Math-Net.Ru

Общероссийский математический портал

Д. В. Матюхин, Об асимптотической сложности дискретного логарифмирования в поле $GF(p)$, *Дискрет. матем.*, 2003, том 15, выпуск 1, 28–49

DOI: <https://doi.org/10.4213/dm184>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.207.199.55

26 апреля 2023 г., 17:00:08

Об асимптотической сложности дискретного логарифмирования в поле $GF(p)$

© 2003 г. Д. В. Матюхин

В работе приводится обоснование модификации алгоритма дискретного логарифмирования в поле $GF(p)$ (p — простое число), схема которой была описана автором ранее. Показано, что предложенная модификация дает наилучшую на сегодняшний день оценку сложности дискретного логарифмирования в конечном простом поле, которая совпадает с наилучшей известной оценкой сложности факторизации целых чисел, полученной Копперсмитом.

1. Введение

В работе изложен и обоснован алгоритм дискретного логарифмирования в поле $GF(p)$ (p — простое число), схема которого описана автором в [1]. При стандартных эвристических предположениях доказана анонсированная в [1] оценка сложности алгоритма, асимптотически при $p \rightarrow \infty$ равная

$$e^{(c+o(1))(\ln p)^{1/3}(\ln \ln p)^{2/3}}$$

двоичных операций, где

$$c = \left(\frac{92 + 26\sqrt{13}}{27} \right)^{1/3} \approx 1,902.$$

Указанная оценка является наилучшей известной на сегодняшний день оценкой сложности дискретного логарифмирования в конечном простом поле и совпадает с наилучшей известной оценкой сложности факторизации целых чисел, полученной Копперсмитом [2]. Предложенное для использования в алгоритме обобщение алгоритма построения степеней в числовых кольцах из [3] может быть использовано при теоретическом обосновании других вариантов метода решета числового поля для дискретного логарифмирования в конечных полях.

2. Вспомогательные результаты

2.1. Алгебраические числа

Пусть $n \in \mathbb{Z}_{>1}$,

$$f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X],$$

$f(X)$ — неприводимый многочлен, $\alpha \in \mathbb{C}$ — фиксированный корень $f(X)$, $K = \mathbb{Q}(\alpha)$ — числовое поле, полученное присоединением α к полю рациональных чисел, $\mathbb{K}$ — кольцо целых алгебраических чисел поля K . В ряде случаев разложение идеалов кольца $\mathbb{K}$, порожденных простыми числами, на простые идеалы определяется следующей теоремой (теорема 4.8.13 в [4]).

Теорема 1. Пусть q — простое число, $q \nmid [\mathbb{K} : \mathbb{Z}[\alpha]]$ и разложение $f(X)$ на неприводимые множители в $\mathbb{Z}/q\mathbb{Z}[X]$ имеет вид

$$f(X) \equiv \prod_{i=1}^m f_i(X)^{e_i} \pmod{q},$$

где $f_i(X)$ унитарны, $i = 1, \dots, m$. Тогда разложение идеала $q\mathbb{K}$ на простые идеалы имеет вид

$$q\mathbb{K} = \prod_{i=1}^m \mathfrak{q}_i^{e_i},$$

где $\mathfrak{q}_i = q\mathbb{K} + f_i(\alpha)\mathbb{K}$, $N_{K/\mathbb{Q}}(\mathfrak{q}_i) = q^{\deg f_i}$, $i = 1, \dots, m$.

Установить, является ли q делителем индекса $[\mathbb{K} : \mathbb{Z}[\alpha]]$, позволяют следующие утверждения.

Лемма 1. Справедливо равенство

$$\text{disc } f = [\mathbb{K} : \mathbb{Z}[\alpha]]^2 \text{disc } K.$$

Следующая лемма известна как критерий Дедекинда (см. гл. 15, §3 в [5]).

Лемма 2. В обозначениях теоремы 1 справедливо следующее утверждение: q делит индекс $[\mathbb{K} : \mathbb{Z}[\alpha]]$ тогда и только тогда, когда существует j , для которого $e_j > 1$ и $f_j(X)$ делит $q^{-1}(f(X) - \prod_{i=1}^m f_i(X)^{e_i})$ в $\mathbb{Z}/q\mathbb{Z}[X]$.

Следуя [6], назовем идеал $\mathfrak{q} \subset \mathbb{K}$ хорошим, если

$$\gcd(N_{K/\mathbb{Q}}(\mathfrak{q}), [\mathbb{K} : \mathbb{Z}[\alpha]]) = 1.$$

Из теоремы 2 вытекает следующая лемма.

Лемма 3. Хорошие простые идеалы первой степени кольца $\mathbb{K}$ есть в точности идеалы вида

$$\mathfrak{q} = q\mathbb{K} + (\alpha - r_q)\mathbb{K},$$

где q — простое число, $q \nmid [\mathbb{K} : \mathbb{Z}[\alpha]]$, r_q — корень многочлена $g \pmod{q}$, то есть эти идеалы однозначно определяются парами (q, r_q) . При этом $N_{K/\mathbb{Q}}(\mathfrak{q}) = q$.

Непосредственно проверяется следующее утверждение.

Лемма 4. Для любых $c, d \in \mathbf{Z}$

$$N_{K/\mathbf{Q}}(c + d\alpha) = (-d)^n f(-c/d) = c^n + \sum_{i=0}^{n-1} a_i c^i (-d)^{n-i}.$$

Следующая лемма есть предложение 2 из [6].

Лемма 5. Пусть c и d — взаимно простые целые числа такие, что $|N_{K/\mathbf{Q}}(c + d\alpha)|$ взаимно просто с $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ и его разложение на простые множители имеет вид

$$N_{K/\mathbf{Q}}(c + d\alpha) = \prod_{k=1}^m q_k^{e_k}.$$

Тогда имеет место разложение

$$(c + d\alpha)\mathcal{O}_K = \prod_{k=1}^m \mathfrak{q}_k^{e_k},$$

где $\mathfrak{q}_k = q_k\mathcal{O}_K + (\alpha + (cd^{-1} \bmod q_k))\mathcal{O}_K$, $k = 1, \dots, m$, суть хорошие простые идеалы кольца $\mathcal{O}_K$.

2.2. Гладкость

Пусть $y > 0$. Как известно, целое число называется y -гладким, если оно не имеет простых делителей, больших y . Мы будем использовать стандартное обозначение

$$L_p[s, c] = e^{(c+o(1))(\ln p)^s (\ln \ln p)^{1-s}},$$

где $o(1) \rightarrow 0$ при $p \rightarrow \infty$.

Лемма 6 ([3]). Если $x = L_p[s, c]$, $y = L_p[s', c']$, где $s, s', c, c' > 0$, то доля y -гладких чисел в множестве $\{1, \dots, x\}$ равна $L_p[s - s', (s' - s)c/c']$.

В приводимом ниже алгоритме дискретного логарифмирования некоторые шаги заключаются в поиске точек конечного множества $M \subset \mathbf{Z}^2$, в которых значения заданной однородной формы $f \in \mathbf{Z}[X, Y]$ являются B -гладкими для некоторого фиксированного B . В этом случае, чтобы воспользоваться леммой 6, мы примем стандартное эвристическое допущение о том, что доля таких точек в M совпадает с долей B -гладких чисел в множестве $\{1, \dots, \max_M |f(X, Y)|\}$.

Указанный поиск может осуществляться методом решета (см., например, [3]) или путем тестирования значений f на гладкость методом эллиптических кривых [7].

Лемма 7 ([3]). Пусть $f \in \mathbf{Z}[X, Y]$ — однородная форма степени n , $B, C > 0$. Тогда трудоемкость поиска B -гладких значений f на множестве

$$M = \{1, \dots, C\} \times \{-C, \dots, C\}$$

методом решета составляет

$$\pi(B)(n + \ln B)^{O(1)} + O(C^2 \ln \ln B)$$

арифметических операций над числами, по абсолютной величине не превосходящими $\max_M |f(X, Y)|$, причем первое слагаемое включает в себя трудоемкость поиска корней многочлена $f(X, 1)$ по модулю простых чисел, не превосходящих B .

Оценка сложности метода эллиптических кривых основана на некотором эвристическом допущении; и поэтому формулируется в виде гипотезы (см. гипотезу 2.10 в [7]), которую, следуя [6], мы сформулируем в частном случае.

Гипотеза 1. Проверка числа N на $L_p[s, c]$ -гладкость с помощью метода эллиптических кривых требует в среднем не более $L_p[s/2, \sqrt{2sc}]$ операций на эллиптических кривых над кольцами вычетов по модулям, не превосходящим N . Эта оценка включает трудоемкость разложения $L_p[s, c]$ -гладкого N на простые множители.

