля**.

Если для некоторых многочленов $g_1, g_2 \in \mathbb{Z}_p[x]/(f)$, $g_1 \neq 0$, $g_2 \neq 0$, верно $g_1(x) \cdot g_2(x) = 0$ в этом кольце, то $g_1(x) \cdot g_2(x) = f(x) \cdot q(x)$ для какого-то многочлена $q \in \mathbb{Z}_p[x]$, чего не может быть.

Следовательно, в этом случае $\mathbb{Z}_p[x]/(f)$ — **конечное целостное кольцо**, а значит, **поле**.

Теорема о поле по модулю многочлена над полем

Доказательство.

2. Если $f(x)$ — приводимый многочлен, т. е. $f(x) = f_1(x) \cdot f_2(x)$ для некоторых **непостоянных** многочленов $f_1, f_2 \in \mathbb{Z}_p[x]$, то покажем, что в кольце $\mathbb{Z}_p[x]/(f)$ **нет обратного элемента к элементу $f_1(x)$** .

Если для некоторого многочлена $g \in \mathbb{Z}_p[x]/(f)$ верно $f_1(x) \cdot g(x) = 1$ в этом кольце, то

$$f_1(x) \cdot g(x) = f(x) \cdot q(x) + 1 = f_1(x) \cdot f_2(x) \cdot q(x) + 1$$

для какого-то многочлена $q \in \mathbb{Z}_p[x]$. Поэтому в кольце $\mathbb{Z}_p[x]$ обязательно выполняется равенство:

$$f_1(x)(g(x) - f_2(x) \cdot q(x)) = 1,$$

чего не может быть.

Следовательно, в этом случае $\mathbb{Z}_p[x]/(f)$ **не является полем**.

Конечные поля из p^n элементов

Если $f(x)$ — неприводимый в кольце $\mathbb{Z}_p[x]$ многочлен, где p — простое число, то кольцо $\mathbb{Z}_p[x]/(f)$ является полем.

Элементы этого поля — всевозможные остатки при делении на многочлен $f(x)$.

Пусть $\deg(f) = n$, т. е.

$$f(x) = \sum_{i=0}^n a_i x^i, \quad a_n \neq 0.$$

Конечные поля из p^n элементов

Тогда при делении на $f(x)$ каждый остаток $g(x)$ имеет вид:

$$g(x) = \sum_{j=0}^{n-1} b_j x^j,$$

где b_0, b_1, \dots, b_{n-1} — какие-то элементы поля \mathbb{Z}_p .

Когда коэффициенты $b_0, b_1, \dots, b_{n-1} \in \mathbb{Z}_p$ пробегают все свои возможные значения, мы получаем все возможные остатки при делении на многочлен $f(x)$.

Возможных остатков найдется p^n . А значит, столько же элементов в поле $\mathbb{Z}_p[x]/(f)$.

Поле из 4-х элементов

Пример. Построим поле из $4 = 2^2$ элементов.

В кольце $\mathbb{Z}_2[x]$ многочлен $f(x) = x^2 + x + 1$ — **неприводим**.

Элементами поля $\mathbb{Z}_2[x]/(f)$ являются остатки при делении на $f(x)$:

$$0, 1, x, x + 1,$$

где 0 — нулевой и 1 — единичный элементы.

Поле из 4-х элементов

Таблица сложения элементов в поле $\mathbb{Z}_2[x]/(x^2 + x + 1)$:

| | | | | |
|---------|---------|---------|---------|---------|
| + | 0 | 1 | x | $x + 1$ |
| 0 | 0 | 1 | x | $x + 1$ |
| 1 | 1 | 0 | $x + 1$ | x |
| x | x | $x + 1$ | 0 | 1 |
| $x + 1$ | $x + 1$ | x | 1 | 0 |

Например:

$$x + (x + 1) = x + x + 1 = 1.$$

Поле из 4-х элементов

Таблица умножения элементов в поле $\mathbb{Z}_2[x]/(x^2 + x + 1)$:

| | | | | |
|---------|---|---------|---------|---------|
| \cdot | 0 | 1 | x | $x + 1$ |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | $x + 1$ |
| x | 0 | x | $x + 1$ | 1 |
| $x + 1$ | 0 | $x + 1$ | 1 | x |

Например:

$$x \cdot (x + 1) = x^2 + x = f(x) + 1 = 1.$$

Вычисления в конечных полях

Рассмотрим поле $F = \mathbb{Z}_p[x]/(f)$ из p^n элементов, где $f(x) \in \mathbb{Z}_p[x]$ — **неприводимый многочлен** над полем \mathbb{Z}_p .

