Механико-математический факультет
Кафедра диф. уравнений и системного анализа

Алгебраические уравнения в кольце вычетов

Чергинец Дмитрий Николаевич

Уравнения первой степени

Уравнение первой степени в кольце вычетов

$$ax \equiv b \pmod{n}, \tag{1}$$

$n \in \mathbb{N}$, $a, b \in \mathbb{Z}_n$. Необходимо найти $x \in \mathbb{Z}_n$, удовлетворяющие (1).

Предположим, что $\gcd(a, n) = 1$.

Тогда $\exists a^{-1} \in \mathbb{Z}_n$ и уравнение (1) имеет единственное в $\mathbb{Z}_n$ решение

$$x \equiv a^{-1} b \pmod{n}.$$

Необход. усл. разрешимости

Пусть теперь $\gcd(a, n) = d > 1$.

Предположим, что уравнение (1) имеет решение x, тогда найдется такое $z \in \mathbb{Z}$, что

$$ax = b + zn;$$

$$ax - zn = b.$$

Так как $ax - zn$ делится на d, то и b делится на d.

Theorem

Если (1) имеет решение, то b делится на d.

Достаточное усл. разрешимости

Предположим, что b делится на d.
Пусть $a = \tilde{a}d$, $b = \tilde{b}d$, $n = \tilde{n}d$.
Тогда $x \in \mathbb{Z}$ удовлетворяет сравнению

$$\tilde{a}dx \equiv \tilde{b}d \pmod{\tilde{n}d}$$

тогда и только тогда, когда

$$\tilde{a}x \equiv \tilde{b} \pmod{\tilde{n}}.$$

Причем $\gcd(\tilde{a}, \tilde{n}) = 1$. Поэтому

$$x \equiv \tilde{a}^{-1}\tilde{b} \pmod{\tilde{n}},$$

а уравнение (1) имеет d решений в $\mathbb{Z}_n$:

$$\tilde{a}^{-1}\tilde{b},\ \ \tilde{a}^{-1}\tilde{b} + \tilde{n},\ \ \tilde{a}^{-1}\tilde{b} + 2\tilde{n},\ \ldots,\ \tilde{a}^{-1}\tilde{b} + (d-1)\tilde{n}.$$

Линейное уравнение

Theorem

Уравнение (1) имеет решение тогда и только тогда, когда b делится на $d = \gcd(a, n)$.
При этом, если $d = 1$, то решение единственно и равно $a^{-1}b \in \mathbb{Z}_n$.
Если $d > 1$, то уравнение (1) имеет d решений:

$$\tilde{a}^{-1}\tilde{b} + k\tilde{n} \in \mathbb{Z}_n, \qquad k = 1, \ldots, d,$$

$\tilde{a} := a/d$, $\tilde{b} := b/d$, $\tilde{n} := n/d$, $\tilde{a}^{-1}$ – один из представителей класса вычетов $\tilde{a}^{-1} \in \mathbb{Z}_{\tilde{n}}$.

Китайская теорема об остатках

Theorem

Пусть $n_1, \ldots, n_k \in \mathbb{N}$, $\gcd(n_i, n_j) = 1$ *при* $i \neq j$, $b_1, \ldots, b_k \in \mathbb{Z}$. *Тогда система уравнений*

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \vdots \\ x \equiv b_k \pmod{n_k}, \end{cases} \tag{2}$$

имеет единственное в кольце $\mathbb{Z}_n$ *решение*

$$x_0 = \sum_{i=1}^{k} b_i N_i C_i,$$

где $n = n_1 \ldots n_k$, $N_i = \frac{n}{n_i}$, C_i *— обратный к* N_i *в* $\mathbb{Z}_{n_i}^*$.

Доказательство

x_0 определено корректно?

$$\gcd(n_i, n_j) = 1 \quad \Rightarrow \quad \gcd(n_i, N_i) = 1$$

$$\gcd(n_i, N_i) = 1 \quad \Rightarrow \quad \exists C_i = N_i^{-1} \pmod{n_i}.$$

x_0 является решением системы?