2.3. Построение степеней в числовом кольце

В большинстве известных вариантов метода решета числового поля для дискретного логарифмирования в конечных полях искомый логарифм сначала вычисляется по модулю примарных делителей порядка мультипликативной группы поля и затем находится по китайской теореме об остатках. На практике метод применяется только к простым делителям, однако получение асимптотических оценок сложности алгоритмов требует его применения ко всем примарным делителям. При этом используются частные случаи следующей общей задачи.

Пусть K — числовое поле, S — некоторое подмножество поля K (или множества идеалов кольца K), l — простое число, $e \in \mathbb{N}$. Обозначим через K_{S, l^e} множество элементов $\gamma \in K$ таких, что γ (соответственно γ_K) разлагается в произведение элементов (идеалов) из S и l^e -й степени элемента (идеала) кольца K .

Дано: $K, K_i, i = 0, \dots, N$ — числовые поля, K, K_i — соответствующие кольца целых алгебраических чисел, γ, γ_i — порядки полей K и K_i соответственно, l — простое число, $e \in \mathbb{N}$, S, S_i — конечные множества элементов или идеалов колец K и K_i соответственно, M_i — конечные подмножества $(\cap K_{S, l^e}) \times (\cap K_{i; S_i, l^e})$,

$$m^{(0,0)} \in \cap K_{S, l^e}, \quad m_0^{(0)} \in 0 \cap K_{0; S_0, l^e}.$$

Найти: Отображение

$$y: \bigcup_{i=0}^N M_i \rightarrow \{0, \dots, l^e - 1\}$$

такое, что числа

$$\begin{aligned} \gamma &= m^{(0,0)} \prod_{i=0}^N \prod_{(m, m_i) \in M_i} m^{y(m, m_i)}, \\ \gamma_0 &= m_0^{(0)} \prod_{(m, m_0) \in M_0} m_0^{y(m, m_0)}, \\ \gamma_i &= \prod_{(m, m_i) \in M_i} m_i^{y(m, m_i)}, \quad i = 1, \dots, N, \end{aligned}$$

являются l^e -ми степенями соответственно в $K, K_i, i = 0, \dots, N$.

Данная задача является обобщением задачи 3.1 в [3], и для ее решения мы используем тот же математический аппарат, который опишем на примере поля K и кольца $\mathbb{O}$.

Пусть l не ветвится в K . Это условие равносильно условию $l \nmid \text{disc } K$, которое на практике может быть проверено с помощью леммы 1. Положим

$$\Gamma_1 = \{\gamma \in \mathbb{O} : l \nmid N_{K/\mathbb{Q}}(\gamma)\}, \\ \varepsilon = \text{lcm}\{ |(\mathbb{O}/l)^*| \},$$

где наименьшее общее кратное lcm берется по простым идеалам $\mathfrak{l} \subset \mathbb{O}$, $\mathfrak{l} \ni l$.

Решение сформулированной выше задачи, как и задачи 3.1 в [3], основано на следующей лемме (см. предложение 3.8 в [3]).

Лемма 8. Пусть $e \in \mathbb{N}$, U — группа единиц кольца $\mathbb{O}_K$,

$$U_{e+1} = \{u \in U : u \equiv 1 \pmod{l^{e+1}}\}.$$

Предположим, что l не делит число классов поля K и $U_{e+1} \subset U^{l^e}$. Пусть $\gamma \in \Gamma_1$ удовлетворяет условиям

$$(1) \quad v_{\mathfrak{p}}(\gamma) \equiv 0 \pmod{l^e} \text{ для всех простых идеалов } \mathfrak{p} \subset \mathbb{O}_K,$$

$$(2) \quad \gamma^e \equiv 1 \pmod{l^{e+1}}.$$

Тогда γ — l^e -я степень в $\mathbb{O}_K$.

Возможность практического применения леммы основана на некоторых эвристических предположениях, высказанных в работах [3, 8]. Сформулируем эти предположения в виде единой гипотезы.

Гипотеза 2. При случайном выборе поля K вероятность того, что l не делит число классов поля K и $U_{e+1} \subset U^{l^e}$, есть $1 - \varepsilon(l)$, где $\varepsilon(l) = O(1/l)$.

Для практического применения леммы 8 определим по индукции следующие множества и отображения. Положим

$$\lambda_1 : \Gamma_1 \rightarrow l\mathbb{O}/l^2\mathbb{O}, \quad \lambda_1(\gamma) = (\gamma^e - 1) + l^2\mathbb{O}.$$

Далее, если для $r > 1$ определены множество Γ_{r-1} и отображение λ_{r-1} , то определим

$$\Gamma_r = \{\gamma \in \Gamma_{r-1} : \lambda_{r-1}(\gamma) = 0\}, \\ \lambda_r : \Gamma_r \rightarrow l^{2^{r-1}}\mathbb{O}/l^{2^r}\mathbb{O}, \quad \lambda_r(\gamma) = (\gamma^e - 1) + l^{2^r}\mathbb{O}.$$

Для практического вычисления значений отображений λ_r воспользуемся тем фактом, что если $\mathbb{O}$ является $\mathbf{Z}$ -модулем с базисом $\{b_j\}_{j=1, \dots, n}$, то $l^{2^{r-1}}\mathbb{O}/l^{2^r}\mathbb{O}$ является $\mathbf{Z}/l^{2^{r-1}}\mathbf{Z}$ -модулем с базисом $\{b_j l^{2^{r-1}} + l^{2^r}\mathbb{O}\}_{j=1, \dots, n}$. Поэтому λ_r задается отображениями $\lambda_{r,j} : \Gamma_r \rightarrow \mathbf{Z}/l^{2^{r-1}}\mathbf{Z}$, определенными равенством

$$\gamma^e - 1 \equiv \sum_{j=1}^n \lambda_{r,j}(\gamma) b_j l^{2^{r-1}} \pmod{l^{2^r}}.$$

Пусть $\sigma \in \mathbb{N}$ удовлетворяет неравенствам $2^\sigma > e \geq 2^{\sigma-1}$. Положим n равным 0, если $S \subset K$ и степени поля K над $\mathbf{Q}$ в остальных случаях. Аналогично определим

$n_i, i = 0, \dots, N$. Обозначим $\varepsilon^{(i)}, \Gamma_r^{(i)}, \lambda_r^{(i)}$ число ε , множество Γ_r и отображение λ_r , соответствующие K_i и i . Предположим, что хотя бы одно из чисел n, n_i не равно 0. Предположим также, что если $n \neq 0$ ($n_i \neq 0$), то

$$m^{(0,0)}, m \in \Gamma_1 \quad (\text{соответственно } m_i \in \Gamma_1^{(i)} \text{ и } m_0^{(0)} \in \Gamma_1^{(0)} \text{ при } i = 0) \quad (1)$$

для всех элементов $(m, m_i) \in M_i$. Пусть также выполнены неравенства

$$|M_i| \geq |S_i| + n_i, \quad i = 0, \dots, N, \quad (2)$$

$$\sum_{i=0}^N |M_i| \geq |S| + \sigma n + \sum_{i=0}^N (|S_i| + \sigma n_i). \quad (3)$$

Тогда алгоритм решения сформулированной выше задачи выглядит следующим образом.

1. Для $i = 0, \dots, N$ и для $(m, m_i) \in M_i$ справедливы равенства

$$\mathcal{M} = \prod_{p \in S} p^{e_p} \mathcal{D}^{l^e}, \quad \mathcal{M}_i = \prod_{p_i \in S_i} p_i^{e_{p_i}} \mathcal{D}_i^{l_i^e}$$

для некоторых $e_p, e_{p_i} \in \mathbb{Z}_{\geq 0}$, где $\mathcal{M} = m$ и $\mathcal{D}$ — некоторый элемент кольца $\mathcal{K}$ при $S \subset K$; $\mathcal{M} = m_{\mathcal{K}}$, $\mathcal{D}$ — некоторый идеал кольца $\mathcal{K}$ в противном случае; смысл обозначений $\mathcal{M}_i, \mathcal{D}_i$ аналогичен. Положим

$$v_{(m, m_i)} = \left(\underbrace{\dots, e_p, \dots, \lambda_{1,1}(m), \dots, \lambda_{1,n}(m)}_{p \in S}, \underbrace{0, \dots, 0}_{\sum_{j=0}^{i-1} (|S_j| + n_j)}, \right. \\ \left. \underbrace{\dots, e_{p_i}, \dots, \lambda_{1,1}^{(i)}(m_i), \dots, \lambda_{1,n_i}^{(i)}(m_i)}_{p_i \in S_i}, \underbrace{0, \dots, 0}_{\sum_{j=i+1}^N (|S_j| + n_j)} \right)^T.$$

Если n или n_i равно 0, то отображения λ_r (соответственно $\lambda_r^{(i)}$) не определены, но для удобства изложения мы будем использовать формальные записи вида $\lambda_{r,1}(\cdot), \dots, \lambda_{r,n}(\cdot)$ (соответственно $\lambda_{r,1}^{(i)}(\cdot), \dots, \lambda_{r,n_i}^{(i)}(\cdot)$), обозначающие пустые последовательности. Знак T означает транспонирование. Аналогично определим $v_{(m^{(0,0)}, m_0^{(0)})}$. Эти векторы имеют размерность $|S| + n + \sum_{i=0}^N (|S_i| + n_i)$.

