Компьютерная алгебра

(курс лекций)

Игорь Алексеевич Малышев

Computer.Algebra@yandex.ru

КСПТ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ПРОГРАММНЫЕ ТЕХНОЛОГИИ

Лекция 13

Факторизация полиномов

Содержание лекции

- Вычисление значений и корней полиномов
- Разложение полиномов
  на неприводимые множители
- Разложение полиномов
  на свободные от квадратов множители
- Разложение на множители полиномов
  над конечными полями

План лекции: тема подраздела

- **Вычисление значений и корней полиномов**
- Разложение полиномов
  на неприводимые множители
- Разложение полиномов
  на свободные от квадратов множители
- Разложение на множители полиномов
  над конечными полями

Значения и корни полиномов

Корень полинома

Пусть J – область целостности. Рассмотрим p (x) в J [x].
Если $\alpha \in J$, то можно разделить p (x) на (x – α)
(это может быть выполнено, т.к.коэффициент при x обратим)
И получить:

$$p(x) = (x - \alpha) * q(x) + r(x)$$
$$\deg(r(x)) < \deg(x - \alpha) = 1$$

т.е. r (x) – это константа из кольца J .
Будем говорить, что $\alpha \in J$ – **корень** или **нуль полинома** p (x) , если p (α) = 0 .

Теорема Этьенна Безу. Пусть J – область целостности, p (x) $\in$ J [x] , $\alpha \in J$.
Тогда α – корень полинома p (x) , если и только если (x – α) | p (x) .

Следствие. Пусть J – область целостности, p (x) $\in$ J [x] , $\alpha \in J$.
Тогда, если мы разделим p (x) на (x – α) ,
то остаток будет равен p (α) .

Значения и корни полиномов

Простые и кратные корни полинома

Пример. Рассмотрим полином $p(x) = x^2 - x - 2 \in \mathbf{Z}[x]$,
имеющий два корня $x = -1$ и $x = 2$.

Тогда очевидно, что

$$(x + 1) \mid (x^2 - x - 2) \qquad \text{и} \qquad (x - 2) \mid (x^2 - x - 2)$$

Более того, если мы разделим $(x^2 - x - 2)$ на $(x - 3)$, то получим в остатке 4 :

$$4 = (3)^2 - (3) - 2$$

Если α – корень полинома $p(x)$ и $p(x) = (x - \alpha)^m * q(x)$, $m \geq 1$, $q(\alpha) \neq 0$,
то m называется **кратностью корня** α .
Если $m = 1$, то α называется **простым корнем**.

Значения и корни полиномов

Количество корней полинома

Теорема. Пусть J – область целостности, $p(x) \in J[x]$, $p(x) \neq 0$.
Если степень полинома p (x) равна n ,
то p (x) имеет не более n корней с учётом кратностей.
Эти корни лежат в J или в большей области.

Как изменится вышеуказанная теорема,
если J – не является областью целостности ?

Пример. Рассмотрим полином $x^2 - 1$ с коэффициентами из кольца $\mathbf{Z}_8$,
содержащего делители нуля.
Этот полином имеет четыре (!) корня $x = 1$, $x = -1$ (или 7) , $x = 3$, $x = 5$,
что превышает степень полинома.

Следствие. Пусть J – область целостности, $p(x) \in J[x]$.
Если степень полинома p (x) равна n и p (x) имеет больше, чем n корней,
то $p(x) = 0$.

Значения и корни полиномов

Метод Руффини – Горнера

Замечание. Данный метод широко известен как метод (схема, правило) Горнера, предложенный **Уильямом Джорджем Горнером** (1819)
и позволяющий эффективно решить следующие задачи:

(1) вычисление значения полинома p (x) в данной точке x = α ;
(2) вычисление нового полинома p (y) , где x = α + y
(по сути, разделив полином p (x) на бином (x – α)) ;
(3) вычисление корней полинома ;
(4) вычисление производных полинома в данной точке.

На пятнадцать лет раньше (1804) этот же метод был предложен **Паоло Руффини**.

Сущность метода Руффини – Горнера (в частности, для решения задачи (1)) – преобразование исходного представления полинома :

$$p(x) = c_0 + c_1 x + \ldots + c_n x^n$$

во вложенную форму:

$$p(\alpha) = c_0 + \alpha (c_1 + \alpha (c_2 + \ldots + \alpha (c_{n-1} + \alpha c_n) \ldots)$$

с помощью следующей рекурсивной схемы :

$$p_0 := c_n$$
$$p_k := \alpha p_{k-1} + c_{n-k} , k > 0$$

Значения и корни полиномов

Сложность метода Руффини – Горнера – 1

Для анализа временной сложности метода Руффини – Горнера
необходимо рассмотреть два случая :

Случай 1. Коэффициенты полинома p (x) и точка α принадлежат (конечному) полю.

Мы имеем n операций сложения и умножения с одинарной точностью, где n = deg (p (x)).
Поэтому p (α) вычисляется за время O (n).

Случай 2. Коэффициенты полинома p (x) и точка α принадлежат кольцу целых чисел.

Мы имеем n операций сложения и умножения длинных целых чисел.
Полагая (как и раньше), что время умножений доминирует над временем сложений,
считаем, что только умножаем n различных членов на α , где n = deg (p (x)).

Тогда, если η – значение наибольшего члена,
полученного при выполнении метода Руффини – Горнера, то

$$T_{RUF-HOR}\ [\ p(x)\ ,\ \alpha\ ]\ = O\ [\ n * L(\alpha) * L(\eta)\ ]$$

Значения и корни полиномов

Сложность метода Руффини – Горнера – 2

Теперь оценим значение η .

Положим $b = | p(x) |_\infty$ – наибольший по абсолютной величине коэффициент $p(x)$.

Рассмотрим «наихудший» возможный случай,
когда все коэффициенты полинома $p(x)$ равны b .
Тогда значение η получается из следующей схемы :

b	b	b	. . .	b
b	$b (\alpha + 1)$	$b (\alpha^2 + \alpha + 1)$	. . .	$b (\alpha^n + \alpha^{n-1} + \ldots + \alpha + 1)$

Т.е. наибольший член, получающийся в течение вычислений –
это значение $p(x)$ в точке $x = \alpha$ и $\eta = b (\alpha^n + \alpha^{n-1} + \ldots + \alpha + 1)$

Однако $\eta = b (\alpha^n + \alpha^{n-1} + \ldots + \alpha + 1) \le b ((n + 1) \alpha^n)$.
Следовательно

$$T_{RUF-HOR} [p(x) , \alpha] = O [n * L(\alpha) * L \{ b ((n + 1) \alpha^n) \}]$$
$$= O [n * L(\alpha) * \{ L(b) + L(n + 1) + n L(\alpha) \}]$$

Однако во всех практических приложениях $L(n+1) = 1$ и $L(b) + n L(\alpha) \le n L(\alpha) L(b) + 1$.
Поэтому

$$T_{RUF-HOR} [p(x) , \alpha] = O [n^2 * L^2(\alpha) * L \{ | p(x) |_\infty \}]$$

Значения и корни полиномов

Применение метода Руффини – Горнера – 1

Пример. Вычислим значение полинома $p(x) = x^3 - 7x + 7$ в точке $\alpha = 3$, работая с целыми числами.

