Лекция 11. Критерий неприводимости многочленов степени 2 или 3. Расширения полей. Вычисления в полях, алгоритм Евклида. Теорема о мультипликативной группе конечного поля.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.su

Корень многочлена

Пусть $R[x]$ — кольцо многочленов над кольцом R, $f(x) \in R[x]$,

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

и $c \in R$.

Значением многочлена $f(x)$ **в точке** c называется элемент

$$f(c) = \sum_{i=0}^{n} a_i c^i \in R.$$

Если $f(c) = 0$, то c называется **корнем** многочлена $f(x)$.

Корень многочлена

Теорема 1. *Пусть $F[x]$ — кольцо многочленов над полем F. Элемент $c \in R$ является корнем многочлена $f(x) \in F[x]$ тогда и только тогда, когда многочлен $f(x)$ делится на многочлен $(x - c)$.*

Доказательство. Поделим с остатком многочлен $f(x)$ на многочлен $(x - c)$:

$$f(x) = (x - c)q(x) + r(x),\ \deg(r) < 1.$$

Т.к. степень многочлена $r(x) \in F[x]$ меньше 1, он является постоянным многочленом: $r(x) = b \in F$.

$\Rightarrow$. Если c — корень многочлена $f(x)$, то

$$0 = f(c) = b.$$

$\Leftarrow$. Если многочлен $f(x)$ делится на многочлен $(x - c)$, то $b = 0$. Отсюда $f(c) = 0$.

Кратные корни многочлена

Элемент $c \in F$ называется **корнем кратности** k $(k \geq 1)$ многочлена $f(x) \in F[x]$ из кольца многочленов над полем F, если многочлен $f(x)$ делится на многочлен $(x-c)^k$ и не делится на многочлен $(x-c)^{k+1}$.

Следствие 1.1. *Если F — поле, и многочлен $f(x) \in F[x]$ имеет степень n, $n \geq 1$, то в поле F у него найдется не более n корней с учетом их кратностей.*

Неприводимые многочлены степени 2 или 3

Теорема 2 (критерий неприводимости многочленов степени 2 и 3). *Пусть $F[x]$ — кольцо многочленов над полем F. Многочлен $f(x) \in F[x]$ степени 2 или 3 неприводим над полем F тогда и только тогда, когда у него нет корней в поле F.*

Доказательство. Рассмотрим разложение

$$f(x) = g(x) \cdot h(x),$$

где $g(x), h(x) \in F[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$.
Т.к. степень многочлена $f(x)$ равна 2 или 3, или $\deg(g) = 1$, или $\deg(h) = 1$.
Отсюда многочлен $f(x)$ неприводим над полем F тогда и только тогда когда у него нет корней в этом поле.

□

Неприводимые многочлены степени 2 или 3

Пример. Многочлен $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$ неприводим над полем $\mathbb{F}_3$, т.к.

c	$f(c)$
0	2
1	2
2	1

Т.е. многочлен $f(x)$ не имеет корней в поле $\mathbb{F}_3$, и, значит, неприводим над этим полем.

Число неприводимых многочленов над полем

Пусть F — поле, и $F[x]$ — кольцо многочленов над полем F. Многочлен $f(x) \in F[x]$ называется **нормированным**, если его старший коэффициент равен 1.

Теорема 3. *Число $M_p(n)$ неприводимых нормированных многочленов степени n над полем $\mathbb{F}_p$ вычисляется по формуле*

$$M_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

где запись «$d \mid n$» означает «число d является делителем числа n», а $\mu(n)$ — функция Мебиуса,

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^k, & \text{если } n - \text{произведение } k \text{ различных} \\ & \text{простых чисел}; \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Число неприводимых многочленов над полем

Примеры. Рассмотрим поле $\mathbb{F}_2$.

1. Если $n = 2$, то

$$M_2(2) = \frac{1}{2}\sum_{d|2}\mu(d)2^{\frac{2}{d}} = \frac{1}{2}(2^2 - 2) = 1.$$

Т.е. существует только один неприводимый многочлен степени 2 над полем $\mathbb{F}_2$: $f(x) = x^2 + x + 1$.