2. Для $i = 0, \dots, N$ выберем какие-либо подмножества $M_{i,1} \subseteq M_i$, удовлетворяющие условиям

$$|M_{i,1}| \geq |S_i| + n_i, \\ \sum_{i=0}^N |M_{i,1}| = \sum_{i=0}^N |M_i| - (\sigma - 1) \left(n + \sum_{i=0}^N n_i \right). \quad (4)$$

Это можно сделать благодаря неравенствам (2) и (3). Введем обозначение

$$M_i \setminus M_{i,1} = \{(m^{(i,k)}, m_i^{(k)})\}_{k=1, \dots, c_{1,i}}.$$

Пусть A и V — матрицы, столбцами которых являются соответственно векторы $v_{(m, m_i)}$ для $(m, m_i) \in M_{i,1}$, $i = 0, \dots, N$ и $v_{(m^{(i,k)}, m_i^{(k)})}$ для $i = 0, \dots, N$, $k = \text{sign } i, \dots, c_{1,i}$. Найдем какое-нибудь решение матричного уравнения

$$AX \equiv -V \pmod{l^e}. \quad (5)$$

Если решение не найдено, возвращаемся в начало данного шага и делаем другой выбор множеств $M_{i,1}$.

3. Пусть $w_{i,k}$ — столбец решения, отвечающий столбцу $v_{(m^{(i,k)}, m_i^{(k)})}$ матрицы V , $w_{i,k}(m, m_j)$ — его компонента, отвечающая столбцу $v_{(m, m_j)}$ матрицы A . Если

$$\sum_{i=0}^N c_{1,i} = 0$$

то есть $\sigma = 1$, $M_{i,1} = M_i$, $i = 0, \dots, N$, то для $i = 0, \dots, N$ и для $(m, m_i) \in M_i$ положим

$$y(m, m_i) = w_{0,0}(m, m_i),$$

и алгоритм заканчивает работу.

Если

$$\sum_{i=0}^N c_{1,i} > 0,$$

то для $i = 0, \dots, N$, $k = \text{sign } i, \dots, c_{1,i}$ положим $y_{i,k,1} = w_{i,k}$, и введем обозначения

$$b_{i,k,1} = m^{(i,k)} \prod_{j=0}^N \prod_{(m, m_j) \in M_{j,1}} m^{y_{i,k,1}(m, m_j)}, \quad (6)$$

$$b_{i,k,1,i} = m_i^{(k)} \prod_{(m, m_i) \in M_{i,1}} m_i^{y_{i,k,1}(m, m_i)}, \quad (7)$$

$$b_{i,k,1,j} = \prod_{(m, m_j) \in M_{j,1}} m_j^{y_{i,k,1}(m, m_j)}, \quad j = 0, \dots, N, \quad j \neq i, \quad (8)$$

и для $r = 2, \dots, \sigma$ выполним следующие действия.

Пусть для $i, j = 0, \dots, N$ определены значение $c_{r-1,i} \in \mathbb{Z}$, множество $M_{j,r-1}$ и для $k = \text{sign } i, \dots, c_{r-1,i}$ определены значения $b_{i,k,r-1} \in \mathbb{O}$, $b_{i,k,r-1,j} \in \mathbb{O}_j$ и отображения

$$y_{i,k,r-1} : \bigcup_{j=0}^N M_{j,r-1} \rightarrow \{0, 1, \dots, l^e - 1\}$$

такие, что

$$b_{i,k,r-1} = \delta_{i,k,r-1}^{l^e} m^{(i,k)} \prod_{j=0}^N \prod_{(m, m_j) \in M_{j,r-1}} m^{y_{i,k,r-1}(m, m_j)}, \quad (9)$$

$$b_{i,k,r-1,i} = \delta_{i,k,r-1,i}^{l^e} m_i^{(k)} \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{i,k,r-1}(m, m_i)}, \quad (10)$$

$$b_{i,k,r-1,j} = \delta_{i,k,r-1,j}^{l^e} \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{i,k,r-1}(m, m_j)}, \quad j = 0, \dots, N, \quad j \neq i, \quad (11)$$

для некоторых $\delta_{i,k,r-1} \in \dots$, $\delta_{i,k,r-1,j} \in \dots_j$. Для $i = 0, 1, \dots, N$ определим $c_{r,i} \in \mathbb{Z}$ так, что

$$0 \leq c_{r,i} \leq c_{r-1,i}, \quad \sum_{i=0}^N c_{r,i} = \sum_{i=0}^N c_{r-1,i} - \left(n + \sum_{i=0}^N n_i \right).$$

Для $i = 0, 1, \dots, N$, $k = \text{sign } i, \dots, c_{r-1,i}$ положим

$$v_{i,k,r} = (\lambda_{r,1}(b_{i,k,r-1}), \dots, \lambda_{r,n}(b_{i,k,r-1}), \lambda_{r,1}^{(0)}(b_{i,k,r-1,0}), \dots, \lambda_{r,n_0}^{(0)}(b_{i,k,r-1,0}), \dots, \lambda_{r,1}^{(N)}(b_{i,k,r-1,N}), \lambda_{r,n_N}^{(N)}(b_{i,k,r-1,N}))^T.$$

Пусть A_r и V_r — матрицы, столбцами которых являются векторы $v_{i,k,r}$ соответственно для $i = 0, 1, \dots, N$, $k = c_{r,i} + 1, \dots, c_{r-1,i}$ и $i = 0, 1, \dots, N$, $k = \text{sign } i, \dots, c_{r,i}$. Найдем какое-нибудь решение матричного уравнения

$$A_r X \equiv -V_r \pmod{l^{2^{r-1}}}. \quad (12)$$

Если решение не найдено, перенумеровываем пары $(m^{(i,k)}, m_i^{(k)})$, $i = 0, 1, \dots, N$, $k = 1, \dots, c_{r-1,i}$ (соответственно перенумеруются отображения $y_{i,k,r-1}$, числа $b_{i,k,r-1}$, $b_{i,k,r,j}$, $j = 0, \dots, N$, векторы $v_{i,k,r}$, изменятся матрицы A_r и V_r) и решаем уравнение с новыми матрицами A_r и V_r . Пусть $w_{i,k,r}$ — столбец решения, отвечающий столбцу $v_{i,k,r}$ матрицы V_r , $w_{i,k,r}(s, t)$ — его компонента, отвечающая столбцу $v_{s,t,r}$ матрицы A_r . Для $i, j = 0, 1, \dots, N$, $k = \text{sign } i, \dots, c_{r,i}$ положим

$$b_{i,k,r} = b_{i,k,r-1} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} b_{s,t,r-1}^{w_{i,k,r}(s,t)},$$

$$b_{i,k,r,j} = b_{i,k,r-1,j} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} b_{s,t,r-1,j}^{w_{i,k,r}(s,t)}.$$

Для $(m, m_j) \in M_{j,r-1}$ положим

$$y_{i,k,r}(m, m_j) \equiv y_{i,k,r-1}(m, m_j) + \sum_{s=0}^N \sum_{t=c_{r,s}+1}^{c_{r-1,s}} y_{s,t,r-1}(m, m_j) w_{i,k,r}(s, t) \pmod{l^e},$$

для $q = c_{r,j} + 1, \dots, c_{r-1,j}$ положим

$$y_{i,k,r}(m_j^{(q)}, m^{(j,q)}) = w_{i,k,r}(j, q),$$

$$M_{j,r} = M_{j,r-1} \cup \{(m_j^{(q)}, m^{(j,q)})\}_{q=c_{r,j}+1, \dots, c_{r-1,j}}.$$

По завершении цикла по r , полагая $y = y_{0,0,\sigma}$, получаем искомое отображение.

Лемма 9. Если при $n > 0$ ($n_i > 0$) для чисел l , e и поля K (соответственно K_i) выполнены условия леммы 8, то найденное в результате работы алгоритма отображение y является решением сформулированной выше задачи.

