5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 11(1). Research Paper 72. 16 p.
6. *Холл М.* Комбинаторика. М.: Мир, 1970.

УДК 511.48 DOI 10.17223/2226308X/13/3

АЛГОРИТМ ВЫЧИСЛЕНИЯ ЭЛЕМЕНТА ШТИКЕЛЬБЕРГЕРА ДЛЯ МНИМЫХ МУЛЬТИКВАДРАТИЧНЫХ ПОЛЕЙ

Д. О. Олефиренко, Е. А. Киршанова, Е. С. Малыгина, С. А. Новоселов

Представлен алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_i \equiv 1 \pmod 4$, $i = 1, \ldots, n$, и d_i попарно взаимно просты. Мы алгоритмизируем идеи, описанные в работе Р. Кучеры 1996 г., доказываем корректность полученных алгоритмов и анализируем их сложность. Для $2^n = [K : \mathbb{Q}]$ алгоритм работает за время $\widetilde{\mathcal{O}}(2^n)$. Полученный результат полезен для решения криптоаналитических задач поиска короткого вектора в идеалах мультиквадратичных полей.

Ключевые слова: *мультиквадратичные поля, идеал Штикельбергера, элемент Штикельбергера, задача поиска короткого вектора.*

Введение

Получение идеала Штикельбергера в явном виде является важной алгоритмической задачей в вычислительной теории чисел, в теории групп классов и, с недавних пор, в криптоанализе. Для числового поля K идеал Штикельбергера I — идеал групповой алгебры $\mathbb{Z}[G_K]$, где $G_K = \mathrm{Gal}(K/\mathbb{Q})$ — группа Галуа поля K. Полезное свойство I заключается в том, что под действием элементов I на Cl_K — группу классов идеалов K — любой класс становится тривиальным (иначе говоря, J^σ — главный идеал для любого $\sigma \in I$ и любого идеала J кольца целых $\mathcal{O}_K$ числового поля K).

Для кругового поля $K = \mathbb{Q}(\zeta_n)$ идеал Штикельбергера, рассматриваемый как решётка в $\mathbb{Z}^n$ с помощью вложения $\mathbb{Z}[G_K] \hookrightarrow \mathbb{Z}^n$, обладает «хорошим» базисом. Явный вид этого базиса описан, например, в [1]. Это свойство идеала Штикельбергера в сочетании с 1) «обнуляющим» действием элементов идеала на целые идеалы $\mathbb{Z}[\zeta_n]$ и 2) существованием (относительно) быстрого алгоритма нахождения короткого вектора в *главных* идеалах $\mathbb{Z}[\zeta_n]$ позволило получить алгоритм нахождения короткого вектора в идеалах кольца целых круговых полей [1]. В современном криптоанализе нахождение короткого вектора в решётках является основополагающей задачей.

Именно приложение идеала Штикельбергера в криптоанализе является нашей главной мотивацией для его изучения. Ввиду большой группы Галуа интересными полями являются мультиквадратичные. Недавние работы по эффективному вычислению короткого вектора в мультиквадратичных полях [2] и по вычислению группы классов [3] подводят к вопросу нахождения коротких векторов в *произвольных* идеалах. Следуя примеру круговых полей, логично обратить внимание на структуру идеала Штикельбергера для мультиквадратичных расширений.

В работе предлагается алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ и d_i попарно взаимно просты. Алгоритм имеет сложность $\widetilde{\mathcal{O}}(2^n)$, а так как $[K : \mathbb{Q}] = 2^n$, то даже для криптографически значимых степеней он эффективен. В основе алгорит-

ма лежит работа Р. Кучеры [4]. Доказательства всех утверждений статьи можно найти в полной версии работы[1].

1. Предварительные сведения

Исходя из условий, наложенных на d_i, справедливо вложение $K \hookrightarrow \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n})$. Кроме того, $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$, где $\ell \leqslant n$, что доказано в лемме 1.