2. Если $n = 3$, то

$$M_2(3) = \frac{1}{3}\sum_{d|3}\mu(d)2^{\frac{3}{d}} = \frac{1}{3}(2^3 - 2) = 2.$$

Т.е. найдется два неприводимых многочленов степени 3 над полем $\mathbb{F}_2$: $f_1(x) = x^3 + x^2 + 1$ и $f_2(x) = x^3 + x + 1$.

Число неприводимых многочленов над полем

Следствие 3.1. *Для каждого простого числа p для каждого натурального числа $n \geq 2$ в кольце многочленов $\mathbb{F}_p[x]$ над полем $\mathbb{F}_p$ найдется хотя бы один неприводимый нормированный многочлен над этим полем.*

Доказательство. По теореме 3

$$M_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Заметим, что $\mu(1) = 1$, и $\mu(d) \geq -1$, если $d \geq 2$.
Тогда

$$M_p(n) \geq \frac{1}{n}(p^n - p^{n-1} - \ldots - p) = \frac{1}{n}\left(p^n - \frac{p^n - p}{p-1}\right) =$$

$$= \frac{1}{n} \cdot \frac{p}{p-1} \cdot \left(p^n - 2p^{n-1} + 1\right) > 0,$$

если $p \geq 2$.

Существование полей из p^n элементов

Следствие 3.2. *Для каждого простого числа p для каждого натурального числа $n \geq 2$ существует конечное поле из p^n элементов*.

Доказательство. По следствию 3.1 найдется неприводимый многочлен $g(x) \in \mathbb{F}_p[x]$ степени n над полем $\mathbb{F}_p$.
Фактор-кольцо $\mathbb{F}_p[x]/(g)$ кольца $\mathbb{F}_p[x]$ по модулю главного идеала по неприводимому в этом кольце многочлену $g(x)$ является полем из p^n элементов.

□

Расширения полей

Рассмотрим поле $F = \mathbb{F}_p[x]/(g)$ из p^n элементов, где $g(x) \in \mathbb{F}_p[x]$ — неприводимый многочлен над полем $\mathbb{F}_p$.
Т.к. многочлен $g(x)$ неприводим над полем $\mathbb{F}_p$, у него нет корней в поле $\mathbb{F}_p$.
Пусть

$$g(x) = \sum_{i=0}^{n} a_i x^i.$$

Тогда для элемента $[x] \in F$ верно

$$g([x]) = \sum_{i=0}^{n} a_i ([x])^i = \left[\sum_{i=0}^{n} a_i x^i \right] = [g] = [0]$$

Т.е. элемент $\theta = [x] \in F$ — корень многочлена $g(x)$ в поле F.

Расширения полей

Говорят, что поле $F = \mathbb{F}_p[x]/(g)$ является **простым алгебраическим расширением** поля $\mathbb{F}_p$, что оно получено из поля $\mathbb{F}_p$ **присоединением корня** θ неприводимого над полем $\mathbb{F}_p$ многочлена $g(x)$ и обозначают $F = \mathbb{F}_p(\theta)$.
Тогда все элементы поля $F = \mathbb{F}_p(\theta)$ имеют вид

$$b_{n-1}\theta^{n-1} + \ldots + b_1\theta + b_0,$$

где коэффициенты $b_{n-1}, \ldots, b_1, b_0$ пробегают все возможные значения из поля $\mathbb{F}_p$.
Значит, каждый элемент поля F можно задавать **набором** из n элементов из поля $\mathbb{F}_p$:

$$(b_{n-1}, \ldots, b_1, b_0),\ \ b_{n-1}, \ldots, b_1, b_0 \in \mathbb{F}_p.$$

При такой записи операция сложения элементов поля F — операция покоординатного сложения задающих их наборов.

Расширения полей

Т.е. поле $F = \mathbb{F}_p(\theta)$ можно рассматривать как **линейной пространство** над полем $\mathbb{F}_p$.
В разных случаях бывает удобной та или иная форма записи элементов поля из p^n элементов.