Пользуясь методом Руффини – Горнера, получаем $p(3) = 13$.

1	0	-7	7
1	3	2	13

В первой строке расположены все коэффициенты полинома $p(x)$, включая нулевые.
Старший коэффициент стоит слева.

Вторая строка формируется следующим образом.
Первый (крайний левый) элемент второй строки – это старший коэффициент полинома $p(x)$.
Этот первый элемент умножаем на α
и прибавляем к полученному произведению второй элемент первой строки.
Записываем сумму как второй элемент второй строки. (При $\alpha = 3$ имеем $1 * 3 + 0 = 3$)
В общем случае, для вычисления «следующего» элемента второй строки,
умножаем последний вычисленный элемент второй строки на α
и прибавляем к произведению «следующий» коэффициент из первой строки.

Значения и корни полиномов

Применение метода Руффини – Горнера – 2

Таким образом, вычисляем остальные элементы второй строки :

3-й элемент : 3 * 3 – 7 = 2
4-й элемент : 2 * 3 + 7 = 13

Заметим, что p (3) = 13 (последний элемент второй строки) –
это остаток, полученный при делении полинома ($x^3 - 7x + 7$) на бином (x – 3) .
Частное q (x) этого деления также вычисляется с помощью вышеуказанной схемы,
т.е. формируется из остальных (за исключением последнего) элементов второй строки :

$q(x) = x^2 + 3x + 2$

Замечание. Учитывая функциональные возможности метода Руффини – Горнера,
он известен также как **синтетический алгоритм деления** полиномов.

Замечание. Последовательно применяя синтетический алгоритм деления,
можно вычислить все коэффициенты полинома p (y),
полученного из исходного полинома p (x) с помощью подстановки $x = \alpha + y$.

Значения и корни полиномов

Вычисление значений ↔ Интерполяция

Рассмотрим полином

$$p(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \qquad (1)$$

с коэффициентами из кольца R .

Он однозначно представим одним из следующих списков :

(1) списком коэффициентов $a_0, a_1, \ldots a_{n-1}$ (2)

(2) списком значений полинома $v_0, v_1, \ldots v_{n-1}$ (3)

$v_j = p(x_j)$ (4)

в n различных точках $x_0, x_1, \ldots x_{n-1}$ (5)

Переход от списка (2) к списку (3) согласно формулам (4)
представляет собой вычисление полинома (1) в n различных точках (5) .

Переход от списка (3) к списку (2) сводится к задаче определения коэффициентов полинома (1) по его значениям в n различных точках, т.е. к задаче отыскания a_i из уравнений $p(x_j) = v_j$
Такая задача называется интерполяционной задачей **Жозефа Луи Лагранжа**.

План лекции: тема подраздела

- Вычисление значений и корней полиномов
- **Разложение полиномов на неприводимые множители**
- Разложение полиномов на свободные от квадратов множители
- Разложение на множители полиномов над конечными полями

Неприводимые множители

Вводные замечания

Замечание 1. Концептуально, задача факторизации полинома p (x)
(от одной переменной, с целыми коэффициентами)
состоит в выяснении существования полиномов g (x) и h (x)
(степени которых строго меньше степени полинома p (x)), таких, что p (x) = g (x) * h (x) .

Замечание 2. Задачу факторизации полиномов
одним из первых решил **Исаак Ньютон** (1707),
предложив в своей работе «Arithmetica Universalis»
метод нахождения линейных и квадратичных множителей
полиномов с целыми коэффициентами.

Замечание 3. Самый простой способ нахождения множителей
данного полинома p (x), (при deg (p (x)) = k) –
это алгебраически найти его корни d_i и тогда имеем:

$$p(x) = (x - d_1) * (x - d_2) * \ldots * (x - d_k)$$

Однако алгебраический метод определения корней полинома
возможен только если $k \leq 4$.

Неприводимые множители

Свойства неприводимых полиномов (в C [x])

Замечание. Неприводимые полиномы играют ту же роль
в задаче факторизации полиномов,
что и простые числа в теории разложения на множители целых чисел.

Теорема (основная теорема алгебры). Каждый полином p (x) из **C** [x] степени ≥ 1
имеет корень в **C**.

Замечание. Известно, что поле **C** было изобретено,
чтобы содержать корни неприводимых полиномов из **R** [x].
(В частности, мнимая единица $i = \sqrt{(-1)}$ – корень полинома $x^2 + 1$).
Кроме того, из вышеуказанной теоремы следует,
что единственные отличные от констант неприводимые полиномы в **C** [x] –
это полиномы степени 1.

Замечание. Знание того, какие полиномы в **R** [x] (или в **C** [x]) неприводимы,
не облегчает разложение данного полинома.

Неприводимые множители

Свойства неприводимых полиномов (в R [x])

Теорема. Отличный от константы полином p (x) из **R** [x] неприводим,
если и только если :

либо $p(x)$ имеет степень 1
либо $p(x) = a x^2 + b x + c$ и $b^2 - 4 a c < 0$

Свойства неприводимых полиномов (в J [x])

Теорема. Пусть J – поле и $p_1(x), p_2(x) \in J[x]$.
Если неприводимый полином $m(x) \in J[x]$ делит произведение $p_1(x) * p_2(x)$,
то m (x) должен делить либо $p_1(x)$, либо $p_2(x)$.

Теорема (о единственности разложения полинома на простые множители).
Пусть J – поле и $p(x) \in J[x]$, $\deg(p(x)) > 0$
Тогда полином p (x) может быть однозначно разложен
в произведение неприводимых нормированных полиномов над J [x] ,
т.е. $p(x) = c * p_1(x) * p_2(x) * \ldots * p_k(x)$, $p_i(x) \in J[x]$, $i = 1, 2, \ldots k$, $c \in J$.
Такое разложения является единственным с точностью до порядка сомножителей.

