Московский Государственный Университет им. М.В.Ломоносова

Механико-математический факультет

Кафедра теории чисел

Курсовая работа

Алгоритм извлечения квадратного корня из числа в решете числового поля

(Algorithm of computing a square root for the number field sieve)

Выполнил:
студент 306 группы
Мирошниченко П.А.

Научный руководитель:
проф. Нестеренко Ю.В.

Москва, 2011 год

Введение

Рассмотрим полином $f \in \mathbf{Z}[\mathbf{x}]$ степени d, со взаимно простыми в совокупности коэффициентами.
Обозначим α - корень многочлена f.
Пусть S - некоторое множество пар целых чисел (a,b) и

$$\gamma = (f'(\alpha))^2 \prod_{(a,b)\in\mathbf{S}} (a + b\alpha),$$

будет квадратом в $Z[\alpha]$.

Нужно найти $\beta \in \mathbf{Z}[\alpha] : \beta^2 = \gamma$.
Алгоритм.
Дано: полином $f(x) \in \mathbf{Z}[\mathbf{x}]$, , со взаимно простыми в совокупности коэффициентами,
$\alpha : f(\alpha) = 0, \gamma \in \mathbf{Z}[\alpha], \deg f = d$.
Выход: $\beta \in \mathbf{Z}[\alpha] : \beta^2 = \gamma$.

1. Найти простое нечётное p такое, что $f(x) \mod p$ неприводим.
2. Найти δ_0 - решение сравнения $\gamma x^2 \equiv 1 \pmod p$.
   Если такого δ_0 нет, то γ - не квадрат.
3. Положить

$$\delta_j = \frac{\delta_{j-1}(3 - \delta_{j-1}^2\gamma)}{2} \mod p^{2^j}.$$

$$\delta_j = \sum_{j=1}^{k} b_j\alpha_j, \qquad |b_j| < \frac{p^{2^j}}{2}, \qquad j = 1, ..., j_0;$$

$$j_0 = 1 + [\log_2 \frac{\log_2(2d^{3/2}||f||^d(2u||f||)^{\#S/2})}{\log_2 p}].$$

   Где S - некоторое множество пар целых чисел (a, b),
   $\#S$ - мощность множества S, $u = \max(|a|, |b|)$ для всех пар из S,
   $||f|| = (\sum_{i=0}^{d} {c_i}^2)^{\frac{1}{2}}, c_i \in \mathbf{Z}$.
4. Проверить $\beta = \delta_{j_0}\gamma$. Если равенство выполняется, то выдать β.

§1. Как найти p?

Будем перебирать простые нечётные p, пока не окажется, что $f \mod p$ неприводим над $F_p[x]$. Обозначим $\overline{f} = f \mod p$, $\overline{f} \in \mathbf{F_p}[\mathbf{x}]$

Покажем следующий изоморфизм:

$$\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq F_p[x]/(\overline{f}),$$

Рассмотрим отображение $\psi : \mathbf{Z}[\alpha] \to F_p[x]/(f)$, $\delta \in \mathbf{Z}[\alpha]$.
Запишем δ в виде: $\delta = A(\alpha)$, где $a_i \in \mathbf{Z}$. $A(x) = \sum_{i=0}^{m} a_i x^i$. Определим многочлен $r(x)$ равенством, $\deg r < \deg f$ и положим $\psi(\delta) = \overline{r}(x) \in \mathbf{F_p}[\mathbf{x}]/(\overline{\mathbf{f}})$.

Проверим корректность, пусть $\delta = A(\alpha) = B(\alpha)$, тогда $A(x) - B(x) = 0$ в точке α, тогда $f(x)|A(x) - B(x)$, значит $B(x) = A(x) + f(x)w(x)$, где $w(x) \in \mathbf{Z}[\mathbf{x}]$, тем самым у $A(x)$ и $B(x)$ одинаковые остатки при делении на $f(x)$. Сюрьекция очевидна, поскольку любой элемент $\overline{r}(x)$

является образом некоторого элемента $r(x)$.