Доказательство. Вначале докажем индукцией по r для $i, j = 0, 1, \dots, N$ и $k = \text{sign } i, \dots, c_{r,i}$ равенства (9)–(11) с заменой $r - 1$ на r и равенства

$$\mathfrak{B}_{i,k,r} = \mathfrak{D}_{i,k,r}^{l^r}, \quad (13)$$

где $\mathfrak{B}_{i,k,r} = b_{i,k,r}$, $\mathfrak{D}_{i,k,r}$ — некоторый элемент кольца $\mathbb{O}_K$ при $S \subset K$, и $\mathfrak{B}_{i,k,r} = b_{i,k,r} \mathbb{O}_K$, $\mathfrak{D}_{i,k,r}$ — некоторый идеал кольца $\mathbb{O}_K$ в противном случае. Также покажем, что

$$\lambda_r(b_{i,k,r}) = 0 \quad (14)$$

при $S \not\subset K$ и

$$\mathfrak{B}_{i,k,r,j} = \mathfrak{D}_{i,k,r,j}^{l^r}, \quad (15)$$

где $\mathfrak{B}_{i,k,r,j} = b_{i,k,r,j}$, $\mathfrak{D}_{i,k,r,j}$ — некоторый элемент кольца $\mathbb{O}_{K_j}$ при $S_j \subset K_j$, и $\mathfrak{B}_{i,k,r,j} = b_{i,k,r,j} \mathbb{O}_{K_j}$, $\mathfrak{D}_{i,k,r,j}$ — некоторый идеал кольца $\mathbb{O}_{K_j}$ в противном случае, а также

$$\lambda_r^{(j)}(b_{i,k,r,j}) = 0 \quad (16)$$

при $S_j \not\subset K_j$ и

$$\sum_{i=0}^N |M_{i,r}| = \sum_{i=0}^N |M_i| - (\sigma - r) \left(n + \sum_{i=0}^N n_i \right). \quad (17)$$

Пусть $r = 1$. Тогда равенства (9)–(11) есть в точности равенства (6)–(8). Равенства (13), (15) следуют из (6)–(8) и уравнений в (5), отвечающих соответственно $p \in S$, S_j и столбцу $v_{(m^{(i,k)}, m_i^{(k)})}$. По построению $b_{i,k,1} \in \Gamma_1$, $b_{i,k,1,j} \in \Gamma_1^{(j)}$, поэтому значения $\lambda_1(b_{i,k,1})$, $\lambda_1^{(j)}(b_{i,k,1,j})$ определены и равенства (14) и (16) следуют из уравнений в (5), отвечающих соответственно $\lambda_{1,1}, \dots, \lambda_{1,n}$ и $\lambda_{1,1}^{(j)}, \dots, \lambda_{1,n_j}^{(j)}$ и столбцу $v_{(m^{(i,k)}, m_i^{(k)})}$. Равенство (17) есть в точности (4).

Пусть $r > 1$. Докажем, что (9), (10), (11) остаются справедливыми при замене $r - 1$ на r . В определение $b_{i,k,r}$, $b_{i,k,r,j}$ подставим соответственно выражения для $b_{s,t,r-1}$, $b_{s,t,r-1,j}$ из формул (9), (10), (11), справедливых по предположению индукции. В полученных выражениях вычислим показатели степеней m , m_j и воспользуемся определением $y_{i,k,r}$:

$$\begin{aligned} b_{i,k,r} &= \left(\delta_{i,k,r-1}^{l^r} m^{(i,k)} \prod_{j=0}^N \prod_{(m,m_j) \in M_{j,r-1}} m^{y_{i,k,r-1}(m,m_j)} \right) \\ &\quad \times \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \left(\delta_{s,t,r-1}^{l^r} m^{(s,t)} \prod_{j=0}^N \prod_{(m,m_j) \in M_{j,r-1}} m^{y_{s,t,r-1}(m,m_j)} \right)^{w_{i,k,r}(s,t)} \\ &= \left(\delta_{i,k,r-1} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \delta_{s,t,r-1}^{w_{i,k,r}(s,t)} \right)^{l^r} m^{(i,k)} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} (m^{(s,t)})^{w_{i,k,r}(s,t)} \\ &\quad \times \prod_{j=0}^N \prod_{(m,m_j) \in M_{j,r-1}} m^{y_{i,k,r-1}(m,m_j) + \sum_{s=0}^N \sum_{t=c_{r,s}+1}^{c_{r-1,s}} y_{s,t,r-1}(m,m_j) w_{i,k,r}(s,t)} \end{aligned}$$

$$\begin{aligned}
&= \delta_{i,k,r}^{l^e} m^{(i,k)} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} (m^{(s,t)})^{y_{i,k,r}(m^{(s,t)}, m_s^{(t)})} \prod_{j=0}^N \prod_{(m, m_j) \in M_{j,r-1}} m^{y_{i,k,r}(m, m_j)}, \\
b_{i,k,r,i} &= \delta_{i,k,r-1,i}^{l^e} m_i^{(k)} \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{i,k,r-1}(m, m_i)} \\
&\quad \times \prod_{t=c_{r,i}+1}^{c_{r-1,i}} \left(\delta_{i,t,r-1,i}^{l^e} m_i^{(t)} \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{i,t,r-1}(m, m_i)} \right)^{w_{i,k,r}(i,t)} \\
&\quad \times \prod_{s=0,1,\dots,N, s \neq i} \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \left(\delta_{s,t,r-1,i}^{l^e} \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{s,t,r-1}(m, m_i)} \right)^{w_{i,k,r}(s,t)} \\
&= \left(\delta_{i,k,r-1,i} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \delta_{s,t,r-1,i}^{w_{i,k,r}(s,t)} \right)^{l^e} m_i^{(k)} \\
&\quad \times \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{i,k,r-1}(m, m_i) + \sum_{s=0}^N \sum_{t=c_{r,s}+1}^{c_{r-1,s}} y_{s,t,r-1}(m, m_i) w_{i,k,r}(s,t)} \prod_{t=c_{r,i}+1}^{c_{r-1,i}} (m_i^{(t)})^{w_{i,k,r}(i,t)} \\
&= \delta_{i,k,r,i}^{l^e} m_i^{(k)} \prod_{(m, m_i) \in M_{i,r-1}} m_i^{y_{i,k,r}(m, m_i)} \prod_{t=c_{r,i}+1}^{c_{r-1,i}} (m_i^{(t)})^{y_{i,k,r}(m^{(i,t)}, m_i^{(t)})}.
\end{aligned}$$

Далее, при $j \neq i$

$$\begin{aligned}
b_{i,k,r,j} &= \delta_{i,k,r-1,j}^{l^e} \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{i,k,r-1}(m, m_j)} \\
&\quad \times \prod_{t=c_{r,j}+1}^{c_{r-1,j}} \left(\delta_{j,t,r-1,j}^{l^e} m_j^{(t)} \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{j,t,r-1}(m, m_j)} \right)^{w_{i,k,r}(j,t)} \\
&\quad \times \prod_{s=0,1,\dots,N, s \neq j} \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \left(\delta_{s,t,r-1,j}^{l^e} \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{s,t,r-1}(m, m_j)} \right)^{w_{i,k,r}(s,t)} \\
&= \left(\delta_{i,k,r-1,j} \prod_{s=0}^N \prod_{t=c_{r,s}+1}^{c_{r-1,s}} \delta_{s,t,r-1,j}^{w_{i,k,r}(s,t)} \right)^{l^e} \\
&\quad \times \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{i,k,r-1}(m, m_j) + \sum_{s=0}^N \sum_{t=c_{r,s}+1}^{c_{r-1,s}} y_{s,t,r-1}(m, m_j) w_{i,k,r}(s,t)} \prod_{t=c_{r,j}+1}^{c_{r-1,j}} (m_j^{(t)})^{w_{i,k,r}(j,t)} \\
&= \delta_{i,k,r,j}^{l^e} \prod_{(m, m_j) \in M_{j,r-1}} m_j^{y_{i,k,r}(m, m_j)} \prod_{t=c_{r,j}+1}^{c_{r-1,j}} (m_j^{(t)})^{y_{i,k,r}(m^{(j,t)}, m_j^{(t)})}
\end{aligned}$$

для некоторых $\delta_{i,k,r} \in$, $\delta_{i,k,r,j} \in$ j . По определению множеств $M_{j,r}$ последнее выражение каждой цепочки равенств совпадает с правой частью соответственно (9), (10), (11) при замене $r-1$ на r . Равенства (13), (15) следуют из определения $b_{i,k,r}$, $b_{i,k,r,j}$ и

предположения индукции. По предположению индукции

$$b_{i,k,r-1} \in \Gamma_r, \quad b_{i,k,r-1,j} \in \Gamma_r^{(j)},$$

поэтому значения $\lambda_r(b_{i,k,r})$, $\lambda_r^{(i)}(b_{i,k,r,j})$ определены, а равенства (14) и (16) следуют соответственно из определения $b_{i,k,r}$ и $b_{i,k,r,j}$ и уравнений в (12), отвечающих $\lambda_{r,1}, \dots, \lambda_{r,n}$ и $\lambda_{r,1}^{(j)}, \dots, \lambda_{r,n_j}^{(j)}$ и столбцу $v_{i,k,r}$. Из определения множеств $M_{i,r}$ и чисел $c_{r,i}$ следует равенство

$$\sum_{i=0}^N |M_{i,r}| = \sum_{i=0}^N (|M_{i,r-1}| + c_{r-1,i} - c_{r,i}) = \sum_{i=0}^N |M_{i,r-1}| + \left(n + \sum_{i=0}^N n_i \right),$$

откуда по предположению индукции получаем (17).