Неприводимые множители

Простые и кратные сомножители

Так же как для целых чисел,
можно записать разложение на множители полинома p (x) в **R** [x] в виде :

$$p(x) = [p_1(x)]^{e_1} * [p_2(x)]^{e_2} * \ldots * [p_k(x)]^{e_k}$$

Если какое-либо из чисел e_i больше единицы,
то говорят, что у полинома p (x) есть **кратный сомножитель**.

Пример. Полином $p(x) = (x - 1)^3 (x + 1)$ имеет кратный сомножитель,
а полином $p(x) = (x - 1)(x + 1)$ его не имеет.
В первом случае говорят, что у p (x) есть **кратный корень** в J ,
а во втором – что p (x) имеет только **простые корни**.

Таким образом, разложение на множители в **R** [x] или в **C** [x]
эквивалентно нахождению корней полинома.

Неприводимые множители

Однозначность разложения на множители

Теорема (Гаусс). Пусть J – область целостности, $p(x) \in J[x]$, $\deg(p(x)) > 0$
Тогда полином $p(x)$ может быть единственным образом
разложен в произведение неприводимых нормированных полиномов над J [x]
при условии, что каждый элемент в кольце J может быть единственным образом
разложен в произведение неразложимых элементов.

Следствие. $\mathbf{Z}[x]$ – это область с однозначным разложение на множители,
хотя она не является евклидовой.

Теорема. Если J – евклидова область,
то она является областью с однозначным разложением на множители,
т.е. каждый её отличный от нуля элемент или обратим,
или может быть представлен в виде конечного произведения
неразложимых элементов.

Неприводимые множители

Неприводимые полиномы в Q [x]

Замечание. В отличие от **R** [x] или **C** [x] ,
где мы можем явно описать все неприводимые полиномы,
в **Q** [x] мы можем дать только некоторые достаточные критерии неприводимости.

Покажем, что разложение на множители в **Q** [x] – это то же самое,
что разложение на множители в **Z** [x] .

Пусть $p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$
– это полином с рациональными коэффициентами.

Замечание. Умножив p (x) на НОК знаменателей коэффициентов,
получим новый полином s (x) с целыми коэффициентами.
Поэтому изучая полиномы в **Q** [x] мы можем всегда предполагать,
что их коэффициенты – целые числа.

Неприводимые множители

Примитивные полиномы в Q [x]

Определение. Полином p (x) $\in$ **Q** [x] называется **примитивным**,
если его коэффициенты – целые числа и их НОД равен 1.

Теорема. Произведение двух примитивных полиномов из **Q** [x]
также является примитивным полиномом в **Q** [x] .

Доказательство:

Очевидно, что произведение двух полиномов с целыми коэффициентами
– это тоже полином с целыми коэффициентами.
Пусть p (x) и q (x) – два примитивных полинома.
Тогда по определению примитивности для любого простого числа p имеем:

$$p(x) \neq 0 \pmod{p} \qquad q(x) \neq 0 \pmod{p}$$

Поэтому такое же свойство верно для произведения, т.е:

$$p(x)\,q(x) \neq 0 \pmod{p}$$

для любого простого p.
Отсюда следует, что никакое простое число
не делит все коэффициенты полинома p (x) q (x) .
Следовательно, НОД коэффициентов полинома p (x) q (x) равен 1
и полином p (x) q (x) примитивен.

Неприводимые множители

Неприводимые полиномы в Z [x]

Определение. Полином $p(x) \in \mathbf{Z}[x]$ называется **неприводимым**, если он не разлагается в произведение двух полиномов степеней ≥ 1 с целыми коэффициентами.

Замечание. В одной из теорем Гаусс доказал, что полином неприводим в $\mathbf{Z}[x]$, если и только если он неприводим как полином в $\mathbf{Q}[x]$.

Теорема. Если $p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$ – это полином в $\mathbf{Z}[x]$ и r / s – его корень, такой, что $(r, s) = 1$, то $s \mid c_n$ и $r \mid c_0$.

Доказательство:

Т.к. r / s – корень полинома $p(x)$, то подставив это значение в полином, получим:

$$c_n (r^n / s^n) + c_{n-1} (r^{n-1} / s^{n-1}) + \ldots + c_1 (r / s) + c_0 = 0$$

Далее, умножая на s^n, получим:

$$c_n r^n + c_{n-1} r^{n-1} s + \ldots + c_1 r s^{n-1} + c_0 s^n = 0$$

Откуда $c_n r^n = \lambda s$ для некоторого $\lambda \in \mathbf{Z}$.

Следовательно, $s \mid c_n r^n$ и учитывая, что $(r, s) = 1$, имеем $s \mid c_n$.

Аналогично, $c_0 s^n = \mu r$ для некоторого $\mu \in \mathbf{Z}$ и т.к. $(r, s) = 1$, то $r \mid c_0$.

Неприводимые множители

Критерий неприводимости полиномов

Теорема (критерий Фердинанда Готтхольда Макса Эйзенштейна, 1850).
Пусть $p(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_{n-1} x + c_n$ – это полином в $\mathbf{Z}[x]$.
Если существует простое число p, такое, что p не делит c_0
и делит остальные целые коэффициенты $c_1, c_2, \ldots, c_{n-1}, c_n$,
но при этом p^2 не делит c_n, то полином $p(x)$ неприводим.

Замечание. Теорема верна и в том случае, когда коэффициенты полинома $p(x)$
принадлежат области целостности,
которая является областью с однозначным разложением на множители.

Пример. Согласно критерию Эйзенштейна полином $p(x) = x^n - 2$ неприводим при любом n.

Замечание. Критерий Эйзенштейна показывает,
что в $\mathbf{Q}[x]$ имеются неприводимые полиномы любой степени.
Однако имеются полиномы, к которым критерий Эйзенштейна неприменим.
В частности, для полинома $p(x) = x^2 - 6x + 7$ критерий Эйзенштейна бесполезен,
однако этот полином неприводим.

Неприводимые множители

Метод Кронекера

Леопольд Кронекер предложил (1882) метод разложения
полинома с целыми коэффициентами на неприводимые множители
над кольцом целых чисел.

Иными словами, для данного полинома f (x) $\in$ **Z** [x] находится полином g (x) $\in$ **Z** [x],
такой, что g (x) | f (x) или доказывается, что такого полинома нет.

Метод Кронекера основан на следующих положениях:

- если степень полинома f (x) равна n,
  то степень хотя бы одного множителя g (x) полинома f (x) не превосходит [*n* / 2];
- значения как f (x), так и g (x) в целых точках — целые числа,
  причём g (i) делит f (i) для любого целого i;
- при фиксированном i, если f (i) ≠ 0, то g (i) может принимать
  только конечное множество значений, состоящее из делителей числа f (i);
- коэффициенты полинома g (x) однозначно восстанавливаются по его значениям
  в [*n* / 2] +1 точке.