Операции сложения $+$ и умножения \cdot в поле F определены.

Т. к. F — поле, для каждого ненулевого элемента $a \in F$ найдется обратный к нему элемент $a^{-1} \in F$.

Как его находить?

Одна из возможностей: умножать элемент a на все элементы поля F , пока в произведении не получим 1.

Но есть более быстрый способ.

Алгоритм Евклида

Пусть $f(x)$ — неприводимый многочлен над полем F .
Тогда для каждого ненулевого многочлена $g(x) \in F[x]$,
 $\deg(g) < \deg(f)$, верно $\text{НОД}(f, g) = 1$.

По алгоритму Евклида можно находить обратный к элементу g
элемент g^{-1} в поле $F[x]/(f)$.

Алгоритм Евклида

Пусть

$$\begin{aligned}f(x) &= g(x)q_1(x) + r_1(x), \quad \deg(r_1) < \deg(g), \\g(x) &= r_1(x)q_2(x) + r_2(x), \quad \deg(r_2) < \deg(r_1), \\&\dots, \\r_{s-2}(x) &= r_{s-1}(x)q_s(x) + a, \quad a \in F, a \neq 0.\end{aligned}$$

Тогда

$$\begin{aligned}r_1(x) &= f(x) - g(x)q_1(x) = g(x)h_1(x) \pmod{f}, \\r_2(x) &= g(x) - r_1(x)q_2(x) = g(x)h_2(x) \pmod{f}, \\&\dots, \\a &= r_{s-2}(x) - r_{s-1}(x)q_s(x) = g(x)h_s(x) \pmod{f},\end{aligned}$$

где многочлены $h_i(x) \in F[x]$, $i = 1, \dots, s$.

Значит, $g^{-1} = a^{-1}h_s \pmod{f}$. (Почему?)

Алгоритм Евклида

Пример. Найдем в поле $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ обратный элемент к элементу $x^2 + 1$. Обозначим: $f(x) = x^3 + x^2 + 1$, $g(x) = x^2 + 1$.

Тогда

$$\begin{aligned} f(x) &= g(x)(x + 1) + x, \\ x &= g(x)(-x - 1) \pmod{f}. \end{aligned}$$

Далее

$$\begin{aligned} g(x) &= x \cdot x + 1, \\ 1 &= g(x) - x \cdot x = g(x) - (g(x)(-x - 1))x = \\ &= g(x)(1 + x^2 + x) \pmod{f}. \end{aligned}$$

Поэтому

$$(x^2 + 1)^{-1} = x^2 + x + 1.$$

Мультипликативная группа конечного поля

Пусть $F = (S; +, \cdot)$ — конечное поле.

По определению поля множество $S \setminus \{0\}$ с операцией умножения \cdot является коммутативной группой.

Эта группа называется **мультипликативной группой поля F** и обозначается как F^* ,

$$F^* = (S \setminus \{0\}; \cdot).$$

Мультипликативная группа конечного поля

Пример. В поле $\mathbb{Z}_3 = (\mathbb{Z}_3; + \pmod{3}, \cdot \pmod{3})$ — мультипликативная группа

$$\mathbb{Z}_3^* = (\{1, 2\}, \cdot \pmod{3}),$$

в которой единица 1, и

$$1 \cdot x = x, \quad x = 1, 2;$$

$$2 \cdot 2 = 1.$$

Теорема мультипликативной группе конечного поля

Теорема 2 (о мультипликативной группе конечного поля).
Мультипликативная группа F^ конечного поля F является циклической.*

Теорема мультипликативной группе конечного поля

Доказательство. Пусть поле F содержит q элементов, $q \geq 3$, и порядок группы F^* равен $|F^*| = q - 1$. Положим $r = q - 1$. Пусть

$$r = p_1^{s_1} \cdot \dots \cdot p_m^{s_m}$$

каноническое разложение числа r на простые множители, p_1, \dots, p_m — различные простые числа, $s_1, \dots, s_m \geq 1$.

Теорема мультипликативной группе конечного поля

Для каждого i , $1 \leq i \leq m$, многочлен

$$f_i(x) = x^{r/p_i} - 1$$

имеет не более r/p_i корней в поле F .

Т.к. $r/p_i < r$, в поле F найдутся **ненулевые элементы, не являющиеся корнями** многочлена $f_i(x)$.

Пусть $a_i \in F^*$ — такой элемент.

Теорема о мультипликативной группе конечного поля

Доказательство. Положим

$$b_i = a_i^{r/p_i^{s_i}}.$$

Тогда

$$b_i^{p_i^{s_i}} = a_i^r = 1. \text{ (Почему?)}$$

Т.е. порядок элемента b_i является делителем числа $p_i^{s_i}$, а значит, имеет вид $p_i^{t_i}$.

