

Алгоритмы компьютерной алгебры

Конспект лекций

2019

Содержание

1	Лекция 1.	3
1.1	Основные факты из теории многочленов	3
1.2	Многочлены с рациональными коэффициентами	4
1.2.1	Алгоритм Кронекера	4
1.2.2	Алгоритм Евклида	5
1.2.3	Каноническое разложение	6

1. Лекция 1.

Предмет изучения компьютерной алгебры - точные вычисления. Рассматриваются именно алгоритмы точного, а не приближенного вычисления, как в вычислительной математике. Эти алгоритмы лежат в основе математических пакетов MATLAB, Mathematica. Основной объект исследований - числовые системы с точными вычислениями.

1.1. Основные факты из теории многочленов

Определение 1. *Числовым полем* называется множество $F \subset \mathbb{C}$, если:

1. $0, 1 \in F$,
2. $|F| \geq 2$,
3. $\forall a, b \in F : a \pm b, ab \in F; b \neq 0, \frac{a}{b} \in F$.

Пример 1. Числовые поля - $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$

Множество многочленов над полем рациональных чисел обозначается как $\mathbb{Q}[x]$, над целыми - $\mathbb{Z}[x]$, над произвольным числовым полем F - $F[x]$.

Определение 2. Многочлен $f(x) \in F[x]$, отличный от константы, называют **приводимым** над полем F , если он допускает представление вида $f(x) = \varphi(x)\psi(x)$, где $\varphi(x), \psi(x) \in F[x]$ и $\deg \varphi, \deg \psi < \deg f$, и **неприводимым**, если он не допускает такого разложения (то есть один из многочленов φ, ψ является константой).

1. $\deg f = 1$. Пусть f допускает разложение: $f(x) = \varphi(x)\psi(x)$.

$$\deg \varphi = 0, \deg \psi = 0 < \deg f \Rightarrow \deg f = 0.$$

Полученное противоречие доказывает неприводимость любого многочлена первой степени.

2. Пусть $\deg f > 1$ и $f(\alpha) = 0, \alpha \in F$.

$$(x - \alpha) \mid f(x) \Rightarrow \exists g(x) : f(x) = (x - \alpha)g(x).$$

$$\deg(x - \alpha) = 1 < \deg f.$$

$$\deg g = \deg f - 1 < \deg f.$$

Если многочлен f имеет корень в поле F , то f приводим над полем F .

Обратное утверждение. Если многочлен $f \in F[x]$ степени 2 или 3 приводим над полем F , то он имеет в этом поле корень.

Доказательство. Допустим, многочлен приводим, следовательно, $f(x) = \varphi(x)\psi(x)$.

$$\deg \varphi, \deg \psi < \deg f \Rightarrow \deg \varphi = 1 \text{ или } \deg \psi = 1.$$

Допустим, $\varphi(x) = ax + b, a \neq 0 \Rightarrow \alpha = -\frac{b}{a}, \alpha \in F.$

□

Пример 2.

1. $f(x) = x^2 - 1 = (x - 1)(x + 1)$. Многочлен приводим над полями $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. У него нет рациональных корней, следовательно, он неприводим над \mathbb{Q} . Но $f(x) = (x - \sqrt{2})(x + \sqrt{2}) \Rightarrow f(x)$ приводим над \mathbb{R} .
3. $f(x) = x^2 + 1$ неприводим над \mathbb{Q} и \mathbb{R} . Но $f(x) = (x - i)(x + i) \Rightarrow f(x)$ приводим над \mathbb{C} .

Многочлены второй и третьей степени приводимы над полем F тогда и только тогда, когда имеют в этом корень. Для многочленов степени, больше чем 3, данное утверждение не является справедливым.

Пример 3. $f(x) = (x^2 + 1)^2 \in \mathbb{R}[x]$ не имеет действительных корней, но приводим.

Определение 3. Многочлен называется **нормированным**, если его старший коэффициент равен единице.

Теорема 1 (Фундаментальная теорема о многочленах). Пусть $f \in F[x]$, $\deg f \geq 1$. Тогда f допускает разложение $f(x) = a_0 \varphi_1(x) \varphi_2(x) \dots \varphi_k(x)$, где $a_0 \in F$, $\varphi_i \in F[x]$ и любой многочлен φ_i - нормированный и неприводимый. При этом данное разложение является единственным с точностью до порядка следования сомножителей.

1.2. Многочлены с рациональными коэффициентами

Задача. Дан многочлен с рациональными коэффициентами. Необходимо найти разложение этого многочлена в произведение многочленов с рациональными коэффициентами.

Пусть $f \in \mathbb{Q}[x]$. Если мы умножим этот многочлен на подходящее число N (наименьшее общее кратное коэффициентов членов многочлена), то $Nf(x) \in \mathbb{Z}[x]$. Таким образом, приводимость f равносильна приводимости Nf , следовательно, разложение многочлена с рациональными коэффициентами можно свести к разложению многочлена с целыми коэффициентами.

Теорема 2. Если многочлен $f \in \mathbb{Z}[x]$ допускает разложение в произведение многочленов с рациональными коэффициентами, то он допускает разложение в произведение многочленов тех же степеней с целыми коэффициентами.

1.2.1. Алгоритм Кронекера

Задача. Дан многочлен $f \in \mathbb{Z}[x]$, $\deg f > 1$. Можно ли подобрать $u(x), v(x)$, $u, v \in \mathbb{Z}[x]$ и $\deg u, \deg v < \deg f$?

Предположение 1. Все возникающие натуральные числа можно факторизовать.