Таким образом, для g (x) получается конечное число возможностей;
непосредственным делением проверяем, получили ли мы делитель полинома f (x) .

Неприводимые множители

Одномерный алгоритм Кронекера

Вход:
f (x) ∈ **Z** [x] , n – степень f (x)

Выход:
g (x) ∈ **Z** [x] , m – степень g (x) ,
если found = TRUE или found = FALSE

[Инициализация]
found := FALSE // Признак того, что делитель найден (по умолчанию – не найден)
[Поиск корней f (x) среди целых чисел от 0 до [n / 2]]
Цикл Для i = 0 .. [n / 2]
Если f (i) = 0 **То** found := TRUE, g (x) : = x – i , m := 1
Конец Цикла // Ответ найден
[Поиск делителей]
Если found = FALSE **То**
U : = множество целочисленных делителей числа f (0)
// Поиск множителя степени i
Цикл Для i = 0 .. [n / 2]
M := множество целочисленных делителей числа f (i)
W := декартово произведение U на M
Цикл Для Каждого w ∈ W
Построить полином g (x) степени i такой, что
g (j) = w (j) для j = 0 .. i
Если f (x) делится на g (x) **То** found := TRUE, m := i, **Выход** // Ответ найден
Конец Цикла
Конец Цикла
Конец Если

Неприводимые множители

Анализ метода Кронекера

Замечание. Достаточно научиться разлагать на множители
полиномы со старшим коэффициентом, равным 1.
Действительно, если старший коэффициент полинома равен a,
то домножив этот полином на a^{n-1} и сделав замену $x = y/a$,
сводим исходную задачу к этому случаю.
После ее решения остается сделать обратную замену
и сократить на общий множитель a^{n-1}.
Однако указанный метод неэффективен (из-за увеличения коэффициентов)
поэтому почти не применяется.

Замечание. Метод Кронекера также применим для факторизации
полиномов от нескольких переменных.
Причём для некоторых областей определения коэффициентов
(в частности, для поля комплексных чисел)
он является единственным известным алгоритмом решения этой задачи.

Замечание. Метод Кронекера является обобщением
первого метода факторизации полиномов – метода Ньютона,
а также метода, предложенного (1793) **Фридрихом фон Шубертом**.

Неприводимые множители

Метод Кронекера (многомерный случай) – 1

Пусть J – область целостности с однозначным разложением на множители.
Требуется разложить полином $f(x_1, x_2, \ldots, x_n) \in J[x_1, x_2, \ldots, x_n]$
на неприводимые множители.

Основная идея решения состоит в следующем.

Исходная задача редуцируется к одномерному случаю
путём введения новой неизвестной и заменой всех переменных
достаточно высокими степенями этой неизвестной.

Далее производится факторизация получившегося полинома.

Наконец, выполняется обратная подстановка,
после которой пробным делением необходимо убедиться,
получено ли желаемое разложение.

Неприводимые множители

Метод Кронекера (многомерный случай) – 2

Таким образом, исходная задача переопределяется следующим образом.

Выберем целое d большее,
чем степени отдельных переменных в $f(x_1, x_2, \ldots, x_n)$.

Заменим все переменные степенями новой неизвестной y:

$$F(y) = S_d(f) = f(y, y^d, \ldots, y^{d^{n-1}})$$

Тогда требуется разложить полученный полином на неприводимые множители:

$$F(y) = g_1(y) \ldots g_s(y) \qquad g_i(y) \in \mathbf{Z}[y] \qquad 1 \le i \le s$$

После выполнения факторизации полинома $F(y)$
получим множество $G = \{ g_i(y) \}$ неприводимых множителей.
Обратное преобразование производится на мономах
с помощью следующей формулы :

$$(S_d(y^{b_1 + d b_2 + \ldots + d^{k-1} b_k}))^{-1} = x_1^{b_1} \ldots x_k^{b_k} \qquad 0 \le b_i \le d \text{ для } 1 \le i \le k \quad k \in \mathbf{Z}$$

Далее $(S_d)^{-1}$ распространяется по линейности.

Неприводимые множители

Многомерный алгоритм Кронекера

Вход:

$F(y) \in \mathbf{Z}[y]$

Выход:

$G = \{ g_i(y) \}$

[Инициализация]

$G := \{\}$

$M := \{ 1, 2, \ldots, s \}$

[Основной цикл]

Цикл Для $m = 1 .. [s / 2]$

Цикл Для Каждого подмножества $\{ i_1, \ldots, i_m \} \subseteq M$

$g_{i_1, \ldots, i_m}(x_1, \ldots, x_n) := (S_d (G_{i_1}(y) \ldots G_{i_m}(y)))^{-1}$

Если f делится на g **То**

добавить g в список G ,

изменить указатель списка G ,

$f := f / g$,

$s := s - m$,

удалить из M текущее подмножество $\{ i_1, \ldots, i_m \}$

Конец Если

Конец Цикла Для Каждого

Конец Цикла Для

Добавить f в список G

План лекции: тема подраздела

- Вычисление значений и корней полиномов
- Разложение полиномов
  на неприводимые множители
- **Разложение полиномов**
  на свободные от квадратов множители
- Разложение на множители полиномов
  над конечными полями

Свободные от квадратов множители

Базовые определения

Определение. Полином p (x) называется **свободным от квадратов**,
если не существует полинома q (x) положительной степени,
такого, что $q^2(x) \mid p(x)$.

Определение. Пусть J – произвольная числовая область и полином $p(x) \in J[x]$.
Тогда p ‘ (x) = D [p (x)] называется **производной** полинома p (x) ,
если выполнены следующие правила:

(1) $D[a x^n] = a n x^{n-1}$ для $a \in J$ и $n \geq 0$

Следует отметить, что $D[a x^n] = 0$ если $J = \mathbf{Z}_n$

(2) D [p (x) + q (x)] = D [p (x)] + D [q (x)]

Напомним, что для производных имеет место известное правило произведения :

D [p (x) * q (x)] = p (x) * D [q (x)] + D [p (x)] * q (x)

Свободные от квадратов множители

Делимость производной полинома

Теорема. Пусть J – область с однозначным разложением на множители характеристики нуль.
Пусть p (x) – примитивный отличный от константы полином в J [x] .
Пусть $p(x) = [p_1(x)]^{e_1} [p_2(x)]^{e_2} \dots [p_n(x)]^{e_n}$
– однозначное разложение полинома p (x)
на неприводимые сомножители и p ‘ (x) – его производная.
Тогда

$$НОД (p(x) , p'(x)) = [p_1(x)]^{e_1 - 1} [p_2(x)]^{e_2 - 1} \dots [p_n(x)]^{e_n - 1}$$

Следствие 1. Если НОД (p (x) , p ‘ (x)) = 1 ,
то p (x) не имеет кратных сомножителей, и наоборот.