Для каждого j, $1 \leq j \leq k$, справедливо сравнение

$$x_0 = \sum_{i=1}^{k} b_i N_i C_i \equiv b_j N_j C_j \equiv b_j \pmod{n_j},$$

следовательно, x_0 — решение.

Доказательство

Докажем единственность решения.

Предположим, что существуют два решения системы

$$x_1, x_2 \in \mathbb{Z}_n.$$

Для сравнений справедливо следующее свойство

$$\begin{cases} x_1 \equiv x_2 \pmod{n_1}, \\ x_1 \equiv x_2 \pmod{n_2}, \\ \gcd(n_1, n_2) = 1; \end{cases} \Rightarrow \; x_1 \equiv x_2 \pmod{n_1 n_2}.$$

Применяя его $k-1$ раз, получаем $x_1 \equiv x_2 \pmod{n}$.

Идея алгоритма Гарнера

Формула, указанная в теореме, хороша, но есть более быстрый алгоритм.
Пусть $x_i \in \mathbb{Z}$, $0 \leq x_i < n_1 \dots n_i$, – решение системы, составленной из первых i уравнений:

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \vdots \\ x \equiv b_i \pmod{n_i}. \end{cases}$$

Методом математической индукции получим формулы для нахождения x_i.
При $i = 1$ имеем $x_1 := b_1 \pmod{n_1}$.

Идея алгоритма Гарнера

Пусть известно x_{i-1}, найдем x_i. Решение будем искать в виде

$$x_i = x_{i-1} + N_i y_i,$$

где $N_i = n_1 n_2 \dots n_{i-1}$.
За счет данного вида число x_i уже является решением $j = 1, \dots, i-1$ уравнения:

$$x_i \equiv x_{i-1} + N_i y_i \equiv x_{i-1} \equiv b_j \pmod{n_j}.$$

Число $y_i, 0 \leq y_i < n_i$, подберем таким образом, чтобы x_i удовлетворяло уравнению

$$x \equiv b_i \pmod{n_i}.$$

Идея алгоритма Гарнера

Подставив x_i в уравнение, получим

$$x_{i-1} + N_i y_i \equiv b_i \pmod{n_i};$$

$$N_i y_i \equiv (b_i - x_{i-1}) \pmod{n_i};$$

$$y_i := C_i(b_i - x_{i-1}) \pmod{n_i},$$

где $C_i := N_i^{-1} \pmod{n_i}$ вычисляется при помощи расширенного алгоритма Евклида.
Отметим, что найденное решение удовлетворяет неравенству

$$x_i = x_{i-1} + N_i y_i < N_i + N_i(n_i - 1) = N_{i+1}.$$

Алгоритм Гарнера

- **Вход:** $b_1, \ldots, b_k \in \mathbb{Z}$,
  $n_1, \ldots, n_k \in \mathbb{N}$ – взаимно простые.
- **Выход:** x, $0 \leq x < n_1 \ldots n_k$, – решение (2).
- 1. Задаем начальные значения переменных:
  $N := 1$,
  $x := b_1 \pmod{n_1}$.
- 2. Для $i := 2, \ldots, k$ последовательно вычисляем:
  $N := N n_{i-1}$,
  $C := N^{-1} \pmod{n_i}$,
  $y := C(b_i - x) \pmod{n_i}$,
  $x := Ny + x$.
- 3. Выдаем результат: x.

Мультипликативная группа $\mathbb{Z}_n^*$ кольца $\mathbb{Z}_n$

Definition

Мультипликативной группой кольца $\mathbb{Z}_n$ называется

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

В частности, если p – простое, то

$$\mathbb{Z}_p^* = \{a \mid 1 \leq a \leq p - 1\}.$$

Квадратичный вычет

Definition

Пусть задано натуральное нечетное число n, $a \in \mathbb{Z}_n^*$. Вычет a называется квадратичным вычетом по модулю n, если уравнение

$$x^2 \equiv a \pmod{n} \tag{3}$$

имеет решение. В противном случае a называется квадратичным невычетом по модулю n.
Множество всех вычетов обозначим через Q_n.
Множество квадратичных невычетов – через $\overline{Q}_n$.
Заметим, что $0 \notin Q_n$ и $0 \notin \overline{Q}_n$

Количество корней

Theorem

Пусть p нечетное простое, $a \in \mathbb{Z}_p^*$. Тогда
1) уравнение (3) имеет либо два корня, либо ни одного.