В тоже время гомоморфизм следует из того, что произведение остатков по модулю p равно остатку произведения, а сумма остатков - остатку суммы.

Пусть δ лежит в ядре, тогда $\overline{r}(x) = 0$, тогда $\overline{A} = A(x) \mod p$ делится на $\overline{f}(x)$, значит $\overline{A} = \overline{f}(x)\overline{u}(x)$, а $A(x) = f(x)u(x)+pv(x)$ и тогда $\delta = A(\alpha) = f(\alpha)u(\alpha)+pv(\alpha) = 0+pv(\alpha) = pv(\alpha)$.

Так как $F_p[x]/(\overline{f})$ - поле, то $(p) = p\mathbf{Z}[\alpha]$ - простой идеал в кольце $\mathbf{Z}[\alpha]$.

Утверждение 1. *Если f неприводим по модулю p, то $f'(\alpha) \notin (p)$.*

Доказательство. От противного. Пусть $f'(\alpha) \in (p)$.

Рассмотрим дискриминант многочлена f, он представим в следующем виде
$D_f = A(x)f(x) + B(x)f'(x)$, где A и B некоторые многочлены, и $\deg B < \deg f$. Поскольку α - корень f(x), то $D_f = B(\alpha)f'(\alpha)$, т.к. $f'(\alpha) \in (p)$, то и $D_f \in (p)$, следовательно $p|D_f$, чего быть не может, так как иначе, рассмотрев по модулю p, получим $\overline{A}(x)\overline{f}(x) = -\overline{B}(x)\overline{f}'(x)$, а так как f - неприводим, то либо $\overline{f}|\overline{B}$, либо $\overline{f}|\overline{f}'$, но этого быть не может, поскольку степени каждого из $B(x)$ и $f'(x)$ меньше степени $f(x)$, противоречие. □

§2. Как найти δ_0?

Пусть p - характеристика поля, $q = p^d$. Тогда для каждого ненулевого $s \in F_q$ $s^r = 1$ либо $s^r = -1$, где $r = \frac{q-1}{2}$, т.к. тогда $s^{\frac{q-1}{2}} = \pm 1$ и $s^{q-1} = 1$.
Будем говорить, что ненулевые элементы s_1 и s_2 в F_q различных типов, если $s_1^r \neq s_2^r$.

Лемма 2. *Пусть s_1 и s_2 неравные, ненулевые в F_q, тогда*

$$\#\{s \in F_q\} = r,$$

где $s_1 + s \neq 0, (s_1 + s)^r \neq (s_2 + s)^r, s_2 + s \neq 0$.

Доказательство. Если $s_i + s \neq 0$, тогда $(s_i + s)^r = 1$ либо $(s_i + s)^r = -1$, $i = 1, 2$. Поэтому, $0 \neq (s_1 + s)^r \neq (s_2 + s)^r \neq 0 \Longleftrightarrow (\frac{s_1+s}{s_2+s})^r = -1$.
Уравнение $x^r + 1 = 0$ имеет r различных корней в F_q и каждый корень t даёт уникальное $s \in F_q$, потому что при $t \neq 1 : s = \frac{s_1-ts_2}{t-1}$.

□

Мы показали, что $f'(\alpha) \notin (p)$. Кроме того, для любой пары $(a, b) \in \mathbf{S}$, $a + b\alpha \notin (p)$ при $(a, b) = 1$, а тогда и $\prod_{(a,b)\in\mathbf{S}}(a+b\alpha) \notin (p)$, т.е. и $\gamma = (f'(\alpha))^2 \prod_{(a,b)\in\mathbf{S}}(a+b\alpha) \notin (p)$, поэтому будем рассматривать коэффициенты γ по модулю p.