Следствие 2. Простые корни полинома не являются корнями его производной.

Следствие 3. Пусть J – поле и p (x) – неприводимый полином в J [x] , который делит $s(x) \in J[x]$
Тогда $[p(x)]^2 \mid s(x)$, если и только если $p(x) \mid s'(x)$

Свободные от квадратов множители

Разложение на свободные от квадратов множители

Пусть p (x) – примитивный отличный положительной степени от одной переменной, определённый на J – области с однозначным разложением на множители.
(Заметим, что выбирая p (x) примитивным,
мы не ограничиваем общности рассмотрения).

Предположим, что $p(x) = [p_1(x)]^{e_1} [p_2(x)]^{e_2} \dots [p_n(x)]^{e_n}$ – разложение полинома p (x) на неприводимые множители $p_i(x)$ положительной степени так, что $e_i > 0$ для каждого i
Пусть $e = \max (e_1 , e_2 , \dots , e_n)$

Для $1 \le i \le e$ положим

$J_i = \{ j : e_j = i \}$

$s_i(x) = \prod p_j(x)$ для всех $j \in J_i$

Тогда очевидно :

$p(x) = \prod [s_i(x)]^i$ для всех $1 \le i \le e$

что называется **разложением полинома** p (x) **на свободные от квадратов множители**.

Свободные от квадратов множители

Вычисление СКВС – 1

Замечание. Некоторые из полиномов $s_i(x)$ могут быть равны 1.

$s_1(x)$ – это произведение всех линейных множителей, соответствующих простым корням.

$s_2(x)$ – это произведение всех сомножителей, соответствующих двойным корням и т.д.

Полиномы $s_i(x)$ – это **свободные от квадратов сомножители** (СКВС) полинома $p(x)$.

Вычисление СКВС осуществимо с помощью теоремы о НОД :

$$r(x) = \text{НОД}(p(x), p'(x)) = \prod [p_i(x)]^{e_i - 1} \text{ для всех } 1 \le i \le n$$
$$= \prod [s_i(x)]^{i-1} \text{ для всех } 1 \le i \le e$$

Заметим, что в приведённых формулах $s_1(x)$ не присутствует.

Свободные от квадратов множители

Вычисление СКВС – 2

Тогда наибольший свободный от квадратов делитель полинома p (x) равен :

$$t(x) = p(x) / r(x) = \prod p_i(x) \quad \text{для всех } 1 \le i \le n$$
$$= \prod s_i(x) \quad \text{для всех } 1 \le i \le e$$

Следовательно :

$$v(x) = \text{НОД}\,(r(x), t(x)) = \prod s_i(x) \quad \text{для всех } 2 \le i \le e$$

Поэтому $s_1(x) = t(x) / v(x)$, т.е. первый СКВС полинома p (x) может быть вычислен с помощью дифференцирования, вычисления НОД и деления.

Повторяя процесс вычислений с r (x) вместо p (x), можно вычислить $s_2(x)$ как первый СКВС полинома r (x) и, в конечном счёте, получить все СКВС полинома p (x).

Свободные от квадратов множители

Алгоритм разложения на СКВС

Вход:
p (x) – примитивный полином
положительной степени от одной переменной
над областью J характеристики нуль
с однозначным разложением на множители

Выход:
Полиномы $s_i(x)$ и число e такие, что
$p(x) = \prod [s_i(x)]^i$ для всех $1 \le i \le e$
(разложение полинома p (x) на СКВС)

[Инициализация]
r (x) : = НОД (p (x) , p ‘ (x))
t (x) : = p (x) / r (x)
j : = 1
[Конец ?]
Если deg [r (x)] = 0 **То** { e := j , $s_j(x)$: = t (x) , **Выход** }
[Вычисление $s_j(x)$ **]**
v (x) : = НОД (r (x) , t (x))
$s_j(x)$: = t (x) / v (x)
[Обновление]
r (x) : = r (x) / v (x) , t (x) : = v (x) , j : = j + 1
Переход к **[Конец ?]**

Свободные от квадратов множители

Анализ временной сложности алгоритма разложения на СКВС – 1

Очевидно, что время работы алгоритма
доминируется вычислениями НОД,
производимыми на шаге **[Вычисление** $s_j(x)$ **]**.

Если n = deg [p (x)] , то n ограничивает
количество выполнений цикла,
состоящего из шагов **[Конец ?] [Вычисление** $s_j(x)$ **] [Обновление] ,**
в котором находится наиболее трудоёмкий шаг **[Вычисление** $s_j(x)$ **]**

Кроме того, время, необходимое для вычисления r (x) : = НОД (p (x) , p ‘ (x))
на шаге **[Инициализация]** – это верхняя граница
времени каждого вычисления НОД
на шаге **[Вычисление** $s_j(x)$ **]**.

Свободные от квадратов множители

Анализ временной сложности алгоритма разложения на СКВС – 2

Имеют место два случая.

Случай 1. Полином $p(x) \in J[x]$, где J – поле.

В этом случае НОД ($p(x)$, $p'(x)$) вычисляется за время $O(n^2)$,
и т.к. необходимо n выполнений шага **[Вычисление** $s_j(x)$ **]**, то

$$\mathbf{T_{сквс} = O(n^3)}$$

Случай 2. Полином $p(x) \in J[x]$, где $J = \mathbf{Z}$.

В этом случае НОД ($p(x)$, $p'(x)$) вычисляется за время $O(n^5 L^2(|p(x)|_\infty))$,
и т.к. необходимо n выполнений шага **[Вычисление** $s_j(x)$ **]**, то

$$\mathbf{T_{сквс} = O(n^6 L^2(|p(x)|_\infty))}$$

Свободные от квадратов множители

Пример применения алгоритма СКВС

Пример. Пусть требуется найти свободные от квадратов сомножители для полинома $p(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$

При первом проходе имеем :

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

$t(x) = x^2 - 1$

$v(x) = x^2 - 1$

$s_1(x) = 1$, т.е. линейные сомножители отсутствуют.

При втором проходе имеем :

$r(x) = x - 1$

$t(x) = x^2 - 1$

$v(x) = x - 1$

$s_2(x) = x + 1$, т.е. $(x + 1)^2$ – сомножитель исходного полинома.