Пусть x_0 – корень уравнения $(3) \Rightarrow a \equiv x_0^2 \pmod{p}$.

$$(3) \quad \Leftrightarrow \quad (x - x_0)(x + x_0) \equiv 0 \pmod{p},$$

так как $\mathbb{Z}_p$ поле, то

$$(3) \quad \Leftrightarrow \quad x \equiv \pm x_0 \pmod{p}.$$

Если предположить, что $x_0 \equiv -x_0$, то получаем

$$2x_0 \equiv 0 \pmod{p} \Rightarrow x_0 \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p}.$$

Количество квадр. вычетов

Theorem

Пусть p нечетное простое, $a \in \mathbb{Z}_p^*$. Тогда
2) число p имеет $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов;

Каждый вычет $x_0 \in \mathbb{Z}_p^*$ является решением только одного уравнения (3) при $a = x_0^2$, группа $\mathbb{Z}_p^*$ содержит $p-1$ элемент, поэтому для $\frac{p-1}{2}$ вычетов $a \in \mathbb{Z}_p^*$ найдутся решения уравнения (3) и вычеты a будут квадратичными вычетами, а для остальных классов вычетов корней не найдется и они будут квадратичными невычетами.

Критерий квадр. вычета

Theorem

Пусть p нечетное простое, $a \in \mathbb{Z}_p^*$. Тогда
3) a является квадратичным вычетом тогда и только тогда, когда

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Пусть a квадратичный вычет и x_0 корень (3):

$$x_0^2 \equiv a \pmod{p} \quad \Rightarrow \quad x_0^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

по малой теореме Ферма получаем, что

$$x_0^{p-1} \equiv 1 \pmod{p} \quad \Rightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Доказательство

Каждый квадратичный вычет является корнем

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Всего квадратичных вычетов $(p-1)/2$.
И так как многочлен степени $(p-1)/2$ не может иметь более $(p-1)/2$ корней в $\mathbb{Z}_p$, то

$$a \quad - \text{кв. вычет} \quad \Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Критерий кв. невычета

Theorem

Пусть p нечетное простое, $a \in \mathbb{Z}_p^*$. Тогда
4) a является квадратичным невычетом в том и только том случае, когда $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Пусть a – квадратичный невычет. По малой теореме Ферма

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

так как вычет в первой скобке не равен нулю, то в связи с отсутствием делителей нуля

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Символ Лежандра

Definition

Символом Лежандра $\left(\frac{a}{p}\right)$, где p — нечетное простое, $a \in \mathbb{Z}$, называется функция

$$\left(\frac{a}{p}\right) := \begin{cases} -1, & \text{если } a \text{ квадр. невычет } p; \\ 0, & \text{если } p \mid a; \\ 1, & \text{если } a \text{ квадр. вычет } p. \end{cases}$$

Согласно предыдущей теореме символ Лежандра можно вычислять по формуле

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

Св-ва символа Лежандра

Из формулы $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$ следуют св-ва:

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
2. Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. Если $p \equiv 3 \pmod 4$, то $\left(\frac{-1}{p}\right) = -1$.
4. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, то есть

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{при } p \equiv \pm 1 \pmod 8; \\ -1, & \text{при } p \equiv \pm 3 \pmod 8. \end{cases}$$

Квадратичный закон взаимности Гаусса

Пусть p, q – нечетные простые числа. Тогда если $p \equiv 1 \pmod 4$ или $q \equiv 1 \pmod 4$, то уравнения

$$\begin{aligned} x^2 &\equiv p \pmod q, \\ x^2 &\equiv q \pmod p, \end{aligned}$$

разрешимы (и неразрешимы) одновременно. Если же $p \equiv q \equiv 3 \pmod 4$, то из уравнений

$$\begin{aligned} x^2 &\equiv p \pmod q, \\ x^2 &\equiv q \pmod p, \end{aligned}$$

разрешимо лишь одно.