Рассмотрим числовые поля $\mathbb{Q} \subseteq K \subseteq L$ и обозначим их соответствующие группы Галуа $G_L = \mathrm{Gal}(L/\mathbb{Q})$ и $G_K = \mathrm{Gal}(K/\mathbb{Q})$; $\mathbb{Q}[G_L] = \{\sum a_i\sigma_i : a_i \in \mathbb{Q}, \sigma_i \in G_L\}$ и $\mathbb{Q}[G_K] = \{\sum a_i\sigma_i : a_i \in \mathbb{Q}, \sigma_i \in G_K\}$ — группы, конечно порождённые элементами G_L (соответственно элементами G_K) над $\mathbb{Q}$. Важными понятиями при вычислении элементов Штикельбергера являются отображения res и cor. Определим эти отображения, согласно [4], для расширения L/K:

$$\mathsf{res}_{L/K} : \mathbb{Q}[G_L] \to \mathbb{Q}[G_K], \quad \mathsf{res}_{L/K}\Big(\sum_{\sigma \in G_L} a_\sigma \sigma\Big) = \sum_{\sigma \in G_L} a_\sigma(\sigma|_K),$$
$$\mathsf{cor}_{L/K} : \mathbb{Q}[G_K] \to \mathbb{Q}[G_L] \quad \mathsf{cor}_{L/K}\Big(\sum_{\sigma \in G_K} a_\sigma \sigma\Big) = \sum_{\sigma \in G_K} a_{\sigma|_K} \sigma,$$

где $\sigma|_K$ означает сужение автоморфизма $\sigma \in G_L$ на поле K; a_σ, $a_{\sigma|_K}$ — коэффициенты, соответствующие автоморфизмам σ, $\sigma|_K$.

Дробную часть числа обозначим $\langle\cdot\rangle$, т. е. $0 < \langle\cdot\rangle < 1$; наибольший общий делитель элементов $a, b \in \mathbb{Z}$ — через (a, b); символ Лежандра этих же элементов — $\left(\frac{a}{b}\right)$. Для произвольного множества A его мощность обозначим $\#A$. Дадим классические определения элемента и идеала Штикельбергера, согласно [5, с. 189].

Определение 1. Для любых $n \in \mathbb{N}$ и $\alpha \in \mathbb{Z}$ и кругового поля $\mathbb{Q}(\zeta_n)$ определим

$$\theta_n(\alpha) = \sum_{(a,n)=1} \left\langle -\frac{\alpha a}{n} \right\rangle \sigma_a^{-1},$$

где $0 < a \leqslant n$ и $\sigma_a \in G_{\mathbb{Q}(\zeta_n)} = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Определение 2. Для любых $n \in \mathbb{N}$ и $\alpha \in \mathbb{Z}$ определим

$$\theta_n'(\alpha) = \left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)} \circ \mathsf{res}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}\right)(\theta_n(\alpha))$$

— элемент Штикельбергера, где K и $\mathbb{Q}(\zeta_n)$ — соответственно числовое и круговое поля.

Определение 3. Идеалом Штикельбергера поля K называется идеал вида

$$I = \{\theta_n'(\alpha) | \alpha, n \in \mathbb{Z}, n \geqslant 1\} \cap \mathbb{Z}[G_K].$$

Теперь дадим определение квадратичным гауссовым суммам, а также покажем, как они взаимосвязаны с автоморфизмами круговых полей.

Определение 4. Пусть $m, k \in \mathbb{Z}$, $k > 0$. Квадратичная гауссова сумма определяется как $g(m, k) = \sum\limits_{b=0}^{k-1} \mathrm{e}^{2\pi i m b^2/k}$.

Следующая теорема позволяет выражать квадратные корни, рассматриваемые как элементы мультиквадратичного поля, через квадратичные гауссовы суммы.

[1] Представлена на страницах авторов `https://crypto-kantiana.com/`.

Теорема 1 [6, 1.5.2, с. 26]. Пусть $(m,k)=1$, $k>0$ и k нечётное. Тогда

$$g(m,k)=\left(\frac{m}{k}\right)g(1,k)=\begin{cases}\left(\dfrac{m}{k}\right)\sqrt{k}, & k\equiv 1 \pmod 4,\\ \left(\dfrac{m}{k}\right)i\sqrt{k}, & k\equiv 3 \pmod 4.\end{cases}$$

Если $-k\equiv 1 \pmod 4$, то $k\equiv 3 \pmod 4$. Тогда $\sqrt{-k}=g(1,k)$ по теореме 1. Рассмотрим отображение $\mathsf{res}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}$. Прокомментируем, как происходит сужение автоморфизмов поля $\mathbb{Q}(\zeta_n)$ на поле $K\cap\mathbb{Q}(\zeta_n)$ и что есть пересечение $K\cap\mathbb{Q}(\zeta_n)$.