В начале третьего (последнего для данного примера) прохода имеем :

$r(x) = 1$

$t(x) = x - 1$

На шаге **[Конец ?]** видим, что степень полинома $r(x)$ равна нулю,
т.е. $s_3(x) = t(x) = x - 1$, т.е. $(x - 1)^3$ – также сомножитель исходного полинома.
Окончательно : $p(x) = (x + 1)^2 (x - 1)^3$

План лекции: тема подраздела

- Вычисление значений и корней полиномов
- Разложение полиномов
  на неприводимые множители
- Разложение полиномов
  на свободные от квадратов множители
- **Разложение на множители полиномов над конечными полями**

Полиномы над конечными полями

Вводные замечания

Замечание. Все ранее рассмотренные методы факторизации полиномов
имеют экспоненциальную временную сложность.
Гораздо лучшие результаты получаются при использовании
методов разложения «по модулю p»
вместе с техникой «подъёма» разложения «по модулю p»
до разложения на множители над целыми числами.

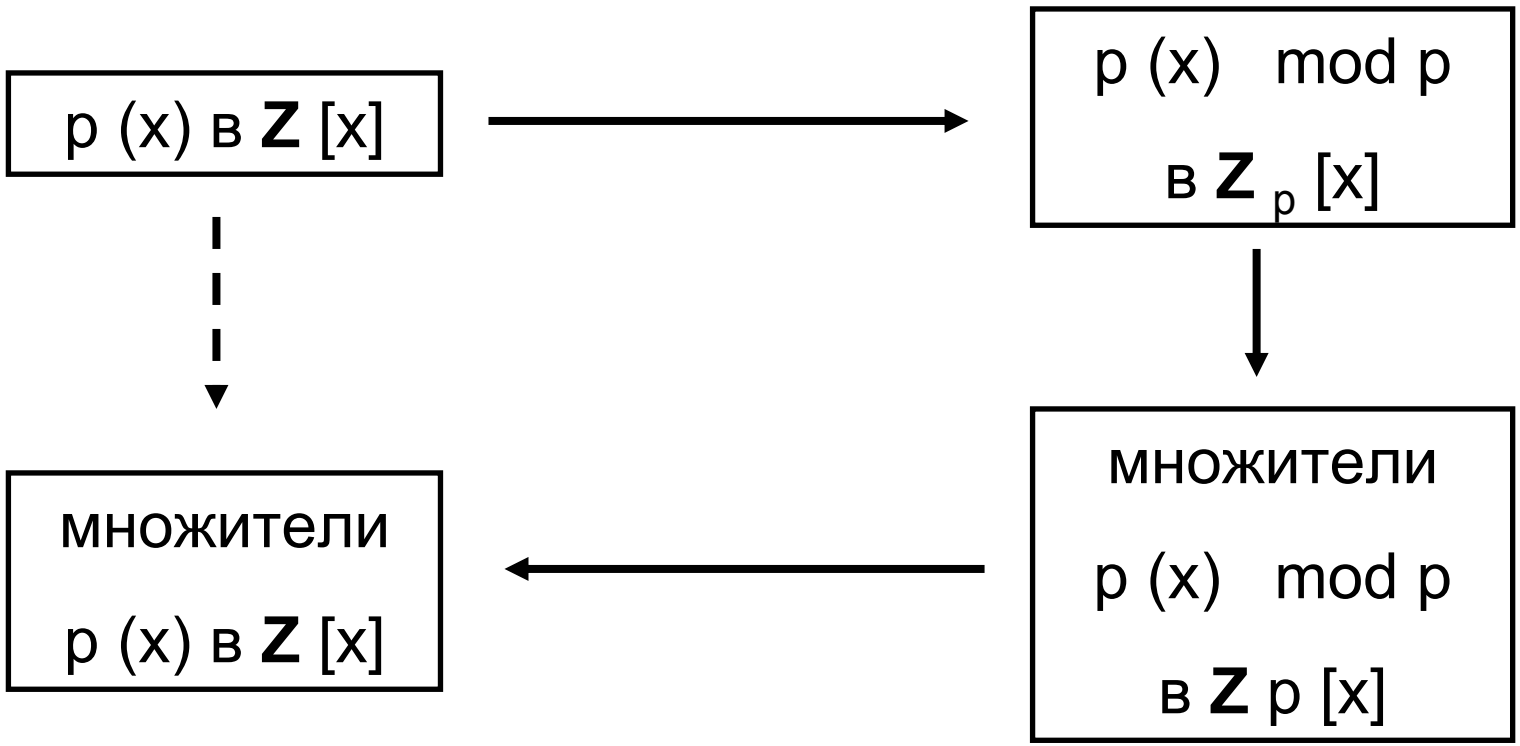
Однако, несмотря на эффективность указанного подхода
почти во всех практических случаях,
в худшем случае и этот подход имеет экспоненциальную границу сложности.

Замечание. Модулярные методы факторизации полиномов иногда называют «окольными»
или методами, использующими схему, т.к. они решают задачу не прямо,
а переопределяя её условия так, чтобы максимально снизить сложность решения.

Замечание. Существует L^3 – метод, так названный, исходя из начальных букв
фамилий его авторов (А. Ленстра, А. Ленстра-мл., Л. Ловас) ,
который с помощью теории решёток позволяет факторизовать полином
за полиномиальное время.

Полиномы над конечными полями

«Окольный» метод факторизации полинома



Полиномы над конечными полями

Основные шаги «окольного» метода

Исходные данные. Полином $p(x) \in \mathbf{Z}[x]$, т.е. $p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$, $c_i \in \mathbf{Z}$ который необходимо разложить на неприводимые множители.
Причём, без потери общности, полагаем, что $p(x)$ нормирован, т.е. $c_n = 1$

Шаг 1. Исключить из $p(x)$ нетривиальные сомножители нулевой степени и кратные сомножители. Это достигается вычислением НОД в $\mathbf{Z}$ и в $\mathbf{Z}[x]$.

Шаг 2. Выбрать простое число p, такое, что разложение на множители в $\mathbf{Z}_p[x]$ возможно.

Шаг 3. Для выбранного числа p выполнить разложение на множители в $\mathbf{Z}_p[x]$:

$p_{SF}(x) \equiv \prod g_k(x) \pmod p$ для всех $1 \le k \le r$, (SF – Square Free – свободные от квадратов)

где $g_k(x) \in \mathbf{Z}_p[x]$, r – количество неприводимых сомножителей

Шаг 4. Используя конструкции (на основе p-адических чисел) **Курта Гензеля**, выполнить линейный и/или квадратичный «подъём» полиномов $g_k(x)$ до соответствующих полиномов $h_k(x) \pmod{p^j}$ таких, что :

$p_{SF}(x) \equiv \prod h_k(x) \pmod{p^j}$ для всех $1 \le k \le r$

для достаточно большого положительного целого числа j .

