2011 Теоретические основы прикладной дискретной математики №3(13)
DOI 10.17223/20710410/13/3
УДК 511.2

МЕТОД КОМПЛЕКСНОГО УМНОЖЕНИЯ ДЛЯ ПОСТРОЕНИЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ И ЕГО ОПТИМИЗАЦИИ[1]

Е. А. Гречников

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: grechnik@mccme.ru

Для построения эллиптических кривых над конечными полями с предписанными требованиями к их порядку используется метод комплексного умножения. В этом методе на этапе, требующем больше всего времени, вычисляется некоторый многочлен с целыми коэффициентами. В работе доказаны необходимые теоретические результаты и подробно описано, каким образом в методе комплексного умножения можно использовать делитель этого многочлена с коэффициентами в некотором расширении поля рациональных чисел.

Ключевые слова: *эллиптические кривые, конечные поля, метод комплексного умножения, совместные приближения.*

Введение

В последнее время эллиптические кривые играют важную роль в разнообразных приложениях, в числе которых можно назвать криптосистемы с открытым ключом [1, 2], алгоритмы разложения на множители [3] и проверки простоты [4] целых чисел. Для этих приложений необходимы эллиптические кривые над конечными полями, порядок которых удовлетворяет определённым ограничениям. Так, для криптографических применений желательно, чтобы порядок кривой был простым числом или, по крайней мере, имел по возможности больший простой делитель.

Один из методов построения эллиптических кривых с заданными условиями на порядок кривой заключается в следующем. Будем случайным образом генерировать коэффициенты уравнения, задающего кривую. Для каждого сгенерированного уравнения вычислим порядок соответствующей кривой и проверим, удовлетворяет ли он нужным условиям; если нет, перейдём к следующей кривой. Распределение значений порядка кривой при таком подходе оказывается приблизительно равномерным, строгое утверждение для случая простого поля характеристики, большей 3, можно найти в [3]. К сожалению, сложность алгоритма подсчёта порядка кривой растёт хоть и полиномиально, но достаточно быстро.

Теория комплексного умножения предоставляет другой, более практичный метод создания кривой с заданными ограничениями на порядок. Здесь сначала подбирается порядок кривой, удовлетворяющий нужным ограничениям, после чего строится кривая с заданным порядком. В п. 1 описываются детали метода и некоторые известные его оптимизации.

Предлагается новый способ оптимизации вычислений. Для его изложения понадобятся теоретические результаты, доказанные в п. 2 и 3. В п. 4 описан предлагаемый подход, в п. 5, 6 и 7 — его детали.

[1]Работа поддержана грантом РФФИ № 11-01-12098.

1. Метод комплексного умножения

1.1. Теоретические основы

Будем везде считать, что $D \in \mathbb{Z}$ такое, что

$$D < 0 \text{ и либо } D \equiv 0 \pmod 4, \text{ либо } D \equiv 1 \pmod 4. \tag{1}$$

Рассмотрим поле $K = \mathbb{Q}(\sqrt{D})$; его дискриминант обозначим через d. Тогда $d < 0$ и

— либо

$$d \equiv 1 \pmod 4 \text{ и } d \text{ свободно от квадратов}, \tag{2}$$

— либо

$$d \equiv 0 \pmod 4, \qquad \frac{d}{4} \text{ свободно от квадратов}, \qquad \frac{d}{4} \not\equiv 1 \pmod 4. \tag{3}$$

Кроме того, $D = f^2 d$, где $f \in \mathbb{N}$. Обозначим через $\mathcal{O} = \mathbb{Z}\left[(d+\sqrt{d})/2\right]$ кольцо целых поля K и через $\mathcal{O}_D = \mathbb{Z}\left[(D+\sqrt{D})/2\right]$ порядок в $\mathcal{O}$ кондуктора f. Если M — произвольное числовое поле, то через $\mathcal{O}_M$ будем обозначать кольцо целых этого поля; так, $\mathcal{O}_K = \mathcal{O}$.