Квадратичный закон взаимности Гаусса

В символах Лежандра данный закон выглядит следующим образом:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}.$$

Так как

$$\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = 1,$$

то

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Символ Якоби

Пусть n — нечетное, большее единицы число, разложение на простые множители которого имеет вид $n = p_1 p_2 \dots p_k$, где среди простых чисел p_i могут быть одинаковые.
Символом Якоби произвольного целого числа a называется число

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right),$$

где $\left(\frac{a}{p_i}\right)$ — символ Лежандра.
Будем считать, что $\left(\frac{a}{1}\right) := 1$.

Свойства символа Якоби

1. $\left(\frac{a}{n}\right) = 0 \Leftrightarrow \gcd(a, n) > 1$.
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
4. Если $a \equiv b \pmod{n}$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
5. $\left(\frac{1}{n}\right) = 1$.
6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
7. Если $\left(\frac{a}{n}\right) = -1$, то уравнение $x^2 \equiv a \pmod{n}$ не имеет решений. Но обратное не верно.

Свойства символа Якоби

8. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, то есть

$$\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{при } n \equiv \pm 1 \pmod 8; \\ -1, & \text{при } n \equiv \pm 3 \pmod 8. \end{cases}$$

9. Если $a, n \in \mathbb{N}$ – нечетные, тогда

$$\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2} \times \frac{n-1}{2}} \left(\frac{n}{a}\right).$$

10. Если $a = 2^s t$, $t, n \in \mathbb{N}$ – нечетные, то

$$\left(\frac{a}{n}\right) = \left(\frac{2^s}{n}\right)\left(\frac{t}{n}\right) = (-1)^{\frac{t-1}{2} \times \frac{n-1}{2}} \left(\frac{n \pmod t}{t}\right)\left(\frac{2^s}{n}\right).$$

Вычисление символа Якоби

Вход: a – целое, n - нечетное натуральное.
Выход: $\left(\frac{a}{n}\right)$ – символ Якоби.
0. Инициализация $J := 1$.
1. Если $n = 1$, то выдаем результат: J, конец алгоритма.
2. Если $a < 0$, то $a := -a$, $J = (-1)^{\frac{n-1}{2}} J$.
3. Если $n = 1$, то выдаем результат: J, конец алгоритма.
4. Если $a = 0$, выдаем результат: 0, конец алгоритма.
5. Методом пробных делений представляем число a в виде

$$a = 2^s t,$$

где t – нечетное.
6. Если s – нечетное и $n \equiv \pm 3 \pmod 8$, то $J := -J$.
7. Если $n \equiv 3 \pmod 4$ и $t \equiv 3 \pmod 4$, то $J := -J$.
8. Вычисляем $a := n \pmod t$, $n := t$, переходим к шагу 3.

Сложность алгоритма

В связи с тем, что на 8 шаге числа a, n уменьшаются, алгоритм закончит работу. Оценим количество операций. Пусть k – количество итераций в цикле алгоритма.

$$k < 2M, \qquad M := \max\{\langle a \rangle, \langle n \rangle\}.$$

Итого во алгоритм выполняет не более

$$f(a,n) < 1 + N + 5k < 12N = 12\max\{\langle a \rangle, \langle n \rangle\} =$$

$$= 12\max\{[\log_2 |a|] + 1, [\log_2 n] + 1\}$$

арифметических операций. Поэтому

$$T(N) = \max_{\langle a \rangle + \langle n \rangle \le N} f(a,n) = O(N).$$

Вычисление корня в случае простого модуля

В случае, когда $n = p \equiv 3 \pmod 4$, уравнение (3) имеет корни $\pm a^{(p+1)/4}$. Действительно,

$$\left(\pm a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a a^{(p-1)/2} \equiv a \pmod p.$$

Theorem

Пусть p нечетное простое, $p-1=2^s t$, t — нечетное, n — квадратичный невычет числа p, $b := n^t \pmod p$.