Шаг 5. Разбить множество полиномов $h_k(x)$ на подмножества h_i, $i = 1, 2, \ldots, f$ такие, что :

$p_i(x) \equiv \prod h_k(x) \pmod{p^j}$ для всех $h(x) \in h_i$

Полиномы над конечными полями

Сущность 1-го шага «окольного» метода

Вычисляем примитивный свободный от квадратов полином.
В качестве результата получаем нормированный свободный от квадратов полином

$$p_{SF}(x) \equiv \mathbf{\Pi}\, p_i(x) \quad \text{для всех } 1 \le i \le q\ ,$$

где все $p_i(x)$ – различные неприводимые полиномы.
Наша цель – вычислить эти q сомножителей $p_i(x)$.

Полиномы над конечными полями

Сущность 2-го шага «окольного» метода – 1

Определим требования к выбору числа p .

Требование 1.

Полином $p_{SF}(x)$, полученный на шаге 1, должен **иметь ту же самую степень** и **оставаться свободным от квадратов** по модулю p.

Т.к. полином $p_{SF}(x)$ нормирован, то p не делит его старший коэффициент, и, следовательно, степень остаётся той же самой по модулю p.
Кроме того, мы можем эффективно проверить,
является ли полином $p_{SF}(x)$ (mod p) свободным от квадратов,
проверив равенство НОД ($p_{SF}(x)$, $p'_{SF}(x)$) = 1 в $\mathbf{Z}_p[x]$.
Справедливость этого утверждения следует из того, что если
$p(x) = [p_1(x)]^2 p_2(x)$, то $p'(x)$ является кратным полинома $p_1(x)$.
Поэтому если НОД ($p(x)$, $p'(x)$) = 1 , то мы знаем, что $p(x)$ свободен от квадратов
В то время как, если НОД ($p(x)$, $p'(x)$) $\neq$ 1 и НОД ($p(x)$, $p'(x)$) $\neq p(x)$,
то нам нужно разложить на множители НОД ($p(x)$, $p'(x)$) и $p(x)$ / НОД ($p(x)$, $p'(x)$) .
Наконец, если НОД ($p(x)$, $p'(x)$) = $p(x)$, то $p(x) = q(x^p) = [q(x)]^p$
и нам нужно разложить на множители $q(x)$.

Полиномы над конечными полями

Сущность 2-го шага «окольного» метода – 2

Требование 2.

Правильность выбора значения используемого простого числа p.

Применение больших простых чисел сокращает количество шагов, необходимых для «подъёма» разложения $p_{SF}(x)$ из $\mathbf{Z}_p[x]$ до $\mathbf{Z}[x]$. Однако эффективные алгоритмы разложения на множители в $\mathbf{Z}_p[x]$ имеются только для малых p.

Полиномы над конечными полями

Сущность 2-го шага «окольного» метода – 3

Требование 3.

Количество r сомножителей в полном разложении по модулю p.

Если $p_{SF}(x)$ – неприводимый полином,
но по модулю p расщепляется на $r > 1$ неприводимых сомножителей,
то в конце «подъёма» мы получаем r сомножителей
и в итоге на шаге 5 для определения истинных сомножителей
полинома $p_{SF}(x)$ над целыми числами
должно рассматриваться 2^{r-1} подмножеств сомножителей.
(Именно это определяет экспоненциальную сложность алгоритма).
Некоторое упрощение задачи получим,
если на шаге 3 разложить $p_{SF}(x)$ на множители
по модулю нескольких простых чисел p^i,
для которых полином остаётся свободным от квадратов,
и выбрать из них в качестве p число,
дающее наименьшее количество неприводимых сомножителей.

Полиномы над конечными полями

Сущность 3-го шага «окольного» метода

Далее будут рассмотрены способы получения такого разложения.

Замечание. Число q истинных сомножителей полинома $p_{SF}(x)$ над кольцом целых чисел (см. шаг 1) **не обязательно равно** числу r сомножителей полинома $p_{SF}(x)$ по модулю p.

Пример.

$x^2 + 2 \equiv (x - 2)(x - 1) \pmod 3$

Замечание. Существуют полиномы, неприводимые над целыми числами, которые могут быть разложены на множители по модулю p для любого простого p.

Пример.

Для любых целых чисел a, b и любого простого числа p полином $p(x) = x^4 + a x^2 + b^2$ разлагается на множители в $\mathbf{Z}_p[x]$.

Полиномы над конечными полями

Сущность 4-го шага «окольного» метода

После «подъёма» каждый истинный сомножитель $p_i(x)$ полинома $p_{SF}(x)$ соответствует :

- или отдельному полиному $h_i(x)$;
- или произведению (mod p^j) некоторых из них.

Это соответствие выявляется на шаге 5.

Сущность 5-го шага «окольного» метода

Истинные сомножители полинома $p_{SF}(x)$ над целыми числами
определяются пробным делением.
Т.е. получив на предыдущем шаге сомножители $h_1(x), h_2(x), \ldots, h_r(x)$
полинома $p_{SF}(x)$ (mod p^j) , мы должны рассмотреть каждое сочетание этих сомножителей,
проверяя делением, является ли их произведение по mod p^j истинным сомножителем.
Если найден истинный сомножитель, то полагаем $p_{SF}(x) := p_{SF}(x) / p_i(x)$
и удаляем соответствующие значения $h_i(x)$ из списка.
Необходимо рассмотреть только те сочетания, для которых степень $\leq \lfloor \deg(p(x)) / 2 \rfloor$

Полиномы над конечными полями

Временная сложность «окольного» метода

В худшем случае «окольный» метод разложения
имеет экспоненциальное время работы,
т.к. r может быть так же велико, как и n ,
и потребуется выполнить большое число пробных делений
(а именно 2^n).

Однако, в среднем $r = \ln(n)$,
и поскольку среднее значение величины 2^r
приблизительно равно n , то **среднее время вычислений**
«окольного» алгоритма имеет полиномиальную оценку.

Полиномы над конечными полями

Алгоритмы факторизации в $Z_p[x]$

Любой полином степени n в $Z_p[x]$
может быть разложен на множители за конечное число шагов,
т.к. существует p^n возможных полиномов степени < n ,
и мы можем просто проверить каждый из них,
используя обычный алгоритм деления полиномов.
Однако, очевидно, что этот метод проб и ошибок очень неэффективен.