Вычисления в конечных полях

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

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

Наибольший общий делитель многочленов

Пусть $F[x]$ — кольцо многочленов над полем F, и $f_1(x), f_2(x) \in F[x]$.

Нормированный многочлен $g(x) \in F[x]$ называется **наибольшим общим делителем** многочленов $f_1(x)$ и $f_2(x)$, если
1) многочлены $f_1(x)$ и $f_2(x)$ делятся на многочлен $g(x)$;
2) многочлен $g(x)$ делится на каждый многочлен, на который делятся одновременно многочлены $f_1(x)$ и $f_2(x)$.

Наибольший общий делитель многочленов $f_1(x)$ и $f_2(x)$ будем обозначать как НОД(f_1, f_2).

Наибольший общий делитель многочленов

Теорема 4. *Пусть $F[x]$ — кольцо многочленов над полем F. Тогда для любых ненулевых многочленов $f_1(x), f_2(x) \in F[x]$ существует однозначно определенный нормированный многочлен $g(x) \in F[x]$, являющийся их наибольшим общим делителем.*

Доказательство. Рассмотрим множество

$$J = \{f_1(x)q_1(x) + f_2(x)q_2(x) \mid q_1(x), q_2(x) \in F[x]\}.$$

Оно является идеалом кольца $F[x]$ (проверить свойства). Кольцо $F[x]$ является кольцом главных идеалов, а значит, найдется такой многочлен $g_0(x) \in F[x]$, что

$$J = (g_0) = \{g_0(x)q(x) \mid q(x) \in F[x]\}.$$

Наибольший общий делитель многочленов

Доказательство. Пусть a — старший коэффициент многочлена $g_0(x)$. Рассмотрим нормированный многочлен $g(x) = a^{-1}g_0(x) \in F[x]$.
1) Заметим, что

$$f_1(x) = f_1(x) \cdot 1 + f_2(x) \cdot 0 \in J,$$

т.е. многочлен $f_1(x)$ делится на многочлен $g(x)$.
Аналогично, многочлен $f_2(x)$ делится на многочлен $g(x)$.
2) Т.к. $g(x) \in J$, найдутся такие многочлены $h_1(x), h_2(x) \in F[x]$, что

$$g(x) = f_1(x)h_1(x) + f_2(x)h_2(x).$$

Но тогда многочлен $g(x)$ делится на любой многочлен, на который одновременно делятся многочлены $f_1(x)$ и $f_2(x)$.
Значит, $g(x) = \text{НОД}(f_1, f_2)$ — существование доказано.

Наибольший общий делитель многочленов

Доказательство. Пусть $g_1(x)$ — другой наибольший общий делитель многочленов $f_1(x)$ и $f_2(x)$.
Т.к. $g(x)$ — наибольший общий делитель многочленов $f_1(x)$ и $f_2(x)$, а $g_1(x)$ — их делитель, найдется такой многочлен $q_1(x) \in F[x]$, что

$$g(x) = g_1(x)q_1(x).$$

Аналогично, найдется такой многочлен $q(x) \in F[x]$, что

$$g_1(x) = g(x)q(x).$$

Тогда

$$g(x) = g_1(x)q_1(x) = (g(x)q(x))q_1(x).$$

Отсюда

$$g(x)(1 - q(x)q_1(x)) = 0.$$

Наибольший общий делитель многочленов

Доказательство.
Т.к. $F[x]$ — целостное кольцо (т.к. наследуется свойство целостности поля F) и $g(x) \neq 0$, верно

$$q(x)q_1(x) = 1.$$

Значит, $q(x)$ и $q_1(x)$ — обратимые элементы кольца $F[x]$, т.е. постоянные ненулевые многочлены.
Т.к. многочлены $g(x)$ и $g_1(x)$ нормированы, $q(x) = q_1(x) = 1$.
Т.е. $g(x) = g_1(x)$ — однозначность доказана.