Предположение 2. Многочлен формальной степени n можно найти с помощью интерполяционного многочлена по $n + 1$ точке x_0, x_1, \dots, x_n и значениям многочлена в этих точках $f(x_0), f(x_1), \dots, f(x_n)$.

$$\begin{cases} f(x_0) = u(x_0)v(x_0), \\ f(x_1) = u(x_1)v(x_1), \\ \dots \\ f(x_n) = u(x_n)v(x_n). \end{cases}$$

Рассмотрим точки $x_0, x_1, \dots, x_n \in \mathbb{Z}$.

$$\forall i \in [0, n] : f(x_i) \in \mathbb{Z} \Rightarrow u(x_i), v(x_i) \in \mathbb{Z}, \deg u = m.$$

Пусть все рассматриваемые точки - не корни многочлена f . Тогда $u(x_i) \mid f(x_i)$, $u(x_i)$ может принимать только конечное множество значений, состоящее из делителей $f(x_i)$. Коэффициенты многочлена u восстанавливаются по его значениям. Далее следует непосредственная проверка того, является ли u делителем f . Алгоритм Кронекера используется для сведения от выбора из бесконечного числа вариантов к выбору из конечного числа вариантов.

Теорема 3 (Признак Эйзенштейна). Пусть многочлен

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x], \quad n > 1, \quad a_0 \neq 0.$$

Если существует простое число p такое, что $p \nmid a_0$, $p \mid a_1$, $p \mid a_2$, ..., $p \mid a_{n-1}$ и $p^2 \nmid a_n$, то f неприводим над \mathbb{Q} .

Пример 4. Многочлен $f(x) = x^n - 2$ не приводим над \mathbb{Q} для $\forall n \geq 1$. Таким образом, существуют неприводимые многочлены над \mathbb{Q} любой степени.

1.2.2. Алгоритм Евклида

Если многочлены $f, g \in F[x]$, $g \neq 0$, то имеет место следующее представление: $f(x) = g(x)h(x) + r(x)$, $h, r \in F[x]$ и $r = 0$ или $r \neq 0$, $\deg r < \deg g$. Если считать, что степень нулевого многочлена $r = 0$ равна $-\infty$, то можно рассматривать только вариант $\deg r < \deg g$.

Определение 4. Если многочлены $f, g \in F[x]$, то многочлен $\varphi \in F[x]$ называют **наибольшим общим делителем (НОД)** f и g , если:

1. $\varphi(x) \mid f(x)$, $\varphi(x) \mid g(x)$,
2. $\forall \psi \in F[x] : \psi(x) \mid f(x), \psi(x) \mid g(x) \Rightarrow \psi(x) \mid \varphi(x)$.

Можно доказать, что НОД всегда существует и находится с точностью до множителя.

Определение 5. Если НОД многочленов $f(x)$ и $g(x)$ - нормированный многочлен, то он обозначается как $(f(x), g(x))$.

Алгоритм Евклида. Шаг 1.

$$f(x) = g(x)h_1(x) + r_1(x).$$

$$(f(x), g(x)) = (g(x), r_1(x)), \deg r_1 < \deg g.$$

Алгоритм Евклида. Шаг 2.

$$g(x) = r_1(x)h_2(x) + r_2(x).$$

$$(g(x), r_1(x)) = (r_1(x), r_2(x)), \deg r_2 < \deg r_1.$$

Если степень многочлена f (делимого) меньше, чем степень многочлена g (делителя), то алгоритм сам поменяет их местами:

$$f(x) = g(x) \cdot 0 + f(x)$$

$$g(x) = f(x)h_1(x) + r_1(x)$$

Поскольку остаток - неотрицательный, то процесс завершится.

Алгоритм Евклида. Заключительные шаги.

$$r_{k-2}(x) = r_{k-1}(x)h_k(x) + r_k(x)$$

$$r_{k-1}(x) = r_k(x)h_{k+1}(x)$$

$$(r_{k-2}(x), r_{k-1}(x)) = (r_{k-1}(x), r_k(x))$$

Строго говоря, $(r_{k-1}(x), r_k(x))$ необязательно равен $r_k(x)$. $r_k(x)$ является лишь одним из НОД.

1.2.3. Каноническое разложение

Определение 6. Пусть для многочлена $f(x)$ существует разложение:

$$f(x) = ap_1(x)p_2(x)...p_k(x),$$

где все многочлены p_i - неприводимые и нормированные. Тогда такое разложение называют **разложением на неприводимые множители** или **факторизацией** многочлена.

Определение 7. Пусть для многочлена $f(x) \in F[x]$ существует разложение:

$$f(x) = a(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_r(x))^{k_r},$$

где все многочлены p_i - неприводимые, нормированные и попарно различные. Тогда такое разложение называют **каноническим разложением над полем**, а значение k_i - **кратностью множителя** p_i . Если $k_i = 1$, то множитель p_i называется **простым**.

Задача. Дан многочлен f . Нужно найти вид $f(x) = a\varphi_1(x)(\varphi_2(x))^2...(\varphi_s(x))^s$, в котором φ_i - произведение всех множителей кратности i .

Пример 5. *Получить каноническое разложение многочлена*

$$f(x) = (x - 1)(x - 2)(x^2 + x + 1)^2(x^2 - x + 1)^2(x^3 - 2)^3.$$

$$f(x) = \varphi_1(x)(\varphi_2(x))^2(\varphi_3(x))^3.$$

$$\varphi_1(x) = (x - 1)(x - 2).$$

$$\varphi_2(x) = (x^2 + x + 1)(x^2 - x + 1).$$

$$\varphi_3(x) = x^3 - 2.$$