Ответим на первый вопрос, определив сужение кругового поля $\mathbb{Q}(\zeta_n)$ на некоторое числовое поле. Рассмотрим общий случай, когда $n=pq$, где $p,q>0$ — взаимно простые. Тогда автоморфизм σ_a поля $\mathbb{Q}(\zeta_{pq})$ можно связать с действием автоморфизмов полей $\mathbb{Q}(\zeta_p)$ и $\mathbb{Q}(\zeta_q)$ на элементы $\sqrt{-p}$ и $\sqrt{-q}$ следующим образом:

$$\sigma_a(\zeta_{pq})=g(a,pq)=\left(\frac{aq}{p}\right)g(1,p)\left(\frac{ap}{q}\right)g(1,q)=\sigma_{aq}(\sqrt{-p})\sigma_{ap}(\sqrt{-q}).$$

Здесь индекс aq в случае $\sigma_{aq}(\sqrt{-p})$ рассматривается по модулю p, индекс ap в случае $\sigma_{ap}(\sqrt{-q})$ — по модулю q. Более детально все вычисления представлены в п. 2. Ответ на второй вопрос даёт следующая

Лемма 1. Пусть $K=\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_n})$ — мультиквадратичное поле, где $d_1\equiv$ $\equiv d_2\equiv\ldots\equiv d_n\equiv 1 \pmod 4$ и все d_i попарно взаимно просты для $i=1,\ldots,n$; $\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_\ell})$ — круговое поле, где $\zeta_{d_1\cdot\ldots\cdot d_\ell}$ — корень степени $d_1\cdot\ldots\cdot d_\ell$ из единицы и $\ell\leqslant n$. Тогда $K\cap\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_\ell})=\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_\ell})$.

Для упрощения дальнейших вычислений дадим альтернативное определение идеалу Штикельбергера; его эквивалентность исходному определению, обеспечивающая корректность работы алгоритма, представлена в полной версии статьи на `https://crypto-kantiana.com/`. Пусть f — кондуктор поля K, тогда $K\cap\mathbb{Q}(\zeta_n)=K\cap\mathbb{Q}(\zeta_{(f,n)})$ для $n\in\mathbb{N}$. Определение кондуктора числового поля можно посмотреть в [7].

Определение 5. Идеалом Штикельбергера поля K с кондуктором f называется идеал вида $I=I'\cap\mathbb{Z}[G_K]$, где

$$I'=\{\sigma\cdot\theta_n'(-1):n|f,\sigma\in G_K\}\bigcup\left\{\frac{1}{2}N_K\right\}.$$

2. Алгоритм

Рассмотрим алгоритм вычисления идеала Штикельбергера для мнимых мультиквадратичных полей в соответствии с описанной в п. 1 теорией.

Вычисление действия отображения res не тривиально в общем случае, поэтому рассмотрим его более детально. Применим квадратичные гауссовы суммы для вычисления $\mathsf{res}_{\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})/K\cap\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})}\theta_{d_1\cdot\ldots\cdot d_n}(-1)$, где

$$\theta_{d_1\cdot\ldots\cdot d_n}(-1)=\sum_{(a,d_1\cdot\ldots\cdot d_n)=1}\left\langle\frac{a}{d_1\cdot\ldots\cdot d_n}\right\rangle\sigma_a^{-1}. \tag{1}$$

Здесь $\sigma_a\in G_{\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})}$ действуют лишь на элемент $\sqrt{d_1\cdot\ldots\cdot d_n}$. По формуле (1) каждый такой автоморфизм сводится к произведению автоморфизмов полей $\mathbb{Q}(\zeta_{d_1})$,

$\ldots$, $\mathbb{Q}(\zeta_{d_n})$. Рассмотрим каждое слагаемое $\left\langle \dfrac{a}{d_1 \cdot \ldots \cdot d_n} \right\rangle \sigma_a^{-1}$. Введём обозначение $\pi_i = a \prod\limits_{j \neq i} d_j$, тогда

$$\left\langle \frac{a}{d_1 \cdot \ldots \cdot d_n} \right\rangle \sigma_a^{-1}(\zeta_{d_1 \cdot \ldots \cdot d_n}) = \sigma_a(\sqrt{d_1 \cdot \ldots \cdot d_n}) =$$
$$= \left\langle \frac{a}{d_1 \cdot \ldots \cdot d_n} \right\rangle \sigma_{\frac{1}{\pi_1 \bmod d_1} \bmod d_1}(\zeta(d_1)) \cdot \ldots \cdot \sigma_{\frac{1}{\pi_n \bmod d_n} \bmod d_n}(\zeta(d_n)).$$

Если $\frac{1}{\pi_1 \bmod d_1} \bmod d_1$ — квадратичный вычет по модулю d_1, то заменяем $\sigma_{\frac{1}{\pi_1 \bmod d_1} \bmod d_1}(\zeta(d_1))$ на id_1, где $id_1 : \sqrt{d_1} \to \sqrt{d_1}$; в противном случае — на σ_1, где $\sigma_1 : \sqrt{d_1} \to -\sqrt{d_1}$. Аналогично рассуждаем для остальных множителей.

