

Р-АДИЧЕСКИЙ АЛГОРИТМ ФАКТОРИЗАЦИИ

И. А. Блинец

В данной работе построен алгоритм факторизации многочленов с целыми коэффициентами, если нам известны его корни в поле p -адических чисел Q_p .

Пусть у нас есть многочлен с целыми коэффициентами, мы хотим найти его разложение в произведение неприводимых многочленов с целыми коэффициентами. Предположим, что мы знаем корни многочлена в Q_p . Мы можем считать, что у $f(x)$ нет кратных корней, иначе находим НОД многочленов $f(x)$, $f'(x)$ и потом просто поделим f на этот НОД, получив многочлен без кратных корней.

Лемма 1 (лемма Гензеля, [3, с.80]) Пусть f – многочлен с целыми коэффициентами a_i :

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

и существует $a \in Z_p$, такое что $|f(a)|_p < 1$ и $|f'(a)|_p = 1$. Тогда существует b такое, что $|b - a|_p \leq |f(a)|_p$ и $f(b) = 0$.

То есть, если $\deg f = n$ и мы нашли у $f(x)$ n различных корней в поле F_p и значение производной не равно 0 в F_p для этих корней, то мы можем легко найти с любой точностью наши корни в Q_p (следующая цифра линейно выражается через предыдущие).

Здесь мы не обсуждаем, как получить корни в Q_p , будет ли их n штук, а считаем, что корни у нас уже и так есть, в частности, в их поисках значительно помогает лемма Гензеля (см [2, 97], [4, 47], [3, 80]). Для многочлена $f(x) = a_0 + a_1x + \dots + x^n$, как известно, абсолютное значение его корней не превосходит $M = 1 + \max |a_i|$, ([3, с 10]). Отсюда видим, что если многочлен с целыми коэффициентами $g(x) = b_0 + b_1x + \dots + x^k$ - делитель многочлена $f(x)$, то $b_{k-1} \leq kM$, более того, $b_{k-i} \leq C_k^i M^i$. Пусть s - это такое минимальное натуральное число, что для любого $0 < i < n$ верно $p^s > C_{n-1}^i M^i$.

Для более точной оценки коэффициентов можно пользоваться следующим результатом (это позволяет уменьшить значение s):

Теорема 1 (неравенство Миньотта, [1, с.171]). Пусть $f(x) = a_0 + a_1x + \dots + a_mx^m$ и $g(x) = b_0 + b_1x + \dots + b_kx^k$ – многочлены с целыми коэффициентами. Тогда если f делится нацело на g , то

$$|b_j| \leq C_{k-1}^j \|f\| + C_{k-1}^{j-1} \|a_m\|,$$

где $\|f\| = \sqrt{a_0^2 + a_1^2 + \dots + a_m^2}$.

Таким образом, зная коэффициенты многочлена, мы можем определить, в каком промежутке лежат коэффициенты делителей.

Пусть x_1, x_2, \dots, x_n – корни $f(x)$ в Q_p . Найдем x_1, x_2, \dots, x_n с точностью до $2s$ p -адических знаков. Пусть $g(x) = \prod_{i=1}^k (x - y_i)$, где y_i – это некоторые различные x_j , $k < n$. Значит $b_{k-1} = -\sum_{i=1}^k y_i$. То есть, если найти $-\sum_{i=1}^k y_i$ с точностью до $2s$ знаков в p -адическом разложении, то мы получим, что цифры стоящие при $p^s, p^{s+1}, \dots, p^{2s-1}$ должны равняться 0 или $p-1$, поскольку иначе не будут выполняться следующие оценки: $b_{k-1} \leq kM$ и $kM < p^s$.

Теорема 2. Следующий алгоритм позволяет разложить $f(x)$ на множители либо установить неприводимость $f(x)$.

1) Находим корни x_1, x_2, \dots, x_n многочлена f в Q_p , с точностью до $2s$ p -адических знаков, где s описано выше.

2) Рассматриваем суммы $x_{i_1} + x_{i_2} + \dots + x_{i_k}, 1 \leq k < n$ из множества x_1, x_2, \dots, x_n с точностью до $2s$ p -адических знаков.

3) Выбираем те суммы $x_{i_1} + x_{i_2} + \dots + x_{i_k}$, в которых цифры при $p^s, p^{s+1}, \dots, p^{2s-1}$ – это 0 или $p-1$.

4) Берем одну из таких сумм и вычисляем $g(x) = \prod_{j=1}^k (x - x_{i_j})$.

5) Пусть $g(x) = \sum_{i=0}^k c_k x^k$. Если для любого коэффициента c_k , цифры стоящие при $p^s, p^{s+1}, \dots, p^{2s-1}$ – это все нули или все $p-1$, то находим многочлен $h(x)$, иначе переходим к шагу 7. $h(x)$ строим из $g(x)$ следующим образом:

$$h(x) = \sum_{i=0}^k d_k x^k$$

Если цифры у c_k при $p^s, p^{s+1}, \dots, p^{2s-1}$ это нули, то $d_k = c_k$, иначе $d_k = -(-c_k \bmod p^s)$

б) Проверяем делится ли $f(x)$ на $h(x)$, если да то находим частное. Таким образом мы получили требуемое, алгоритм завершен.

7) Если $g(x)$ не обладает свойством описанным в пункте 5, либо $f(x)$ не кратно $h(x)$, рассматриваем следующую сумму. Если таких сумм нет, то наш многочлен неприводим, алгоритм завершен.