Но

$$b_i^{p_i^{s_i-1}} = a_i^{r/p_i} \neq 1. \text{ (Почему?)}$$

Значит, порядок элемента b_i равен $p_i^{s_i}$.

Теорема о мультипликативной группе конечного поля

Доказательство. Положим

$$b = b_1 \cdot \dots \cdot b_m.$$

Докажем от противного, что b — образующий элемент группы F^* , т. е. что его порядок равен r .

Теорема о мультипликативной группе конечного поля

Пусть это не так: пусть порядок элемента b — **собственный делитель** числа r . Значит, его порядок — делитель хотя бы одного из чисел

$$r/p_1, \dots, r/p_m.$$

Пусть он делитель числа r/p_1 . Тогда

$$1 = b^{r/p_1} = b_1^{r/p_1} \cdot b_2^{r/p_1} \cdot \dots \cdot b_m^{r/p_1}.$$

Для всех $i = 2, \dots, m$ получаем

$$b_i^{r/p_1} = \left(b_i^{p_i^{s_i}} \right)^{(\dots)} = 1^{(\dots)} = 1.$$

Теорема о мультипликативной группе конечного поля

Доказательство.

Поэтому

$$b_1^{r/p_1} = 1.$$

Т. е. порядок элемента b_i является делителем числа r/p_1 — противоречие с тем, что порядок элемента b_1 равен $p_1^{s_1}$.

Значит, $F^* = \langle b \rangle$.



Примитивный элемент конечного поля

Образующий элемент циклической мультипликативной группы F^* конечного поля F называется **примитивным элементом** поля F и обозначается как e .

Примитивный элемент конечного поля

Примеры.

1. Найдем примитивный элемент поля $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Получаем: $r = 4 = 2^2$.

У многочлена $f(x) = x^2 - 1$ есть два корня в поле \mathbb{Z}_5 : $x = 1$ и $x = 4$.

Ненулевые элементы **2 и 3 не являются его корнями.**

Значит, **$e = 2$ и $e = 3$ — примитивные элементы** поля \mathbb{Z}_5 :

| x | x^2 | x^3 | x^4 |
|-----|-------|-------|-------|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 2 | 4 | 3 | 1 |
| 3 | 4 | 2 | 1 |
| 4 | 1 | 4 | 1 |

Примитивный элемент конечного поля

Примеры.

2. Найдем примитивный элемент поля $\mathbb{Z}_{13} = \{0, 1, \dots, 12\}$.

Получаем: $r = 12 = 2^2 \cdot 3$.

Для многочлена $f_1(x) = x^6 - 1$ ненулевой элемент $a_1 = 2$ не является его корнем. Действительно:

$$2^6 = 2^4 \cdot 4 = 3 \cdot 4 = 12 \pmod{13}.$$

Поэтому $b_1 = a_1^3 = 2^3 = 8$.

Для многочлена $f_2(x) = x^4 - 1$ ненулевой элемент $a_2 = 2$ не является его корнем. Действительно:

$$2^4 = 2^4 = 3 \pmod{13}.$$

Поэтому $b_2 = a_2^4 = 3$.

Примитивный элемент конечного поля

Значит, $e = 8 \cdot 3 = 11 = -2 \pmod{13}$ — примитивный элемент поля \mathbb{Z}_{13} (далее перечислены степени $e = -2$ в поле \mathbb{Z}_{13}):

$$-2 = 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1.$$

Примитивный элемент конечного поля

Примеры.

3. Найдем примитивный элемент поля из 4-х элементов

$$F = \mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}.$$

Получаем: $r = 3$.

У многочлена $f(x) = x^2 + x + 1$ есть один корень в поле F : $x = 1$.

Ненулевые элементы x и $x + 1$ не являются его корнями.

Значит, $e = x$ и $e = x + 1$ — примитивные элементы поля F :

| x | x^2 | x^3 |
|---------|---------|-------|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| x | $x + 1$ | 1 |
| $x + 1$ | x | 1 |

Задачи для самостоятельного решения

1. Доказать, что если F — поле из $q = p^n$ элементов, где p — простое число, $n \geq 1$, то

$$\sum_{a \in F} a^i = \begin{cases} 0, & 1 \leq i \leq q-2, \\ q-1, & i = q-1. \end{cases}$$

2. Выяснить, сколько примитивных элементов найдется в конечном поле F , содержащем q элементов.

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Гл. 1, с. 36–37, 42–44, 46–51, 69.

Конец лекции