Для **малых** простых p **Элвин Берлекэмп**
предложил (1967) эффективный алгоритм разложения на множители в $Z_p[x]$.
Этот алгоритм переводит задачу разложения на множители
в задачу решения системы линейных уравнений с коэффициентами в $Z_p[x]$
и нахождения НОД.
Эффективность алгоритма Берлекэмпа обусловлена тем,
что каждая из переопределённых задач (система уравнений и НОД)
могут быть решены очень эффективно,

Замечание. Существует другой разработанный (1970) Берлекэмпом алгоритм
для разложения на множители полиномов в $Z_p[x]$ при **больших** простых p .

Полиномы над конечными полями

Обоснование алгоритма Берлекэмпа

Пусть полином p (x) свободен от квадратов.

Сформулируем несколько хорошо известных фактов
о вычислениях по модулю p.

Утверждение. Если a и b – два полинома по модулю p ,
то $(a + b)^{p} \equiv a^{p} + b^{p}$

Утверждение. Если a (x) – полином, то $a (x)^{p} \equiv a (x^{p})$ по модулю p .

Замечание. Указанные утверждения
обобщают аналогичные утверждения,
выполнимые для целых чисел.

Полиномы над конечными полями

Теорема Берлекэмпа – 1

Пусть полином $p(x)$ разлагается в произведение r неприводимых полиномов:

$$p(x) = p_1(x)\, p_2(x) \ldots p_r(x)$$

(Заметим, что в настоящий момент r неизвестно).
Поскольку $p(x)$ не имеет кратных сомножителей,
то полиномы $p_i(x)$ взаимно просты.

Пусть $s_1, \ldots, s_r$ – целые числа по модулю простого числа p.
По китайской теореме об остатках (см. следующую лекцию)
существует полином $v(x)$ такой, что

$$v(x) \equiv s_i \ (\mathrm{mod}\ p, p_i(x)) \qquad (*)$$

где вычисления выполняются по модулю полинома $p_i(x)$
и по модулю простого числа p.
Кроме того, степень полинома $v(x)$ меньше степени произведения полиномов $p_i(x)$,
т.е. степени полинома $p(x)$.
Полезность рассмотрения такого полинома $v(x)$ следует из того, что если $s_i \neq s_j$,
то НОД $(p(x), v(x) - s_i)$ делится на $p_i(x)$, но не делится на $p_j(x)$,
что приводит к разложению полинома $p(x)$.

Полиномы над конечными полями

Теорема Берлекэмпа – 2

Имеем следующее соотношение:

$$v(x)^p \equiv s_j^p \equiv s_j, \equiv v(x) \pmod{p_j(x), p}$$

Тогда по китайской теореме об остатках:

$$v(x)^p \equiv v(x) \pmod{p_j(x), p} \qquad (**)$$

Заменяя x на $v(x)$ в следствии из малой теоремы Фермы,
в котором утверждается, что каждое целое число по модулю p
является корнем полинома $x^p - x$, поэтому

$$x^p - x \equiv (x - 0)(x - 1) \ldots (x - (p - 1))$$

получаем, что:

$$v(x)^p - v(x) \equiv (v(x) - 0)(v(x) - 1) \ldots (v(x) - (p - 1)) \pmod{p} \qquad (***)$$

Таким образом, если $v(x)$ удовлетворяет соотношению (**),
то $p(x)$ делит левую часть соотношения (***),
а каждый из его неприводимых множителей $p_i(x)$
делит один из полиномов в правой части соотношения (***).
Но из этого следует, что полином $v(x)$ эквивалентен по модулю $p_i(x)$ целому числу,
т.е. что $v(x)$ удовлетворяет соотношению (*).

Теорема Берлекэмпа (1967). Решения $v(x)$ сравнения (*)
суть в точности решения сравнения (**)

Полиномы над конечными полями

Основная идея алгоритма Берлекэмпа

По теореме Берлекэмпа решения сравнения (*)
дают информацию о разложении полинома p (x) на множители.
Но вопрос о том, как их найти, остаётся открытым.

Основная идея алгоритма Берлекэмпа в том, что соотношение (**)
– это система линейных уравнений по модулю p на коэффициенты полинома v (x).

Пусть n – степень полинома p (x) .
Рассмотрим матрицу Q :

$$\begin{matrix} q_{00} & q_{01} & \cdots & q_{0\,n-1} \\ q_{10} & q_{11} & \cdots & q_{1\,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ q_{n-1\,0} & q_{n-1\,1} & \cdots & q_{n-1\,n-1} \end{matrix}$$

где элементы q определяются из сравнения :

$$x^{pk} \equiv q_{k\,n-1}\, x^{n-1} + \ldots + q_{k\,1}\, x + q_{k\,0} \quad (\mathrm{mod}\ p(x), p)$$

Если рассматривать полином как вектор его коэффициентов, то умножение на матрицу Q соответствует вычислению p-й степени полинома.
Таким образом, решения уравнения (**)
– это собственные векторы матрицы Q (mod p) для собственного значения.

Полиномы над конечными полями

Алгоритм Берлекэмпа

[Шаг 1]
Проверить, что у p (x) нет кратных сомножителей.
Если они есть, то выполнить разложение p (x)
на свободные от квадратов множители и применить данный алгоритм к каждому из них.
[Шаг 2]
Вычислить матрицу Q.
[Шаг 3]
Найти базис собственных векторов для собственного значения 1.
Всегда одним из собственных векторов является вектор [1 , 0 , … , 0].
Это отражает тот факт, что целые числа всегда являются решениями сравнения (**).
Число элементов в этом базисе равно числу неприводимых сомножителей полинома p (x).
[Шаг 4]
Вычислить НОД (p (x) , v (x) – s) для каждого целого числа s по модулю p ,
где v (x) – полином, соответствующий нетривиальному собственному вектору.
Это приведёт к разложению p (x) на множители.
Если при этом мы найдём меньше множителей, чем нужно,
то можно воспользоваться другим собственным вектором.

Полиномы над конечными полями

Сложность алгоритма Берлекэмпа

Время работы алгоритма равно

$$O(n^3 + p\,r\,n^2)$$

где r – число сомножителей
(как уже отмечалось ранее, его среднее значение равно $\ln(n)$).

Данный алгоритм является очень быстрым при малых p,
но может оказаться очень медленным при больших p.

Самым трудоёмким шагом алгоритма является шаг 4.
Вместе с тем, после шага 3
уже определено число неприводимых сомножителей.

Спасибо за внимание !

Вопросы ?