Дробным идеалом порядка $\mathcal{O}_D$ будем называть подмножество K, являющееся конечно порождённым $\mathcal{O}_D$-модулем и содержащее ненулевой элемент; целым идеалом или просто идеалом $\mathcal{O}_D$ — дробный идеал, содержащийся в $\mathcal{O}_D$ (что совпадает с обычным определением идеала кольца с исключением нулевого идеала). Собственным (дробным) идеалом порядка $\mathcal{O}_D$ будем называть (дробный) идеал $\mathfrak{a}$, такой, что $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_D$. Все собственные дробные идеалы порядка $\mathcal{O}_D$ образуют абелеву группу относительно операции умножения идеалов [5, §7], которую будем обозначать $I(\mathcal{O}_D)$. Легко видеть, что главные дробные идеалы, т. е. множества вида $\alpha\mathcal{O}_D$ с $\alpha \in K^*$, образуют подгруппу в $I(\mathcal{O}_D)$, которую будем обозначать $P(\mathcal{O}_D)$. Будем называть эквивалентными идеалы, отличающиеся умножением на главный дробный идеал; запись $\mathfrak{a} \sim \mathfrak{b}$ будет обозначать эквивалентность дробных идеалов $\mathfrak{a}$ и $\mathfrak{b}$. Будем для краткости называть класс эквивалентных собственных дробных идеалов просто классом идеалов. Поскольку $P(\mathcal{O}_D)$ — подгруппа, то классы идеалов образуют фактор-группу $\mathcal{H}_D = I(\mathcal{O}_D)/P(\mathcal{O}_D)$. Она называется группой классов идеалов и является конечной абелевой группой [5, §7]. Поскольку $\mathcal{O}_D$ и K инвариантны относительно комплексного сопряжения, то комплексное сопряжение дробного идеала как множества само является дробным идеалом; операция комплексного сопряжения идеалов индуцирует корректно определённую операцию на $\mathcal{H}_D$.

Квадратичной формой назовём выражение вида $Ax^2 + Bxy + Cy^2$, где $A, B, C \in \mathbb{Z}$. Будем также обозначать такие выражения тройками (A, B, C). Дискриминантом квадратичной формы назовём величину $B^2 - 4AC$, две формы назовём эквивалентными, если одна переходит в другую заменой переменных (x, y) с целочисленной матрицей определителя 1. Назовём квадратичную форму положительно определённой, если её дискриминант отрицателен и $A > 0$, и примитивной, если $\gcd(A, B, C) = 1$. Далее будем рассматривать только примитивные положительно определённые квадратичные формы дискриминанта D, для краткости не оговаривая этого явно. Корнем формы будем называть (единственный) корень τ уравнения $A\tau^2 + B\tau + C = 0$, лежащий в верхней комплексной полуплоскости $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$, т. е. $\tau = \dfrac{-B+\sqrt{D}}{2A} \in K \cap \mathbb{H}$. Приведённой формой назовём такую форму, что $|B| \leqslant A \leqslant C$, и если $B < 0$, то $|B| < A < C$. Каждая форма эквивалентна ровно одной приведённой форме [5, Theorem 2.8].

Элементы группы $\mathcal{H}_D$ находятся во взаимно-однозначном соответствии с приведёнными формами, которое будем обозначать буквой $\mathfrak{h}$, а именно [5, Theorem 7.7]: форме $\xi = (A, B, C)$ с корнем τ можно сопоставить класс $\mathfrak{h}(\xi) = \mathfrak{h}(A, B, C)$ идеалов $\mathcal{O}_D$, содержащий $\langle 1, \tau \rangle_{\mathbb{Z}}$ (который является собственным дробным идеалом $\mathcal{O}_D$), причём эквивалентным формам будет сопоставлен один и тот же класс.

Все приведённые формы легко перечислить: нетрудно видеть, что для такой формы справедливы неравенства $|B| \leqslant A \leqslant \sqrt{|D|/3}$ и при фиксированных A, B существует не более одного варианта для C. Это делает приведённые формы удобным способом задания элементов $\mathcal{H}_D$.

Наряду с классическим определением модулярного инварианта j как функции на верхней полуплоскости $\mathbb{H}$ [6, §46] можно также определить j-инвариант решётки в $\mathbb{C}$ [5, §10], не меняющийся при умножении решётки на любое ненулевое комплексное число, так, что при $\tau \in \mathbb{H}$ выполнено равенство $j(\tau) = j\left(\langle 1, \tau \rangle_{\mathbb{Z}}\right)$. Если $\mathfrak{a}$ — собственный дробный идеал $\mathcal{O}_D$, то он является решёткой в $\mathbb{C}$. При этом умножение идеала $\mathfrak{a}$ на главный идеал приводит к умножению решётки на элемент из K^*; следовательно, значение $j(\mathfrak{a})$ зависит только от класса идеала $\mathfrak{a}$. С вычислительной точки зрения если дробный идеал $\mathfrak{a}$ принадлежит классу, заданному формой $Ax^2 + Bxy + Cy^2$ с корнем τ, то есть $\mathfrak{a} \sim \langle 1, \tau \rangle_{\mathbb{Z}}$, то $j(\mathfrak{a}) = j(\tau)$.