Докажем, что отображение u действительно решает поставленную задачу, то есть определенные в ее формулировке числа γ , γ_i при данном u являются l^e -ми степенями в $\mathbb{O}_K$, $\mathbb{O}_{K_i}$ соответственно.

Из определения γ , u и равенства (9) при $i = k = 0$, $r - 1 = \sigma$ следует, что

$$b_{0,0,\sigma} = \delta_{0,0,\sigma}^{l^e} \gamma. \quad (18)$$

То, что γ является l^e -й степенью в $\mathbb{O}_K$, при $S \subset K$ следует из равенств (13) при $i = k = 0$, $r = \sigma$ и (18). В противном случае из тех же равенств следует, что γ удовлетворяет условию (1) леммы 8. В этом случае для доказательства того, что γ является l^e -й степенью в $\mathbb{O}_K$, достаточно доказать выполнение условия (2). Из равенства (14) при $i = k = 0$, $r = \sigma$, определения λ и неравенства $2^\sigma > e$ следует, что

$$b_{0,0,\sigma}^\varepsilon \equiv 1 \pmod{l^{e+1}\mathbb{O}_K}. \quad (19)$$

Возведем (18) в степень ε и воспользуемся (19), тогда

$$(\delta_{0,0,\sigma}^\varepsilon)^{l^e} \gamma^\varepsilon \equiv 1 \pmod{l^{e+1}\mathbb{O}_K}. \quad (20)$$

Из алгоритма следует, что $\delta_{0,0,\sigma} \in \Gamma_1$, поэтому из определения ε получаем, что

$$\delta_{0,0,\sigma}^\varepsilon \equiv 1 \pmod{l\mathbb{O}_K},$$

откуда индукцией по e с применением формулы бинома Ньютона получаем, что

$$(\delta_{0,0,\sigma}^\varepsilon)^{l^e} \equiv 1 \pmod{l^{e+1}\mathbb{O}_K},$$

что вместе с (20) доказывает выполнение условия (2) леммы 8.

Аналогично доказывается, что γ_i является l^e -й степенью в $\mathbb{O}_{K_i}$, $i = 0, 1, \dots, N$. Для этого достаточно вместо равенств (9) при $i = k = 0$, $r - 1 = \sigma$, (13), (14) при $i = k = 0$, $r = \sigma$ использовать соответственно равенства (10), (11) при $i = k = 0$, $r - 1 = \sigma$, (15), (16) при $i = k = 0$, $r = \sigma$.

Лемма доказана.

Лемма 10. Пусть

$$v = |S| + n + \sum_{i=0}^N (|S_i| + n_i),$$

β — суммарное число ненулевых элементов матриц A и V . Если коэффициенты разложения элементов $m^{(0,0)}, m_0^{(0)}, m, m_i$, где $(m, m_i) \in M_i, i = 0, \dots, N$, для которых в алгоритме вычисляются значения отображений $\lambda_{r,j}, \lambda_{r,j}^{(i)}$, в соответствующих базисах по абсолютной величине не превосходят l^{2^σ} и уравнения (5), (12) имеют решения, то изложенный выше алгоритм может быть реализован с трудоемкостью

$$O \left((e \ln l)^2 \beta v + (\ln e + 1)(e \ln l)^3 \left(n + \sum_{i=0}^N n_i \right) \left(\sum_{j=0}^N |M_j| (n^3 + n_j^3) \right) + (e \ln l)^3 \left(n + \sum_{i=0}^N n_i \right)^2 \left(n^3 + \sum_{i=0}^N n_i^3 \right) \right).$$

Доказательство. На шаге 1 для $i = 0, 1, \dots, N, (m, m_i) \in M_i$ предварительно вычислим $m^\varepsilon \bmod l^{2^\sigma}, m_i^\varepsilon \bmod l^{2^\sigma}$ и аналогично для $(m^{(0,0)}, m_0^{(0)})$. Вычисление $m^\varepsilon \bmod l^{2^\sigma}$ требует $O(\ln \varepsilon) = O(n \ln l)$ умножений по модулю l^{2^σ} , каждое из которых требует $O(n^3)$ арифметических операций по модулю l^{2^σ} . Поэтому суммарная трудоемкость указанных вычислений составляет

$$O \left(2^{2^\sigma} \ln^3 l \sum_{i=0}^N |M_i| (n^4 + n_i^4) \right). \quad (21)$$

Если $r \in \{1, \dots, \sigma\}$ и для $\gamma \in \Gamma_r$ вычислены $x_j \in \{0, 1, \dots, l^{2^r} - 1\}$ такие, что

$$\gamma^\varepsilon - 1 = \sum_{j=1}^n x_j b_j \bmod l^{2^\sigma},$$

то $\lambda_{r,j}(\gamma)$ вычисляются как $(x_j \bmod l^{2^r}) / l^{2^{r-1}}$ с суммарной трудоемкостью $O((2^{\sigma+r} - 2^{2r})n \ln^2 l)$. Поэтому трудоемкость остальных вычислений на шаге 1 составляет

$$O \left(2^\sigma \ln^2 l \sum_{i=0}^N |M_i| (n + n_i) \right)$$

и, следовательно, трудоемкость шага 1 равна (21).

Уравнение (5) может быть решено с трудоемкостью $O((\beta_A + Q)v)$ операций по модулю l^e , где β_A — число ненулевых элементов матрицы A , Q — трудоемкость вычисления скалярных произведений столбцов матрицы $A^T V$ на фиксированный вектор w с элементами из $\mathbb{Z}/l^e \mathbb{Z}$ (см. [9]). Указанные произведения есть компоненты вектора $(A^T V)^T w = V^T (Aw)$ и поэтому могут быть вычислены с трудоемкостью $Q = O(\beta_A + \beta_V)$ операций по модулю l^e , где β_V — число ненулевых элементов матрицы V . Таким образом, трудоемкость шага 2 есть

$$O((e \ln l)^2 \beta v). \quad (22)$$

Опишем реализацию шага 3 и оценим ее трудоемкость. Если

$$\sum_{i=0}^N c_{1,i} > 0,$$

то для $i, j = 0, 1, \dots, N$, $k = \text{sign } i, \dots, c_{1,i}$, используя определение $b_{i,k,1}, b_{i,k,1,j}$ и результаты предварительных вычислений на шаге 1, вычислим

$$b_{i,k,1}^\varepsilon \bmod l^{2^\sigma} \mathbb{O}, \quad b_{i,k,1,j}^\varepsilon \bmod l^{2^\sigma} \mathbb{O}_j.$$

Одно значение вычисляется соответственно за

$$\sum_{j=0}^N \sum_{(m, m_j) \in M_{j,1}} (1 + O(\ln y_{i,k,1}(m, m_j))) = O \left(e \ln l \sum_{j=0}^N |M_{j,1}| \right)$$

умножений по модулю $l^{2^\sigma} \mathbb{O}$, или за

$$\sum_{(m, m_j) \in M_{j,1}} (1 + O(\ln y_{i,k,1}(m, m_j))) = O(e |M_{j,1}| \ln l)$$

умножений по модулю $l^{2^\sigma} \mathbb{O}_j$. Поэтому трудоемкость вычисления всех указанных значений есть

$$\begin{aligned} & O \left(2^{2^\sigma} e \ln^3 l \left(\sum_{i=0}^N c_{1,i} \right) \left(\sum_{j=0}^N |M_{j,1}| (n^3 + n_j^3) \right) \right) \\ & = O \left(2^{2^\sigma} e (\sigma - 1) \ln^3 l \left(n + \sum_{i=0}^N n_i \right) \left(\sum_{j=0}^N |M_j| (n^3 + n_j^3) \right) \right). \end{aligned} \quad (23)$$

В цикле по $r = 2, \dots, \sigma$ последовательно вычислим для $i, j = 0, 1, \dots, N$, $k = \text{sign } i, \dots, c_{r,i}$ значения

$$b_{i,k,r}^\varepsilon \bmod l^{2^\sigma} \mathbb{O}, \quad b_{i,k,r,j}^\varepsilon \bmod l^{2^\sigma} \mathbb{O}_j,$$

используя определение $b_{i,k,r}, b_{i,k,r,j}$. Одно значение вычисляется за

$$\sum_{s=0}^N (c_{r-1,s} - c_{r,s}) (1 + O(\ln w_{i,k,r}(s, t))) = O \left(2^r \ln l \sum_{s=0}^N (c_{r-1,s} - c_{r,s}) \right)$$