□

Наибольший общий делитель многочленов

Следствие 4.1. *Пусть $F[x]$ — кольцо многочленов над полем F. Тогда если многочлен $g(x) \in F[x]$ является наибольшим общим делителем ненулевых многочленов $f_1(x), f_2(x) \in F[x]$, то найдутся такие многочлены $h_1(x), h_2(x) \in F[x]$, что*

$$g(x) = f_1(x)h_1(x) + f_2(x)h_2(x).$$

Алгоритм Евклида

Теорема 5 (алгоритм Евклида). *Пусть $F[x]$ — кольцо многочленов над полем F, $f_1(x), f_2(x) \in F[x]$ — ненулевые многочлены, и*

$$
\begin{aligned}
&f_1(x) = f_2(x)q_1(x) + r_1(x),\ \deg(r_1) < \deg(f_2);\\
&f_2(x) = r_1(x)q_2(x) + r_2(x),\ \deg(r_2) < \deg(r_1);\\
&r_1(x) = r_2(x)q_3(x) + r_3(x),\ \deg(r_3) < \deg(r_2);\\
&\ldots;\\
&r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x),\ \deg(r_s) < \deg(r_{s-1});\\
&r_{s-1}(x) = r_s(x)q_{s+1}(x).
\end{aligned}
$$

Тогда если $a \in F$ — старший коэффициент многочлена $r_s(x)$, то НОД$(f_1, f_2) = a^{-1}r_s(x)$.

Алгоритм Евклида

Доказательство. Пусть

$$
\begin{aligned}
&f_1(x) = f_2(x)q_1(x) + r_1(x),\ \deg(r_1) < \deg(f_2);\\
&f_2(x) = r_1(x)q_2(x) + r_2(x),\ \deg(r_2) < \deg(r_1);\\
&r_1(x) = r_2(x)q_3(x) + r_3(x),\ \deg(r_3) < \deg(r_2);\\
&\ldots;\\
&r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x),\ \deg(r_s) < \deg(r_{s-1});\\
&r_{s-1}(x) = r_s(x)q_{s+1}(x).
\end{aligned}
$$

1) Просматривая равенства «снизу вверх» получаем, что на многочлен $r_s(x)$ делятся многочлены $f_1(x)$ и $f_2(x)$.
2) Если на многочлен $h(x)$ одновременно делятся многочлены $f_1(x)$ и $f_2(x)$, то, просматривая равенства «сверху вниз», получаем, что на многочлен $h(x)$ делится и многочлен $r_s(x)$.
Значит, НОД$(f_1, f_2) = a^{-1}r_s(x)$. □

Алгоритм Евклида

Пример. По алгоритму Евклида найдем наибольший общий делитель многочленов $f_1(x) = x^4 + x$ и $f_2(x) = x^2 + 1$ из кольца $\mathbb{F}_2[x]$.
Тогда

$$x^4 + x = (x^2 + 1)(x^2 + 1) + (x + 1);$$
$$x^2 + 1 = (x + 1)(x + 1).$$

Отсюда, НОД$(x^4 + x, x^2 + 1) = x + 1$.

Алгоритм Евклида

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

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

Алгоритм Евклида

Пусть

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

Тогда

$$
\begin{aligned}
&r_1(x) = g(x) - r(x)q_1(x) = r(x)h_1'(x) + g(x)h_1''(x);\\
&r_2(x) = r(x) - r_1(x)q_2(x) = r(x)h_2'(x) + g(x)h_2''(x);\\
&\ldots;\\
&a = r_{s-2}(x) - r_{s-1}(x)q_s(x) = r(x)h_s'(x) + g(x)h_s''(x),
\end{aligned}
$$

где многочлены $h_i'(x), h_i''(x) \in F[x]$, $i = 1, \ldots, s$.
Отсюда $([r])^{-1} = [a^{-1}h_s']$ (почему?).