Полученные композиции автоморфизмов переобозначим следующим образом:

$$\begin{gathered} id_1 \cdot id_2 \cdot \ldots \cdot id_n = id : \sqrt{d_1} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_n}, \\ \ldots \\ \sigma_1 \cdot \ldots \cdot \sigma_{n-1} \cdot \sigma_n = \tau_m : \sqrt{d_1} + \ldots + \sqrt{d_{n-1}} + \sqrt{d_n} \to -\sqrt{d_1} - \ldots - \sqrt{d_n}. \end{gathered} \tag{2}$$

Очевидно, что общее количество получившихся композиций автоморфизмов равно 2^n. Поскольку первый автоморфизм обозначен id, то $m = 2^n - 1$. Процедура вычисления res представлена в алгоритме 1.

Алгоритм 1. Вычисление $\mathsf{res}(\theta_n(-1))$

Вход: $K = \mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})$.
Выход: $\mathsf{res}(\theta_n(-1))$.

1: $f := \prod\limits_{j=1}^{k} d'_j$. // f — *кондуктор* K
2: **Для** $a \in \mathbb{Z}_f^*$
3: **Для** $j = 1, \ldots, k$
4: $t := \dfrac{a \cdot d'_1 \cdot \ldots \cdot d'_k}{d'_j} \bmod d'_j$;
5: $index := \dfrac{1}{t} \bmod d'_j$.
6: **Если** $\left(\dfrac{index}{d'_j}\right) = 1$, **то**
7: $\sigma_a^{-1} := \sigma_a^{-1} \cdot id_j$, // id_j — *тождественный в* $\mathbb{Q}(\sqrt{d'_j})$
8: **иначе Если** $\left(\dfrac{index}{d'_j}\right) = -1$, **то**
9: $\sigma_a^{-1} := \sigma_a^{-1} \cdot \sigma_j$; // σ_j — *сопряжение в* $\mathbb{Q}(\sqrt{d'_j})$
10: $\sigma_a^{-1} := \dfrac{a}{f} \cdot \sigma_a^{-1}$;
11: $\theta := \sum\limits_{a \in \mathbb{Z}_f^*} \sigma_a^{-1}$;
12: res: заменить получившиеся комбинации автоморфизмов в каждом слагаемом θ на соответствующие τ_i в соответствии с формулами (2).
13: **Вернуть** res.

Вычисление cor**.** Автоморфизмы, полученные после вычисления res, являются автоморфизмами поля $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n})$. Вычисление действия отображения cor представляет собой переход от этих автоморфизмов к автоморфизмам поля K. Обозначим автоморфизмы поля K следующим образом: сопоставим действие автоморфизма ρ_i с бинарным вектором из $\mathbb{Z}_2^n$, причём если i-я координата вектора (считая слева направо) есть 1, то $\rho_i : \sqrt{d_i} \to -\sqrt{d_i}$ (например, $\rho_1 : \sqrt{d_1} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \ldots - \sqrt{d_n}$).

Если $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n}) = K$, то отображение cor действует тождественно (полученные автоморфизмы τ_i совпадают с ρ_i). Такой случай возникает при вычислении $\theta'_{d_1 \cdot \ldots \cdot d_n}(-1)$. А как быть, если мы вычисляем, например, элемент Штикельбергера вида $\theta'_{d_1 \cdot \ldots \cdot d_\ell}(-1)$, где $\ell < n$? Рассмотрим случай, когда $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell}) = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$. Результатом действия отображения res в этом случае является

$$a_1 \cdot id_l + a_2 \cdot \tau_1 + \ldots + a_{2^l-1} \cdot \tau_{2^l-2} + a_{2^l} \cdot \tau_{2^l-1},$$

где id_l, τ_i — автоморфизмы поля $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$, $i = 1, \ldots, 2^l - 1$. Нумерация автоморфизмов τ_i аналогична нумерации автоморфизмов ρ_i.