умножений соответственно по модулю $l^{2^\sigma} \mathbb{O}$ или по модулю $l^{2^\sigma} \mathbb{O}_j$. Поэтому трудоемкость вычисления всех указанных значений есть

$$O \left(2^{2^\sigma+r} \ln^3 l \left(\sum_{i=0}^N c_{r,i} \right) \left(n^3 + \sum_{j=0}^N n_j^3 \right) \left(\sum_{s=0}^N (c_{r-1,s} - c_{r,s}) \right) \right). \quad (24)$$

Вычисление векторов $v_{i,k,r}$ требует еще

$$O \left((2^{\sigma+r} - 2^{2r}) \ln^2 l \left(\sum_{i=0}^N c_{r-1,i} \right) \left(n + \sum_{j=0}^N n_j \right) \right) \quad (25)$$

двоичных операций. Решение уравнения (12) методом гауссова исключения требует

$$O\left(\left(\sum_{i=0}^N (c_{r-1,i} - c_{r,i})\right)^2 \sum_{i=0}^N c_{r-1,i}\right)$$

операций по модулю $l^{2^{r-1}}$ или

$$O\left(2^{2r} \ln^2 l \left(\sum_{i=0}^N (c_{r-1,i} - c_{r,i})\right)^2 \sum_{i=0}^N c_{r-1,i}\right) \quad (26)$$

двоичных операций. Сумма трудоемкостей (24)–(26) с учетом следующих из определения $c_{r,i}$ равенств

$$\sum_{i=0}^N c_{r,i} = (\sigma - r)(n + \sum_{i=0}^N n_i), \quad r = 1, \dots, \sigma,$$

равна

$$O\left(2^{2\sigma+r}(\sigma-r+1)\ln^3 l\left(n^3+\sum_{i=0}^N n_i^3\right)\left(n+\sum_{i=0}^N n_i\right)^2\right),$$

то есть трудоемкость цикла по r есть

$$O\left(2^{3\sigma} \ln^3 l \left(n^3 + \sum_{i=0}^N n_i^3\right) \left(n + \sum_{i=0}^N n_i\right)^2\right). \quad (27)$$

Суммируя трудоемкости (21), (22), (23), (27) с учетом неравенства $2^\sigma > e \geq 2^{\sigma-1}$ и замечая, что величину вида (21) можно записать в виде (23), получаем утверждение леммы.

Чтобы использовать данную лемму для оценки трудоемкости применения изложенного алгоритма в излагаемом ниже алгоритме дискретного логарифмирования, мы примем эвристическое допущение о выполнении ее условий при соответствующих входных данных алгоритма. Приведем некоторые соображения в пользу такого допущения. Заметим, что матрица A имеет вид

$$\begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots \\ A_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & A_1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & A_N \end{pmatrix},$$

где $A_i, i = 0, 1, \dots, N$, — матрицы, столбцами которых являются векторы

$$(\underbrace{\dots, e_{\mathbf{p}_i}, \dots}_{\mathbf{p}_i \in \mathcal{S}_i}, \lambda_{1,1}^{(i)}(m_i), \dots, \lambda_{1,n_i}^{(i)}(m_i))^T, (m, m_i) \in M_{i,1}.$$

Иными словами, уравнение (5) содержит линейные подсистемы с матрицами A_i . Неравенства (2) означают, что эти подсистемы не являются переопределенными, а неравенство (3) — что уравнение (5) в целом не является переопределенным, тем самым позволяя надеяться на его разрешимость. Уравнение (12) также не является переопределенным, так как из алгоритма следует, что матрица A_r — квадратная.

3. Алгоритм

Дано: p — простое число, $a, b \in \{2, \dots, p-1\}$,

$$(\mathbb{Z}/p\mathbb{Z})^* = \langle a \bmod p \rangle,$$

параметры алгоритма — $n, B_0, B_Q, B_\alpha, C, D, D_0, l_0, N \in \mathbb{N}, l_0 \geq B_\alpha$.

Найти: $x = \log_a b \in \{1, \dots, p-2\}$ такое, что $a^x \equiv b \bmod p$.

1. Разложим число $p-1$ на простые множители по алгоритму работы [2].
2. Стандартным образом (см., например, [3]) находим $z \in \{0, 1, \dots, p-2\}$, $t \in \mathbb{N}$, и для $k = 1, \dots, t$ — простые числа q_k , $q_k \leq B_0$, $e_k \in \mathbb{N}$ такие, что

$$a^z b \equiv \prod_{k=1}^t q_k^{e_k} \bmod p.$$

Для каждого $k = 1, \dots, t$ выполняем следующие шаги 3–8.

3. Следуя [3], положим $m = 2^h q_k$, где h выбрано так, что $p^{1/n} < m < 2p^{1/n}$. Построим многочлен

$$f_0 = \sum_{j=0}^{n_0} a_{0,j} X^j \in \mathbb{Z}[X]$$

степени n_0 , обладающий следующими свойствами:

- (1) f_0 неприводим,
- (2) f_0 унитарен,
- (3) $n_0 \leq n$,
- (4) $f_0(m) \equiv 0 \bmod p$,
- (5) $a_{0,0}$ является B_α -гладким числом,
- (6) $\gcd(p-1, \text{disc } f_0)$ является l_0 -гладким.

Многочлен f_0 строится следующим образом. Пусть $\sum_{j=0}^n b_j m^j$ — разложение числа $\lceil m^n/p \rceil p$ по основанию m . Методом решета находим такое $d_0 \in \{-D_0, \dots, D_0\}$, что число $b_0 - d_0 m$ является B_α -гладким. Разложим многочлен

$$\sum_{j=0}^n b_j X^j + d_0(X - m)$$

на неприводимые множители над $\mathbb{Z}$ и в качестве f_0 возьмем тот из них, который обладает свойствами (4) и (6).

4. Для $i = 1, \dots, N$ построим отличные от f_0 многочлены

$$f_i = \sum_{j=0}^{n_i} a_{i,j} X^j \in \mathbb{Z}[X]$$

степеней n_i , обладающие теми же свойствами, что и f_0 , за исключением, может быть, свойства (5). Это делается аналогично построению многочлена f_0 , только вместо d_0 можно взять $d_i = i$.

5. Для $i = 0, 1, \dots, N$ обозначим α_i фиксированный корень многочлена f_i , и пусть $K_i = \mathbb{Q}(\alpha_i)$, K_i — кольцо целых алгебраических чисел поля K_i . Построим множество S , состоящее из простых чисел, не превосходящих $B_{\mathbb{Q}}$, и для $i = 0, 1, \dots, N$ — множества S_i , состоящие из хороших простых идеалов первой степени колец K_i , норма которых не превосходит B_{α} .

Шаги 6 и 7 выполняются аналогично [2].

6. Методом решета найдем пары взаимно простых целых чисел

$$(c, d) \in \{1, \dots, C\} \times \{-D, \dots, D\}$$

такие, что $c + dm$ является $B_{\mathbb{Q}}$ -гладким числом.

7. Для каждого $i = 0, 1, \dots, N$ построим множество M_i всех пар $(c + dm, c + d\alpha_i)$, где пара (c, d) найдена на шаге 6 и идеал $(c + d\alpha_i)_{K_i}$ разлагается в произведение идеалов из множества S_i . С этой целью для каждой пары (c, d) , найденной на шаге 6, и $i = 0, 1, \dots, N$ по лемме 4 вычисляем $N_{K_i/\mathbb{Q}}(c + d\alpha_i)$, проверяем, является ли это число B_{α} -гладким (методом эллиптических кривых [7]) и взаимно простым с $[O_{K_i} : \mathbb{Z}[\alpha_i]]$ (с помощью лемм 1, 2). Если да, то $(c, d) \in S_i$ и, используя полученное разложение $N_{K_i/\mathbb{Q}}(c + d\alpha_i)$ на простые множители, по лемме 5 получаем искомое разложение $(c + d\alpha_i)_{K_i}$. Добавим в множество M_0 пару $(a, 1)$.

8. Для каждого простого l такого, что $l \mid p-1$, $l > l_0$, применим алгоритм из раздела 2.3 со следующими входными данными:

$$\begin{aligned} K &= \mathbb{Q}, & &= \mathbb{Z}; & i &= \mathbb{Z}[\alpha_i], & i &= 0, 1, \dots, N; \\ e &= v_l(p-1), & m^{(0,0)} &= 2^h, & m^{(0)} &= \alpha_0 \end{aligned}$$

(остальные входные данные соответствуют обозначениям излагаемого алгоритма). Возможность применения алгоритма следует из условий

$$l \nmid \text{disc } f_i, \quad i = 0, 1, \dots, N,$$

выполненных в силу свойства (6) многочлена, и из неравенств $l > l_0 \geq B_{\alpha}$, которые обеспечивают выполнение условия (1).

Если в результате работы алгоритма найдено отображение y , то положим

$$x_k^{(l)} \equiv y(a, 1) \bmod l^{v_l(p-1)},$$

в противном случае возвращаемся на шаг 4 и набираем дополнительное количество пар (c, d) .