Поскольку, $p \nmid \gamma = \beta^2$, то $p \nmid \beta$, т.е. $\overline{\beta} \neq 0$, где $\overline{\beta} = \beta \mod p$ Обозначим $g(y) = \gamma y^2 - 1 \in \mathbf{F_p}$
Рассмотрим НОД $(g(y - s), y^r - 1)$
Пусть $k(y) =$ НОД $(g(y), (y + s)^r - 1)$, где $g(y) = (y - s_1)(y - s_2), s_1 = \frac{1}{\beta}, s_2 = -\frac{1}{\beta}$
Мы, хотим, чтобы $k(y) \neq 1$, а $(y - s_1)|k(y)$ или $(y - s_1)|k(y)$.
Это происходит тогда и только тогда, когда s_1 и s_2 различных типов. В противном случае, мы случайно выбираем $s \in \mathbf{F_p}$ и вместо $g(y) \to g(y - s)$.

По лемме при первом случайном выборе s, $s_1 + s$ и $s_2 + s$ - корни $g(y - s)$ различных типов с вероятностью $\frac{1}{2}$. При втором выборе - с вероятностью $\frac{3}{4}$, при третьем - с вероятностью $\frac{7}{8}$ и т.д.
Заметим, что $k(y)$ - нетривиальный, если s_1 - корень k(y), а s_2 - не корень $k(y)$.
Существует $r = \frac{p-1}{2}$ возможностей, что $\deg k(y) = 1$ с вероятностью $\frac{1}{2}$.
$\gamma y^2 \equiv 1(p)$. Обозначим данное y за δ_0. Этот δ_0 единственный с точностью до знака.

§3. **Построение последовательности δ_j.**

Теорема 3.

$$\delta_{j-1}^2\gamma - 1 \equiv 0 \pmod{p^{2^j}}, j \geq 1.$$

Где, начиная с δ_0, δ_j вычисляется итерациями Ньютона:

$$\delta_j = \frac{\delta_{j-1}(3 - \delta_{j-1}^2\gamma)}{2} \mod p^{2^j}.$$

Доказательство. Доказательство проведём индукцией по j. Для δ_0 это известно. Пусть теперь это верно для всех меньших j, тогда

$$\delta_j^2\gamma - 1 = \frac{\delta_{j-1}^2(9 - 6\delta_{j-1}^2\gamma + \delta_{j-1}^4\gamma^2) - 4}{4} = \frac{\gamma^3\delta_{j-1}^6 - 6\gamma^2\delta_{j-1}^4 + 9\gamma\delta_{j-1}^2 - 4}{4} =$$
$$= \frac{(\gamma\delta_{j-1}^2 - 1)(\gamma^2\delta_{j-1}^4 - 5\gamma\delta_{j-1}^2 + 4)}{4} = \frac{(\gamma\delta_{j-1}^2 - 1)^2(\gamma\delta_{j-1}^2 - 4)}{4}.$$

Из левой части видно, что это число целое, а из правой, что оно делится на $(p^{2^{j-1}})^2 = p^{2^j}$. □

Для $\beta = \sum_{i=0}^{d-1} b_i\alpha_i$ можно добиться, чтобы

$$|b_i| < \frac{p^{2^j}}{2}.$$

§4. **Оценка коэффициентов β.**

Предложение 4. *Пусть* $f = \sum_{i=0}^{d} c_i x^i$, $||f|| = (\sum_{i=0}^{d} {c_i}^2)^{\frac{1}{2}}$, *также пусть* $u = max(|a|, |b|)$ *для всех пар* $(a, b) \in \mathbf{S}$.
И пусть

$$\beta = b_0 + b_1\alpha + ... + b_{d-1}\alpha^{d-1},$$

удовлетворяет равенству $\beta^2 = \gamma$, *тогда*

$$|b_i| \leq d^{\frac{3}{2}} ||f||^{d-i} (2u||f||)^{\frac{\#S}{2}}, 0 \leq i \leq d-1.$$

Доказательство.

