

# Метод Диксона разложения целых чисел на множители с использованием метода сопряженных градиентов решения СЛАУ

Балахнин Сергей

## 1 Описание метода Диксона

Метод Диксона является обобщением метода факторизации Ферма:

Пусть  $n$  - нечетное число. Тогда можно найти такие  $s, t$ , что  $n = s^2 - t^2 = (s + t)(s - t)$

Теперь давайте искать  $s, t$ , такие что  $s^2 \equiv t^2 \pmod{n}$

тогда  $(s + t)(s - t) \equiv 0 \pmod{n} \Rightarrow \gcd(s + t, n); \gcd(s - t, n)$  являются делителями  $n$  и, если  $s \not\equiv \pm t \pmod{n}$ , то они являются не тривиальными делителями  $n$ . Опишем способ нахождения  $s$  и  $t$ :

Возьмем множество простых чисел  $B = \{p_1, \dots, p_h\}$  и будем случайно выбирать числа  $b$ . Назовем число  $b$   $B$ -гладким, если  $b^2 \pmod{n}$  является произведением простых чисел из  $B$ . Сделаем из  $B$ -гладких чисел и  $p_i$  числа  $s$  и  $t$ : Пусть  $b^2 \equiv p_1^{a_1} p_2^{a_2} \dots p_h^{a_h} \pmod{n}, a_1 \dots a_h \in \mathbb{N}$ .

Для каждого  $b$  определим  $\varepsilon = (a_1 \pmod{2}, a_2 \pmod{2}, \dots, a_h \pmod{2}) \in \mathbb{F}_2^h$  найдем такие  $b_1, b_2, \dots, b_l$ , что  $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_l = 0$ . При  $l \geq h + 1$  соответствующее множество  $\varepsilon_i$  точно найдется, так как это множество будет ЛЗ в поле  $\mathbb{F}_2^h$  (\*)

Рассмотрим  $b_i^2 = \prod_{j=1}^h p_j^{a_{ij}}$

определим  $\gamma_j = \frac{1}{2} \sum_{i=1}^l a_{ij}$  (так как для каждого  $p_j$  сумма  $a_j$  по всем  $b_{1..l}$  - четная, то  $\gamma_j \in \mathbb{N}$ ).

$$\left(\prod_{i=1}^l b_i\right)^2 = \prod_{j=1}^h p_j^{\sum_{i=1}^l a_{ij}} = \prod_{j=1}^h p_j^{2\gamma_j} = \left(\prod_{j=1}^h p_j^{\gamma_j}\right)^2$$

Соответственно  $s = \prod_{i=1}^l b_i \pmod{n}$ ,  $t = \left(\prod_{j=1}^h p_j^{\gamma_j}\right) \pmod{n}$  но эти  $s$  и  $t$  могут быть равны по модулю  $n$ , тогда они не помогут для решения задачи факторизации. Какова вероятность такого исхода? Пусть  $n$  является произведением степеней  $r$  различных простых чисел. Из китайской теоремы об остатках количество корней квадрата в  $\mathbb{Z}_n$  равно  $2^r$ , т.е.  $\text{prob}(s \equiv \pm t \pmod{n}) = \frac{2}{2^r}$ , при  $r \geq 2$ , то есть, если  $N$  составное число, то вероятность получить  $s \equiv \pm t \pmod{n}$  не больше  $\frac{1}{2}$ .

## 2 Метод сопряженных градиентов решения СЛАУ

Для поиска  $s$  необходимо было найти такое подмножество  $\{b_i\}, i = 1..h + 1$ , что соответствующая сумма  $\varepsilon_i$  была нулевой, то есть решить систему линейных уравнений на векторах  $\varepsilon$ . От выбора способа решения зависит скорость работы алгоритма.

Рассмотрим метод сопряженных градиентов решения СЛАУ Пусть дана система уравнений, записанная в матричном виде

$$Ax = \omega$$

$A$  - симметричная положительно определенная матрица.

Тогда решение этой СЛАУ совпадает с минимумом функционала

$$(Ax, x) - 2(\omega, x) - > \min$$

Итеративный алгоритм:

Подготовка

1. выберем начальное приближение  $x^0$
2.  $r^0 = \omega - Ax^0$
3.  $z^0 = r^0$

Описание k-ой итерации

1.  $a^k = \frac{(r^{k-1}, r^{k-1})}{(Az^{k-1}, z^{k-1})}$
2.  $x^k = x^{k-1} + a_k z^{k-1}$
3.  $r^k = r^{k-1} - a_k Az^{k-1}$
4.  $\beta^k = \frac{(r^k, r^k)}{(r^{k-1}, r^{k-1})}$
5.  $z^k = r^k + \beta_k z^{k-1}$

Однако в нашей задаче матрица не симметрична, а СЛАУ имеет вид  $Bx = u$ , где  $B$  - матрица  $h \times (h + 1)$ , причем матрица  $B$  разреженная получим матрицу  $A$  для данного метода следующим способом: Выберем конечное поле  $F$  с  $|F| \gg n$  и сгенерируем диагональную матрицу  $D$   $h \times h$  с элементами на диагонали, выбранными случайно из поля  $F \setminus \{0\}$

$$A = B^T D^2 B$$

$$\omega = B^T D^2 u$$

с высокой вероятностью решения изначального и преобразованного уравнений будут равны. В случае если это не так, нужно сгенерировать новую матрицу  $D$ . Также проблемой могут стать самоортогональные вектора, в поле  $F$ . Чтобы ее избежать обычно в качестве поля  $F$  выбирают поле  $GF(2^r)$  где  $r=19..21$ . При реализации данного метода в качестве оптимизации может использоваться хранение разреженной матрицы  $B$  как списка строк в которых есть ненулевые элементы.

### 3 Архитектура программы

Планируется разбить решение на 2 файла: класс разреженной матрицы, в которой будет реализован метод сопряженных векторов, а также основной файл с алгоритмом Диксона.

В основном файле будет создана функция `factorize`, которая в цикле выполняет следующие действия:

1. Создает список простых чисел
2. генерирует В-гладкие числа на основе простых
3. создает СЛАУ из векторов  $\varepsilon$  и решает ее используя класс `SparseMatrix`
4. получает числа  $s$  и  $t$  с помощью решения СЛАУ, проверяет, подходят ли они, заканчивает если да, возвращается к пункту один, если нет

### 4 Литература

1. Solving large sparse linear systems over finite fields. / LaMacchia, B. A.; Odlyzko, A. M. *Advances in Cryptology – CRYPTO 1990, Proceedings.* ed. / Alfred J. Menezes; Scott A. Vanstone. Springer Verlag, 1991. p. 109-133 (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 537 LNCS).
2. Joachim von zur Gathen, Jürgen Gerhard: *Modern Computer Algebra* (3. ed.). Cambridge University Press 2013, ISBN 978-1-107-03903-2.
3. Метод сопряжённых градиентов (для решения СЛАУ), Википедия