9. Для каждого простого l такого, что $l \mid p - 1$, $l > l_0$, проверяем выполнение условия

$$a^{\left(\sum_{k=1}^t e_k x_k^{(l)} - z\right)(p-1)/l^{v_l(p-1)}} \equiv b^{(p-1)/l^{v_l(p-1)}} \pmod{p} \quad (28)$$

которое, очевидно, эквивалентно условию

$$\sum_{k=1}^t e_k x_k^{(l)} - z \equiv \log_a b \pmod{l^{v_l(p-1)}}.$$

Если хотя бы для одного l оно не выполнено, то алгоритм завершает работу, не найдя $\log_a b$.

10. Для каждого простого l , $l \mid p - 1$, такого, что $l \leq l_0$, найдем $\log_a b \pmod{l^{v_l(p-1)}}$ по алгоритму Полига–Хеллмана [10].

11. Найдем $\log_a b$ по китайской теореме об остатках.

4. Обоснование алгоритма

Для обоснования алгоритма достаточно доказать равенство (28). То, что отображение y является решением задачи из раздела 2.3 с входными данными, определенными на шаге 8, означает, что для чисел

$$\begin{aligned} \gamma &= 2^h a^{y(a,1)} \prod_{i=0}^N \prod_{(c+dm, c+d\alpha_i) \in M_i} (c+dm)^{y(c+dm, c+d\alpha_i)}, \\ \gamma_0 &= \alpha_0 \prod_{(c+dm, c+d\alpha_0) \in M_0} (c+d\alpha_0)^{y(c+dm, c+d\alpha_0)}, \\ \gamma_i &= \prod_{(c+dm, c+d\alpha_i) \in M_i} (c+d\alpha_i)^{y(c+dm, c+d\alpha_i)}, \quad i = 1, \dots, N, \end{aligned}$$

выполнены равенства

$$\gamma = \delta^{l^e}, \quad \gamma_i = \delta_i^{l^e}, \quad i = 0, \dots, N,$$

для некоторых $\delta \in \mathbb{Z}$, $\delta_i \in \mathbb{O}_{K_i}$. Умножим обе части равенства, соответствующего i , на $[\mathbb{O}_{K_i} : \mathbb{Z}[\alpha_i]]^{l^e}$ и к полученному равенству применим гомоморфизм

$$\varphi_i : \mathbb{Z}[\alpha_i] \rightarrow \mathbb{Z}/p\mathbb{Z},$$

определяемый соответствием $\alpha_i \rightarrow m$. В результате получаем, что

$$\begin{aligned} [\mathbb{O}_{K_0} : \mathbb{Z}[\alpha_0]]^{l^e} m \prod_{(c+dm, c+d\alpha_0) \in M_0} (c+dm)^{y(c+dm, c+d\alpha_0)} \\ \equiv (\varphi_0([\mathbb{O}_{K_0} : \mathbb{Z}[\alpha_0]]\delta_0))^{l^e} \pmod{p}, \end{aligned} \quad (29)$$

$$\begin{aligned} [\mathbb{O}_{K_i} : \mathbb{Z}[\alpha_i]]^{l^e} \prod_{(c+dm, c+d\alpha_i) \in M_i} (c+dm)^{y(c+dm, c+d\alpha_i)} \\ \equiv (\varphi_i([\mathbb{O}_{K_i} : \mathbb{Z}[\alpha_i]]\delta_i))^{l^e} \pmod{p}, \quad i = 1, \dots, N. \end{aligned} \quad (30)$$

Из равенств $\gamma = \delta^{l^e}$, $m = 2^h b$, (29), (30) получаем, что

$$a^{y(a,1)} \equiv b\delta^{l^e} \pmod{p}$$

для некоторого $\delta' \pmod{p} \in (\mathbf{Z}/p\mathbf{Z})^*$, откуда следует (28).

5. Выбор параметров и оценка сложности

Вначале оценим асимптотическую сложность шагов 5–8, а затем докажем, что полученная оценка верна и для остальных шагов алгоритма. Будем искать оптимальные значения параметров в виде

$$\begin{aligned} B_Q &= L_p[s_Q, c_Q], \quad B_\alpha = L_p[s_\alpha, c_\alpha], \quad p^{1/n} = L_p[s_1, c_1], \\ C &= L_p[s_2, c_2], \quad D = L_p[s_2, c_2], \quad D_0 = L_p[s_{2,0}, c_{2,0}], \quad N = L_p[s_3, c_3] \end{aligned}$$

для некоторых положительных констант $s_Q, s_\alpha, s_1, s_2, s_{2,0}, s_3, c_Q, c_\alpha, c_1, c_2, c_{2,0}, c_3$.

На шаге 6 проверяются на B_Q -гладкость числа $|c + dm|$, не превосходящие

$$C + 2Dp^{1/n} = L_p[s_1, c_1]L_p[s_2, c_2] = L_p[\max(s_1, s_2), c_4] \quad (31)$$

для некоторого c_4 , поэтому доля B_Q -гладких среди них по лемме 6 не менее

$$L_p[\max(s_1, s_2) - s_Q, (s_Q - \max(s_1, s_2))c_4/c_Q] = L_p[\max(s_1, s_2) - s_Q, -c_5]$$

для некоторого c_5 , и на данном шаге мы находим не менее

$$L_p[s_2, 2c_2]L_p[\max(s_1, s_2) - s_Q, -c_5]$$

таких пар (c, d) . С помощью леммы 7 заключаем, что суммарная трудоемкость шагов 5 и 6 не превосходит

$$L_p[s_Q, c_Q] + L_p[s_3, c_3]L_p[s_\alpha, c_\alpha] + L_p[s_2, 2c_2].$$

Для $i = 0, 1, \dots, N$ коэффициенты многочленов f_i удовлетворяют неравенствам

$$|a_{i,0}| \leq |b_0| + |d_i|m \leq (\max(D_0, N) + 1)m,$$

и, согласно теореме 3.5.1 в [4],

$$\begin{aligned} |a_{i,j}| &\leq \binom{n_i-1}{j} \sqrt{(b_0 - d_i m)^2 + (b_1 + d_i)^2 + \sum_{k=2}^n b_k^2} + \binom{n_i-1}{j-1} |b_n| \\ &\leq \binom{n_i}{j} \left(\sum_{k=0}^n |b_k| + |d_i|(m+1) \right) \\ &< \binom{n_i}{j} (2np^{1/n} + \max(D_0, N)(2p^{1/n} + 1)), \quad j = 1, \dots, n_i. \end{aligned}$$

Таким образом, на шаге 7 проверяются на B_α -гладкость числа

$$\left| \sum_{j=0}^{n_i} a_{i,j} c^j (-d)^{n_i-j} \right|,$$

не превосходящие

$$\begin{aligned} & (2np^{1/n} + \max(D_0, N)(2p^{1/n} + 1)) (C + D)^{n_i} \\ &= \max(L_p[s_{2,0}, c_{2,0}], L_p[s_3, c_3]) L_p[s_1, c_1] L_p[1 + s_2 - s_1, c_2/c_1] \\ &= L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1), c_6] \quad (32) \end{aligned}$$

для некоторого c_6 , $i = 0, 1, \dots, N$. Поэтому по лемме 6 каждое из них является B_α -гладким с вероятностью, не меньшей

$$\begin{aligned} & L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha, (s_\alpha - \max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1))c_6/c_\alpha] \\ &= L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha, -c_{10}], \end{aligned}$$

для некоторого c_7 , откуда с учетом числа пар (c, d) , найденных на шаге 6, получаем, что

$$\begin{aligned} |M_i| &\geq L_p[s_2, 2c_2] L_p[\max(s_1, s_2) - s_Q, -c_5] \\ &\quad \times L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha, -c_7], \quad i = 0, \dots, N. \quad (33) \end{aligned}$$

Согласно гипотезе 1 трудоемкость каждой проверки не превосходит

$$L_p[s_\alpha/2, \sqrt{2s_\alpha c_\alpha}]$$

операций на эллиптических кривых над кольцами вычетов по соответствующим модулям, следовательно, трудоемкость данного шага не больше

$$L_p[s_2, 2c_2] L_p[\max(s_1, s_2) - s_Q, -c_5] L_p[s_3, c_3] L_p[s_\alpha/2, \sqrt{2s_\alpha c_\alpha}].$$

Из (33) следует, что условия (2), (3) применимости алгоритма из раздела 2.3 на шаге 8 имеют вид

$$\begin{aligned} & L_p[s_2, 2c_2] L_p[\max(s_1, s_2) - s_Q, -c_5] L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha, -c_7] \\ &\geq L_p[s_\alpha, c_\alpha], \quad (34) \end{aligned}$$

$$\begin{aligned} & L_p[s_2, 2c_2] L_p[\max(s_1, s_2) - s_Q, -c_5] L_p[\max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha, -c_7] L_p[s_3, c_3] \\ &\geq L_p[s_Q, c_Q] + L_p[s_3, c_3] L_p[s_\alpha, c_\alpha]. \quad (35) \end{aligned}$$