Лемма (неравенство Ландау) 5. *Пусть*

$$Q = \sum_{k=0}^{m} c_k x^k, z \in \mathbf{C},$$

тогда

$$||(x+z)Q(x)|| = ||(\overline{z}x+1)Q(x)||,$$

Доказательство. Пусть $c_{-1} = c_{m+1} = 0$, тогда левая часть:

$$||(x+z)Q(x)|| = \sqrt{\sum_{k=0}^{m}(zc_k + c_{k-1})^2} = \sqrt{\sum_{k=0}^{m}(zc_k + c_{k-1})(\overline{z}\overline{c}_k + \overline{c}_{k-1})} =$$
$$= \sqrt{|z|^2 \sum_{k=0}^{m+1} |c_k|^2 + \sum_{k=0}^{m+1} |c_{k-1}|^2 + \sum_{k=0}^{m}(\overline{z}\overline{c}_k\overline{c}_{k-1} + zc_k\overline{c}_{k-1})} =$$
$$= \sqrt{(|z|^2+1)||Q||^2 + \sum_{k=0}^{m}(\overline{z}\overline{c}_k\overline{c}_{k-1} + zc_k\overline{c}_{k-1})},$$

А правая часть

$$||(\overline{z}x+1)Q(x)|| = \sqrt{\sum_{k=0}^{m}(c_k + c_{k-1}\overline{z})^2} =$$
$$= \sqrt{\sum_{k=0}^{m}|c_k|^2 + \sum_{k=0}^{m}|c_{k-1}|^2|z|^2 + \sum_{k=0}^{m}(c_k\overline{c}_{k-1}z + \overline{c}_k\overline{c}_{k-1}\overline{z})},$$

откуда и следует их равенство. □

Теперь, пусть $\alpha^{(1)}, ..., \alpha^{(k)}$ - корни f(x): $|\alpha^{(i)}| > 1$, $i = 1, ..., k$.

Обозначим $R(x) = \prod_{j=1}^{k}(\overline{\alpha^{(j)}}x - 1)\prod_{j=k+1}^{d}(x - \alpha^{(j)}) = b_0x^d + ... + b_d$,
и пусть $f(x) = \prod_{j=1}^{k}(x - \alpha^{(j)})\prod_{j=k+1}^{d}(x - \alpha^{(j)})$.
Также пусть $Q(x) := \prod_{j=k+1}^{d}(x - \alpha^{(j)})$, применим лемму. Заметим, что на норму знаки влиять

не будут, и тогда $||R(x)|| = ||f(x)||$.
Теперь,

$$\prod_{j=1}^{d} \max(1, |\alpha^{(j)}|) = \prod_{j=1}^{k} |\alpha^{(j)}| = |b_0| \leq ||R|| = ||f||.$$

У многочлена f - d комплексных корней. Тогда

$$f = \prod_{i=1}^{d} (x - \alpha^{(i)}).$$

Пусть

$$\delta_0, \delta_1, \ldots, \delta_{d-1} \in \mathbf{K} : \quad \sum_{i=0}^{d-1} \delta_i x^i = \frac{f}{x - \alpha},$$

тогда

$$\delta_i = \sum_{j=0}^{d-1-i} c_{i+j+1} \alpha^{(j)}.$$

Из интерполяционной формулы Лагранжа

$$\sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \frac{f(x)}{x - \alpha^{(i)}} = x^{k+1}, k = 0, \ldots, d-2.$$

и

$$\sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \frac{f(x)}{x - \alpha^{(i)}} = x^d - f(x), k = d-1.$$

поскольку по d точкам $\alpha^{(1)}, \ldots, \alpha^{(d)}$ однозначно определяется многочлен степени $d-1$.
Значит,

$$x^{k+1} = \sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \frac{f(x)}{x - \alpha^{(i)}} = \sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \sum_{i=1}^{d} \delta_l^{(i)} x^l,$$

т.е.

$$x^{k+1} = \sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \delta_l^{(i)} = 0, l \neq k+1;$$

$$x^{k+1} = \sum_{i=1}^{d} \frac{(\alpha^{(i)})^{k+1}}{f'(\alpha^{(i)})} \delta_l^{(i)} = 1, l = k+1.$$

Откуда

$$Tr(\frac{\delta_i \beta}{f'(\alpha)}) = \sum_{k=0}^{d-1} b_k Tr(\frac{\alpha^k \delta_i}{f'(\alpha)}) = b_i.$$

Перепишем в следующем виде

$$b_i = \sum_{k=1}^{d} \frac{\delta_i^{(k)} \beta^{(k)}}{f'(\alpha^{(k)})}.$$

Заметим, что

$$\max(1, |\alpha^{(k)}|) \leq \prod_{j=1}^{d} \max(1, |\alpha^{(j)}|) \leq ||f||,$$

где первое неравенство очевидно, т.к. в произведении все множители не меньше единицы. А второе неравенство сразу следует из леммы о неравенстве Ландау.