Тогда

1) b имеет порядок 2^s в мультипликативной группе $\mathbb{Z}_p^*$.

2) Решением уравнения

$$x^{2^s} \equiv 1 \pmod p$$

являются элементы подгруппы

$$< b >:= \{b, b^2, b^3, \ldots, b^{2^s} = 1\}.$$

Доказательство 1)

Элемент b порождает циклическую подгруппу

$$< b >:= \{b, b^2, \ldots, b^m = 1\},$$

здесь $b^i \neq 1$ при $i < m$.
Так как

$$b^{2^s} \equiv n^{p-1} \equiv 1 \,(\mathrm{mod}\, p),$$

то m делит 2^s. Поэтому $m = 2^{s_0}$, $0 \leq s_0 \leq s$.
Если предположить, что $s_0 < s$, то

$$-1 \equiv n^{\frac{p-1}{2}} \equiv b^{2^{s-1}} = (b^{2^{s_0}})^{2^{s-s_0-1}} \equiv 1^{2^{s-s_0-1}} \equiv 1 \,(\mathrm{mod}\, p).$$

Противоречие, поэтому порядок b равен 2^s.

Доказательство 2)

Непосредственной подстановкой в уравнение

$$x^{2^s} \equiv 1 \,(\mathrm{mod}\, p)$$

убеждаемся, что все элементы циклической группы

$$< b >:= \{b, b^2, \ldots, b^{2^s} = 1\}$$

являются корнями

$$(b^i)^{2^s} \equiv (b^{2^s})^i \equiv 1^i \equiv 1 \,(\mathrm{mod}\, p).$$

Всего корней у данного уравнения не более 2^s, поэтому все они имеют вид b^d, $1 \leq d \leq 2^s$.

Алгоритм Шенкса. Введение

На данный момент существуют лишь вероятностные полиномиальные алгоритмы вычисления квадратного корня в случае простого модуля. Рассмотрим алгоритм Шенкса, который является вероятностным, так как в нем методом перебора находится невычет по модулю p. Каждое второе число является невычетом, поэтому на практике данного алгоритма вполне достаточно, чтобы быстро вычислить квадратный корень по простому модулю.

Алгоритм Шенкса. Обоснование

Пусть $p-1=t2^s$, t – нечетное.
Справедливо равенство

$$\left(a^{\frac{t+1}{2}}\right)^2 = aa^t.$$

Откуда

$$a = \left(a^{\frac{t+1}{2}}\right)^2 a^{-t}.$$

Задача свелась к нахождению $\sqrt{a^{-t}}$.
Так как

$$\left(a^{-t}\right)^{2^s} \equiv \left(a^{p-1}\right)^{-1} \equiv 1 \,(\mathrm{mod}\, p),$$

то $a^{-t} \in < b >$.

Алгоритм Шенкса. Обоснование

$$a^{-t} \in < b > \quad \Rightarrow \quad \exists d(a^{-t} \equiv b^d \pmod p),$$

где

$$d = d_0 + d_1 2 + \cdots + d_{s-1} 2^{s-1}, \qquad d_i \in \{0, 1\}.$$

Найдем d_i.

$d_0 = 0$

$$a^{-t} \equiv b^d \pmod{p} \qquad \Rightarrow \qquad a^t b^d \equiv 1 \pmod{p}.$$

Так как

$$a^{\frac{p-1}{2}} \equiv a^{t2^{s-1}} \equiv 1 \pmod{p},$$

то

$$b^{d2^{s-1}} \equiv b^{d2^{s-1}} a^{t2^{s-1}} \equiv (a^t b^d)^{2^{s-1}} \equiv 1 \pmod{p}.$$

С другой стороны

$$b^{d2^{s-1}} = b^{d_0 2^{s-1}} \left(b^{2^s}\right)^{d_1 + d_2 2 + \cdots + d_{s-1} 2^{s-2}} \equiv b^{d_0 2^{s-1}} \pmod{p}$$

и $b^{2^{s-1}} \not\equiv 1 \pmod{p}$. Поэтому $d_0 = 0$.

d_i

Для $i := 1, \ldots, s-1$, последовательно находим d_i. Пусть $d_1, \ldots, d_{i-1}$ уже найдены, найдем d_i.