Трудоемкость шага 8 оценим, используя лемму 10. Для $i = 0, 1, \dots, N$ число ненулевых элементов в столбце матрицы A или V , отвечающем паре $(c + dm, c + d\alpha_i)$, не превосходит

$$\beta_{i,c,d} = v(c + dm) + v\left(\sum_{j=0}^{n_i} a_{i,j} c^j (-d)^{n_i-j}\right) + n_i.$$

Из (31), (32), выбора n и неравенства $v(x) \leq \log_2 |x|$ следует, что $\beta_{i,c,d} = (\ln p)^{O(1)}$. Для числа ненулевых элементов в столбцах, отвечающих парам $(a, 1)$, $(2^h, \alpha_0)$, верна аналогичная оценка. Поэтому

$$\beta = (\ln p)^{O(1)} \sum_{i=0}^N |M_i|,$$

и с учетом (33) и (35) трудоемкость шага 8 по лемме 10 не больше

$$(L_p[s_Q, c_Q] + L_p[s_3, c_3]L_p[s_\alpha, c_\alpha])^2 + (L_p[s_3, c_3])^3.$$

Таким образом, суммарная трудоемкость шагов 5–8 не больше

$$T' = L_p[\max(s_Q, s_\alpha, s_1 - s_Q, s_2, s_3), c_T]$$

для некоторой константы c_T . Минимизируем T' при условиях (34), (35). Из (34), (35) следует, что

$$\begin{aligned} s_2 &\geq \max(s_\alpha, \max(s_1, s_2) - s_Q, \max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha), \\ \max(s_2, s_3) &\geq \max(s_Q, s_3, s_\alpha, \max(s_1, s_2) - s_Q, \max(s_1, s_{2,0}, s_3, 1 + s_2 - s_1) - s_\alpha). \end{aligned}$$

Минимизируя при этих условиях $\max(s_Q, s_\alpha, s_1 - s_Q, s_2, s_3)$, получим, что

$$s_Q = s_\alpha = s_2 = 1/3, \quad s_1 = 2/3, s_{2,0} \leq 2/3, \quad s_3 \leq 1/3,$$

откуда

$$\begin{aligned} c_4 &= c_1, \\ c_5 &= c_1/(3c_Q), \\ c_6 &= c_1 + c_2/c_1, \\ c_7 &= (c_1 + c_2/c_1)/(3c_\alpha), \\ c_T &= \begin{cases} 2 \max(c_Q, c_\alpha, c_2), & \text{если } s_3 < 1/3, \\ \max(2c_2, 2c_2 - c_1/(3c_Q) + c_3, 2c_Q, 2c_3 + 2c_\alpha, 3c_3), & \text{если } s_3 = 1/3. \end{cases} \end{aligned}$$

Условия (34), (35) принимают вид

$$\begin{aligned} s_3 < 1/3, \quad 2c_2 - \frac{c_1}{3c_Q} - \frac{1}{3c_\alpha} \left(c_1 + \frac{c_2}{c_1} \right) &\geq \max(c_Q, c_\alpha), \\ s_3 = 1/3, \quad 2c_2 - \frac{c_1}{3c_Q} + c_3 - \frac{1}{3c_\alpha} \left(c_1 + \frac{c_2}{c_1} \right) &\geq \max(c_Q, c_3 + c_\alpha). \end{aligned}$$

Минимизируя c_T при этих условиях, получим, что

$$\begin{aligned} s_3 &= 1/3, \quad c_Q = c_2 = \left(\frac{46 + 13\sqrt{13}}{108} \right)^{1/3}, \\ c_\alpha &= c_2 \left(\frac{\sqrt{13} - 1}{3} \right), \quad c_1 = \frac{3}{c_2(4\sqrt{13} - 10)}, \\ c_3 &= c_Q - c_\alpha, \quad c_T = 2c_2 = \left(\frac{92 + 26\sqrt{13}}{27} \right)^{1/3}. \end{aligned}$$

Легко видеть, что при найденных значениях параметров трудоемкость шагов 5–8 действительно равна

$$T' = L_p \left[1/3, \left(\frac{92 + 26\sqrt{13}}{27} \right)^{1/3} \right].$$

Трудоёмкость шага 1 также равна (см. [2])

$$L_p \left[1/3, \left(\frac{92 + 26\sqrt{13}}{27} \right)^{1/3} \right].$$

То, что выбор a B_Q -гладким не ограничивает общности, следует из теоремы 3 в [11].

С использованием гипотезы 1 нетрудно показать, что минимальная оценка трудоёмкости шага 2 достигается при

$$B_0 = L_p[2/3, 1/3^{1/3}]$$

и составляет $L_p[1/3, 3^{1/3}]$, что для достаточно больших p меньше T' .

На шаге 3 для $i = 0, 1, \dots, N$ трудоёмкость разложения многочлена

$$\sum_{j=0}^n b_j X^j + d_i(X - m)$$

есть

$$O \left(n^{12} + n^9 \ln^3 \sqrt{(b_0 - d_i m)^2 + (b_1 + d_i)^2 + \sum_{i=2}^n b_j^2} \right)$$

(см. [12]), что равно $(\ln p)^{O(1)}$, как и трудоёмкость остальных вычислений для построения f_i . Поэтому трудоёмкость данного шага есть

$$N(\ln p)^{O(1)} = L_p[1/3, (4 - \sqrt{13})c_2/3],$$

что для достаточно больших p меньше $T' = L_p[1/3, 2c_2]$.

Согласно лемме 9 и гипотезе 2 в предположении случайности выбора полей K , K_i равенство (28) выполнено для всех рассматриваемых значений k, l с вероятностью

$$1 - tN O \left(\sum_{l|p-1, l > l_0} 1/l \right).$$

Величина $tN \sum_{l|p-1, l > l_0} 1/l$ не превосходит $L_p[1/3, c_3]/l_0$. Выбор $l_0 = L_p[1/3, c]$, где $c_\alpha < c < 2c_T$, гарантирует, что для достаточно больших p выполнено условие $l_0 \geq B_\alpha$, трудоёмкость шага 10 не превосходит T' , и вероятность успешного завершения алгоритма стремится к 1 при $p \rightarrow \infty$.

Трудоёмкость шага 11 есть $(\ln p)^{O(1)}$.

Таким образом, при стандартных эвристических предположениях вероятность успешного завершения алгоритма стремится к 1 при $p \rightarrow \infty$, а сложность алгоритма не превосходит

$$\exp \left\{ \left(\left(\frac{92 + 26\sqrt{13}}{27} \right)^{1/3} + o(1) \right) (\ln p)^{1/3} (\ln \ln p)^{2/3} \right\}$$

двоичных операций, где $o(1) \rightarrow 0$ при $p \rightarrow \infty$. Эта оценка совпадает с наилучшей известной оценкой сложности факторизации целых чисел, полученной Д. Копперсмитом [2].

Автор благодарен своему научному руководителю О. Н. Василенко за полезные обсуждения, которые помогли улучшить изложение.

Список литературы

1. Матюхин Д. В., Мурашов Н. Н., Модификация метода решета числового поля для дискретного логарифмирования в поле $GF(p)$. *Обозрение прикладной и промышленной математики* (2000) 7, №2, 387–389.
2. Coppersmith D., Modifications to the number field sieve. *J. Cryptology* (1993) 6, 169–180.
3. Schirokauer O., Discrete logarithms and local units. *Phil. Trans. Royal Soc. Lond.* (1993) 345, 409–423.
4. Cohen H., *A course in computational algebraic number theory*. Springer, New York, 1993.
5. Dedekind R., *Gesammelte mathematische Werke, Bd I.*, Braunschweig, 1930.
6. Gordon D., Discrete logarithms in $GF(p)$ using the number field sieve. *SIAM J. Disc. Math.* (1993) 6, 124–138.
7. Lenstra H. W., Factoring integers with elliptic curves. *Ann. Math.* (1987) 126, 649–673.
8. Cohen H., Lenstra H. W., Heuristics on class groups of number fields. *Lect. Notes Math.* (1984) 1068, 33–62.
9. LaMacchia B., Odlyzko A. M., Solving large sparse linear systems over finite fields. *Lect. Notes Computer Sci.* (1991) 537, 109–133.
10. Pohlig S., Hellman M., An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory* (1978) 24, 106–110.
11. Shoup V., Searching for primitive roots in finite fields. *Math. Comp.* (1992) 58, 369–380.
12. Lenstra A. K., Lenstra H. W., Lovász L., Factoring polynomials with rational coefficients. *Math. Ann.* (1982) 261, 515–534.

Статья поступила 28.10.02.