Далее переходим от перечисленных автоморфизмов поля $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$ к автоморфизмам ρ_i поля K. Если ρ_i относительно элемента $\sqrt{d_1} + \ldots + \sqrt{d_l}$ действует как id_l, то все такие автоморфизмы ρ_i участвуют в записи элемента Штикельбергера с коэффициентом a_1. Аналогично, если ρ_i относительно $\sqrt{d_1} + \ldots + \sqrt{d_l}$ действует как τ_1, то все такие автоморфизмы ρ_i участвуют в записи элемента Штикельбергера с коэффициентом a_2. Применяя такой подход для всех остальных случаев, получаем

$$\theta'_{d_1 \cdot \ldots \cdot d_\ell}(-1) = a_1 \cdot id + a_1 \cdot \rho_1 + \ldots + a_{2^l} \cdot \rho_{m-1} + a_{2^l} \cdot \rho_m.$$

Таким образом, в общем случае элемент Штикельбергера примет вид

$$\theta'_n(-1) = c_0 \cdot id + c_1 \cdot \rho_1 + \ldots + c_{m-1} \cdot \rho_{m-1} + c_m \cdot \rho_m,$$

где $c_i \in \mathbb{Z}$ для $i = 0, \ldots, m$ и $m = 2^n - 1$.

Очевидно, что общее количество элементов Штикельбергера в поле K равно $2^n - 1$ (по количеству всех возможных подполей). Таким образом, необходимо умножить 2^n автоморфизов на каждый из $2^n - 1$ элементов Штикельбергера.

Количество различных комбинаций зависит от количества различных коэффициентов в элементе Штикельбергера. Будем записывать все различные комбинации в множество I'; общее количество различных элементов для мультиквадратичного поля будет равно $\#I'$. В результате получим следующий результат:

$$I = s_1 \cdot \theta_1 + \ldots + s_{\#I'} \cdot \theta_{\#I'} = \sum_{i=1}^{\#I'} s_i \cdot \theta_i, \quad s_i \in \mathbb{Z}.$$

Описанные действия представлены в алгоритме 2.

Алгоритм 2. Вычисление идеала Штикельбергера

Вход: $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$.
Выход: $I = I' \cap \mathbb{Z}[Gal(K/\mathbb{Q})]$.

1: Построить массив A, состоящий из всех подполей K.
2: **Для** $i = 1, \ldots, 2^n - 1$:
3: $\quad \mathsf{res}_i := \mathsf{res}_{\mathbb{Q}(\zeta_{d'_1 \cdot \ldots \cdot d'_k})/\mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})} \theta_i$; // алгоритм 1, вход: $A[i]$
4: $\quad \theta'_i := \mathsf{cor}_{K/\mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})} \mathsf{res}_i$;
5: $I' - \varnothing$;
6: **Для** $i = 1, \ldots, 2^n - 1$
7: $\quad$ **Для** $j = 1, \ldots, 2^n$
8: $\quad\quad t := \rho_j \cdot \theta'_i$; $I' := A \cup t$;
9: $I := \prod_{i=1}^{\#I'} s_i \cdot I'_i$.
10: **Вернуть** I.

Лемма 2. Пусть $d = \max\limits_i d_i$. Тогда вычислительная сложность алгоритма 2 равна

$$\mathcal{O}(e^{n \log n} \cdot 2^{2n} \cdot n^4 \cdot \log^3 d \cdot \log^3 n).$$

ЛИТЕРАТУРА

1. *Cramer R., Ducas L., and Wesolowski B.* Short Stickelberger class relations and application to ideal-SVP // Advances in Cryptology — Eucrocrypt 2017. Springer, 2017. P. 324–348.
2. *Bauch J., Bernstein D. J., de Valence H., et al.* Short generators without quantum computers: The case of multiquadratics // Advances in Cryptology — EUROCRYPT 2017. Springer, 2017. P. 27–59.
3. *Biasse J.-F. and Vredendaal C.* Fast multiquadratic S-unit computation and application to the calculation of class groups // Open Book Series. 2019. V. 2. P. 103–118.
4. *Kucera R.* On the Stickelberger ideal and circular units of a compositum of quadratic fields // J. Number Theory. 1996. V. 56. No. 1. P. 139–166.
5. *Sinnott W.* On the Stickelberger ideal and the circular units of an Abelian field // Invent. Math. 1980. V. 62. P. 181–234.
6. *Berndt B. C., Evans R. J., and Williams K. S.* Topics in Commutative Ring Theory. N.Y.: Wiley, 1998.
7. *Cohen H. and Stevenhagen P.* Computational Class Field Theory. 2008. `https://arxiv.org/pdf/0802.3843.pdf`