С одной стороны $\left(a^t b^d\right)^{2^{s-1-i}} \equiv 1 \pmod{p}$,

С другой стороны

$$\left(a^t b^d\right)^{2^{s-1-i}} \equiv \left(a^t b^{d_1 2 + \cdots + d_i 2^i}\right)^{2^{s-1-i}} \equiv$$

$$\equiv \left(a^t b^{d_1 2 + \cdots + d_{i-1} 2^{i-1}}\right)^{2^{s-1-i}} b^{d_i 2^{s-1}} \pmod{p}.$$

Поэтому, если

$$\left(a^t b^{d_1 2 + \cdots + d_{i-1} 2^{i-1}}\right)^{2^{s-1-i}} \equiv 1 \pmod{p},$$

то $d_i = 0$, иначе $d_i = 1$.

После того как все d_i будут найдены, получим

$$\sqrt{a^{-t}} \equiv b^{d/2} \pmod{p}.$$

Алгоритм Шенкса.

Вход: p – простое, a – квадратичный вычет по модулю p.
Выход: Корень уравнения $x^2 \equiv a \pmod{p}$.

1. Методом пробных делений на 2 находим такие $s, t \in \mathbb{N}$, t – нечетное, что $p - 1 = t2^s$.
2. Случайным образом выбираем невычет n числа p при помощи условия $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
3. Вычисляем $b := n^t \pmod{p}$, $r := a^{\frac{t+1}{2}} \pmod{p}$.
4. Задаем начальные значения параметров

$$d := 0, \qquad f := a^t \pmod{p}, \qquad \tilde{b} := b.$$

5. Для $i := 1, \ldots, s-1$, выполняем шаги 5.1, 5.2:
   5.1. Вычисляем $\tilde{b} := \tilde{b}^2 \pmod{p}$.
   5.2. Если $f^{2^{s-1-i}} \not\equiv 1 \pmod{p}$, то
   $d := d + 2^i$,
   $f := f\tilde{b} \pmod{p}$.
6. Выдаем результат $x := rb^{d/2} \pmod{p}$.

Сложность алгоритма

Количество итераций цикла не превосходит

$$s < \log_2 p.$$

на каждой итерации самая сложная операция это возведение в степень, которую можно выполнить за $O(\ln p)$ операций, поэтому

$$f(a, p) = O(\ln^2 p),$$

$$T(N) = O(N^2).$$

Случай составного модуля

Пусть $n = p_1 p_2 \dots p_k$,
p_i — простые нечетные числа, $p_i \neq p_j$,
a — квадратичный вычет по модулю n.
Тогда

$$x^2 \equiv a \pmod{n} \quad \Leftrightarrow \quad \begin{cases} x^2 \equiv a \pmod{p_1}, \\ x^2 \equiv a \pmod{p_2}, \\ \dots \\ x^2 \equiv a \pmod{p_k}. \end{cases}$$

Из чего следует, что

$$a \in Q_n \quad \Leftrightarrow \quad a \in Q_{p_1}, a \in Q_{p_2}, \dots, a \in Q_{p_k}.$$

Случай составного модуля

Уравнение (3) в случае

$$n = p_1 p_2 \dots p_k,$$

решается следующим образом.