Таким образом,

$$|\delta_i^{(k)}|^2 \le ||f||^2 \sum_{j=0}^{d-1-i} |\alpha^{(k)}|^{2j} \le d||f||^{(2d-2i-2)+2} = d||f||^{2(d-i)}, 0 \le i \le d-1,$$

где первое неравенство следует из неравенства Коши-Шварца, а второе из замеченного выше.

Кроме того,

$$|\frac{\beta^{(k)}}{f'(\alpha^{(k)})}|^2 = \prod_{(a,b)\in \mathbf{S}} |a + b\alpha^{(k)}| \le (2u||f||)^{\#S},$$

а тогда

$$|b_i| = |\sum_{k=1}^{d} \frac{\delta_i^{(k)}\beta^{(k)}}{f'(\alpha^{(k)})}| \le d^{3/2}||f||^{d-i}(2u||f||)^{\#S/2}.$$

□

§5. Завершение обоснования алгоритма.

Найдём j_0 - количество итераций Ньютона, необходимых для нахождения $\beta_{j_0} = \beta$. Итак, $\delta_j^2\gamma \equiv 1(p^{2^j}),\ \ \beta_j \equiv \delta_j\gamma(p^{2^j})$,

$$\beta_j^2 \equiv \delta_j^2\gamma^2 \pmod{p^{2^j}},\ \ \beta_j^2 \equiv \gamma \pmod{p^{2^j}}.$$

А необходимо $\beta : \beta^2 = \gamma$, поэтому

$$\beta^2 - \beta_j^2 \equiv 0 \pmod{p^{2^j}},\ \ (\beta - \beta_j)(\beta + \beta_j) \equiv 0 \pmod{p^{2^j}}.$$

Очевидно, что множитель p не может входить в обе скобки, иначе, рассмотрим их сумму, и получим, что $p|2\beta$, но p - нечётное простое, взаимно простое с β.

Итак, ровно одна скобка делится на p^{2^j}. А поскольку, $|\beta| < \frac{p^{2^j}}{2}$ и $|\beta_j| < \frac{p^{2^j}}{2}$, то

$$0 < |\beta + \beta_j| \le |\beta| + |\beta_j| < \frac{p^{2^j}}{2}.$$

Поэтому остаётся только одна возможность: $\beta \equiv \beta_j \pmod{p^{2^j}}$.

|коэффициент $(\beta - \beta_j)| \le d^{3/2}||f||^{d-i}(2u||f||)^{\#S/2} + \frac{p^{2^j}}{2} < p^{2^j}$.

$$2d^{3/2}||f||^{d-i}(2u||f||)^{\#S/2} < p^{2^j},$$

и тогда

$$\log_2 \log_p(2d^{3/2}||f||^{d-i}(2u||f||)^{\#S/2}) < j.$$

Поскольку эта оценка должна выполняться для каждого b_i, в том числе и для b_0, при котором она будет наибольшей, то в полученном неравенстве считаем, что $i = 0$, тем самым, j_0 - номер последней итерации Ньютона, находится как

$$j_0 = 1 + [\log_2 \frac{\log_2(2d^{3/2}||f||^d(2u||f||)^{\#S/2})}{\log_2 p}].$$

Отсюда следует, что $\beta = \beta_{j_0}$.

Список литературы

[1] Jean-Marc Couveignes, Computing a square root for the number field sieve, this volume.

[2] J. P. Buhler, H. W. Lenstra, Jr. and C. Pomerance, Factoring integers with the number field sieve, 1994

[3] P.J.Weinberger, L.P.Rothschild, Factoring polynomials over algebraic number fields, ACM Trans. Math. Software 2, 1976.