Алгоритм Евклида

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

$$x^3+x^2+1 = (x^2+1)(x+1)+x;$$
$$x = r(x)(-x-1)+g(x).$$

Далее

$$x^2+1 = x\cdot x+1;$$
$$1 = r(x)-x\cdot x = r(x)-(r(x)(-x-1)+g(x))x =$$
$$= r(x)(1+x^2+x)-g(x)x.$$

Отсюда

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

Несложно проверить, что

$$(x^2+1)(x^2+x+1) = x^4+x^3+x+1 = (x^3+x^2+1)x+1.$$

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^*,

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

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

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

в которой единица 1, и

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

Теорема мультипликативной группе конечного поля

Теорема 6 (о мультипликативной группе конечного поля). *Мультипликативная группа F^* конечного поля F является циклической.*

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

Пусть

$$h = p_1^{s_1} \cdot \ldots \cdot p_m^{s_m}$$

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

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

$$f_i(x) = x^{\frac{h}{p_i}} - 1$$

имеет не более $\frac{h}{p_i}$ корней в поле F (по следствию 1.1).

Т.к. $\frac{h}{p_i} < h$, в поле F есть ненулевые элементы, **не являющиеся** корнями многочлена $f_i(x)$.

Пусть $a_i \in F^*$ — такой элемент.

Теорема о мультипликативной группе конечного поля

Доказательство. Положим

$$b_i = a_i^{\frac{h}{p_i^{s_i}}}.$$

Тогда

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

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

$$b_i^{p_i^{s_i-1}} = a_i^{\frac{h}{p_i}} \neq 1 \text{ (почему?)}.$$

Отсюда порядок элемента b_i равен $p_i^{s_i}$.

Теорема о мультипликативной группе конечного поля

Доказательство. Положим

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

Докажем от противного, что b — образующий элемент группы F^*, т.е. что его порядок равен h.
Пусть это не так: порядок элемента b — собственный делитель числа h. Значит, его порядок делитель хотя бы одного из чисел

$$\frac{h}{p_1}, \ldots, \frac{h}{p_m}.$$

Пусть он делитель числа $\frac{h}{p_1}$. Тогда

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} \ldots b_m^{\frac{h}{p_1}}.$$

Для всех $i = 2, \ldots, m$ получаем

$$b_i^{\frac{h}{p_1}} = \left(b_i^{p_i^{s_i}} \right)^{(\ldots)} = 1^{(\ldots)} = 1.$$

Теорема о мультипликативной группе конечного поля

Доказательство.
Отсюда

$$b_1^{\frac{h}{p_1}} = 1.$$

Т.е. порядок элемента b_i является делителем числа $\frac{h}{p_1}$ — противоречие с тем, что порядок элемента b_1 равен $p_1^{s_1}$.
Значит, $F^* =< b >$.

□

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 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

Получаем: $h = 4 = 2^2$.

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

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

Поэтому $e = 2$ — примитивный элемент поля $\mathbb{F}_5$, и $e = 3$ — примитивный элемент поля $\mathbb{F}_5$:

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
$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, \theta, \theta + 1\}$.
Получаем: $h = 3$.
У многочлена $f(x) = x - 1$ есть один корень в поле $\mathbb{F}_4$: $x = 1$.
Ненулевые элементы θ и $\theta + 1$ **не являются** его корнями.
Поэтому $e = \theta$ — примитивный элемент поля $\mathbb{F}_4$, и $e = \theta + 1$ — примитивный элемент поля $\mathbb{F}_4$:

x	x^2	x^3
0	0	0
1	1	1
θ	$\theta + \mathbf{1}$	$\mathbf{1}$
$\theta + \mathbf{1}$	θ	$\mathbf{1}$

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. Найти НОД(f_1, f_2), если $f_1(x) = x^5 + x + 1 \in \mathbb{F}_2[x]$ и $f_2(x) = x^6 + x^5 + x^4 + 1 \in \mathbb{F}_2[x]$.

3. Найти обратные элементы к элементам

1) 5 и 12 в поле $\mathbb{F}_{17}$;

2) $[2x + 1]$ и $[x^2 + x + 2]$ в поле $\mathbb{F}_3[x]/(x^3 + x^2 + 2)$.

4. Найти примитивные элементы полей

1) $\mathbb{F}_7$;

2) $\mathbb{F}_3[x]/(x^2 + 1)$.

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