1. Находятся корни $\pm x_i$ уравнения $x^2 \equiv a \pmod{p_i}$, $i = 1, 2, \dots, k$.
2. Решения уравнения (3) находятся при помощи Китайской теоремы об остатках из 2^k систем

$$\begin{aligned} x &\equiv \pm x_1 \pmod{p_1}, \\ x &\equiv \pm x_2 \pmod{p_2}, \\ &\dots, \\ x &\equiv \pm x_k \pmod{p_k}. \end{aligned}$$

Числа Блюма

Definition

Числом Блюма называется число

$$n = pq,$$

где p, q – различные простые числа,

$$p \equiv q \equiv 3 \pmod 4.$$

Модуль – число Блюма

Theorem

Пусть $n = pq$ – число Блюма, a — квадратичный вычет по модулю n.
Тогда уравнение (3) имеет четыре корня $x_1, x_2, x_3, x_4 \in \mathbb{Z}_n$, удовлетворяющие условиям:

- $$0 < x_1, x_2 \leq \frac{n-1}{2} < x_3, x_4 < n,$$
- $$\left(\frac{x_1}{n}\right) = \left(\frac{x_3}{n}\right) = 1, \qquad \left(\frac{x_2}{n}\right) = \left(\frac{x_4}{n}\right) = -1.$$
- $x_1 \in Q_n$, $x_2, x_3, x_4 \in \overline{Q}_n$.

Доказательство

a — квадратичный вычет числа n, т. е. уравнение $x^2 \equiv a \pmod{n}$ имеет решение, следовательно уравнения

$$x^2 \equiv a \pmod{p}, \qquad x^2 \equiv a \pmod{q},$$

также имеют решения $\pm x_p$, $\pm x_q$ соответственно. Так как

$$\gcd(a, p) = \gcd(a, q) = 1,$$

то

$$\gcd(\pm x_p, p) = \gcd(\pm x_q, q) = 1.$$

Доказательство

$$\left(\frac{x_p}{p}\right) = \left(\frac{-1(-x_p)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-x_p}{p}\right) =$$

$$= -\left(\frac{-x_p}{p}\right) \neq 0.$$

Поэтому среди корней $\pm x_p$ один вычет и один невычет. Пусть для определенности x_p и x_q квадратичные вычеты, а $-x_p$, $-x_q$ квадратичные невычеты по модулям p и q соответственно.

x_1

Через x_1 обозначим корень уравнения $x^2 \equiv a \pmod{n}$ такой, что

$$x_1 \equiv x_p \pmod{p}, \quad x_1 \equiv x_q \pmod{q},$$

Вычислим символ Якоби $x_1, -x_1$

$$\left(\frac{x_1}{n}\right) = \left(\frac{x_1}{p}\right)\left(\frac{x_1}{q}\right) = \left(\frac{x_p}{p}\right)\left(\frac{x_q}{q}\right) = 1 \times 1 = 1;$$

$$\left(\frac{-x_1}{n}\right) = \left(\frac{-x_p}{p}\right)\left(\frac{-x_q}{q}\right) = -1 \times (-1) = 1;$$

Через x_2 обозначим корень уравнения $x^2 \equiv a \pmod{n}$ такой, что

$$x_2 \equiv -x_p \pmod{p}, \quad x_2 \equiv x_q \pmod{q}.$$

Вычислим символы Якоби корней x_2, $-x_2$

$$\left(\frac{x_2}{n}\right) = \left(\frac{-x_p}{p}\right)\left(\frac{x_q}{q}\right) = -1 \times 1 = -1;$$

$$\left(\frac{-x_2}{n}\right) = \left(\frac{x_p}{p}\right)\left(\frac{-x_q}{q}\right) = 1 \times (-1) = -1.$$

$x_1 \in Q_n$

Для x_1

$$\left(\frac{x_1}{p}\right) = \left(\frac{x_1}{q}\right) = 1,$$

поэтому система

$$x^2 \equiv x_1 \pmod{p}, \qquad x^2 \equiv x_1 \pmod{q}$$

имеет решение, а значит, $x^2 \equiv x_1 \pmod{n}$ имеет решение и $x_1 \in Q_n$.

Остальные корни $-x_1$, $\pm x_2$ не являются квадратичными вычетами одновременно по модулям p, q, поэтому $-x_1$, $\pm x_2 \in \overline{Q}_n$.