Пример 1. Рассмотрим многочлен $f(x) = x^4 - 4x^3 + 7x^2 - 6x - 4$.

Если факторизация возможна, то только на два многочлена второй степени, ведь у f нет целых корней. Из неравенства Миньотта получаем, что коэффициенты делителя меньше 7^2 .

Находим его корни в Q_7 с точностью не меньшей 4 знаков: $x_1 = ..10616, x_2 = ..16274, x_3 = ..50455, x_4 = ..56053$. Поскольку многочлен f не имеет целых корней и сам он 4-й степени, то мы находим только попарные суммы $x_i + x_j$:

$$x_1 + x_2 = ...30133,$$

$$x_1 + x_3 = ...61404,$$

$$x_1 + x_4 = ...00002,$$

$$x_2 + x_3 = ...00002,$$

$$x_2 + x_4 = ...05300,$$

$$x_3 + x_4 = ...36541.$$

Получаем суммы с достаточным количеством лидирующих нулей (или $p-1$) в двух случаях: $x_1 + x_4$ и $x_2 + x_3$. Находим многочлены $g_1(x) = x - x_1 \quad x - x_4$ и $g_2(x) = x - x_2 \quad x - x_3$.

$$(x - x_1)(x - x_4) = x^2 - 2x + 4,$$

$$(x - x_2)(x - x_3) = x^2 - 2x + ..66666.$$

То, что мы получаем в $x_2x_3 = ...66666$ большое количество цифр $p-1$ (в нашем случае 6), говорит о том, что с большой вероятностью число отрицательное и равно -1, ведь в $Q_7 \quad ...00001 + ...66666 = ...00000$

Сейчас построим многочлены $h_1(x)$ и $h_2(x)$:

$$h_1(x) = x^2 - 2x + 4,$$

$$h_2(x) = x^2 - 2x - 1.$$

Проверяем, что

$$f(x) = (x^2 - 2x + 4)(x^2 - 2x - 1).$$

Таким образом, мы получили разложение $f(x)$ на 2 неприводимых множителя. Конец алгоритма.

Таким образом, мы здесь описали алгоритм разложения многочлена на множители над Z при условии, что мы знаем его корни в каком-то Q_p .

Литература

1. *Прасолов В.В.* Многочлены. Москва: МНЦМО 2003.
2. *Коблиц Н.* p -адические числа, p -адический анализ и дзета функции. М., 1982.
3. *Schikhof W.H.* Ultrametric calculus. An introduction to p -adic analysis. Cambridge University Press, 1984.
4. *Радына А.Я., Радына Я.В.* Элементарныя ўводзіны ў p -адычны анализ. Мн., 2006.

КОНЕЧНЫЕ ЭЛЕМЕНТЫ ДЛЯ ПРИБЛИЖЕНИЙ ПОЛЯ ЦЕНТРАЛЬНЫХ СИЛ И ВАЛЕНТНО-СИЛОВОГО ПОЛЯ

Е. А. Расюкевич

Для реализации механических моделей наноструктур с использованием конечных элементов в виде упругого отрезка и упругого угла, которые имитируют валентное и невалентное взаимодействие атомов [1], необходимо показать их соответствие моделям структурной химии и молекулярной спектроскопии. Это можно сделать, сравнив их матрицы жесткости и матрицы потенциальной энергии.

Сначала рассмотрим приближение поля центральных сил, понятие о котором возникает, если предположить, что вдоль отрезков, соединяющих атомы, направлены как силы, действующие между валентно связанными атомами так и остальными [2]. В качестве обобщенных координат используются изменения длин валентных и невалентных связей.

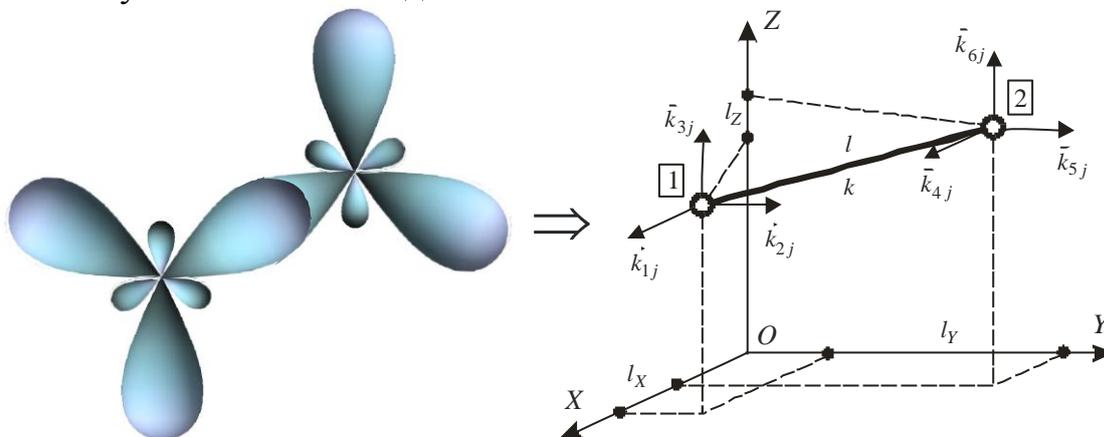


Рис. 1. Два атома и соответствующий упругий отрезок