Для любой эллиптической кривой при $n \in \mathbb{Z}$ определим отображение $[n]$, переводящее точку P в точку nP. В частности, отображение $[1]$ — тождественное. Изогенией двух эллиптических кривых будем называть морфизм (в смысле алгебраической геометрии), переводящий бесконечно удалённую точку одной кривой в бесконечно удалённую точку другой, эндоморфизмом эллиптической кривой будем называть изогению в себя. При любом $n \in \mathbb{Z}$ отображение $[n]$ является эндоморфизмом эллиптической кривой [7, Example III.4.1] и коммутирует с любым другим эндоморфизмом (поскольку любая изогения эллиптических кривых является гомоморфизмом групп точек в силу [7, Theorem III.4.8]); кольцо эндоморфизмов эллиптической кривой является $\mathbb{Z}$-модулем относительно действия $n\varphi = [n] \circ \varphi$, где $n \in \mathbb{Z}$, φ — эндоморфизм. Эндоморфизмы $\{[n] : n \in \mathbb{Z}\}$ образуют кольцо, изоморфное $\mathbb{Z}$ [7, Proposition III.4.2].

Кольцо эндоморфизмов эллиптической кривой над $\mathbb{C}$ либо совпадает с $\{[n] : n \in \mathbb{Z}\}$, либо изоморфно порядку в некотором мнимоквадратичном поле [7, Corollary III.9.4 и Exercise 3.18b]. В последнем случае говорят, что кривая имеет комплексное умножение на этот порядок. Есть ровно $|\mathcal{H}_D|$ неизоморфных эллиптических кривых с умножением на $\mathcal{O}_D$ [7, Proposition C.11.1], эти кривые характеризуются тем, что их j-инвариант совпадает со значением модулярного инварианта $j(\mathfrak{a})$, вычисленного на представителях классов идеалов $\mathcal{O}_D$. Эти значения называются сингулярными значениями. Любое такое значение генерирует над K одно и то же поле $L = L(D) = K(j(\mathfrak{a}))$, называемое полем классов кольца $\mathcal{O}_D$ (*ring class field*) [5, Theorem 11.1]. Группа Галуа расширения L/K изоморфна группе $\mathcal{H}_D$ [5, §9]. Канонический изоморфизм, который будем обозначать Ω, сопоставляет классу идеалов с представителем $\mathfrak{b}$ автоморфизм, переводящий $j(\mathfrak{a})$ в $j(\mathfrak{a}\mathfrak{b}^{-1})$ [5, Corollary 11.37]. Комплексное сопряжение действует следующим образом: $\overline{j(\mathfrak{a})} = j(\overline{\mathfrak{a}})$ по определению j [5, §10], $\mathfrak{a}\overline{\mathfrak{a}} \sim \mathcal{O}_D$ [5, (7.6)], следовательно, $\overline{j(\mathfrak{a})} = j(\mathfrak{a}^{-1})$.

Рассмотрим многочлен $H_D[j](x) = \prod_{i=1}^{h} (x - j(\mathfrak{a}_i))$, где $h = |\mathcal{H}_D|$ и $\mathfrak{a}_i$ — представители всех классов идеалов. Его коэффициенты лежат в L, инвариантны относительно действия $\mathrm{Gal}(L/K)$ и комплексного сопряжения, то есть лежат в $\mathbb{Q}$. Более того, $j(\mathfrak{a}_i)$ — целые алгебраические числа [5, Theorem 11.1], так что $H_D[j](x) \in \mathbb{Z}[x]$.

Пусть p простое, n натуральное, $q = p^n$, эллиптическая кривая E определена над конечным полем $\mathbb{F}_q$. Под точками и эндоморфизмами кривой E при отсутствии явного указания основного поля будем понимать $\overline{\mathbb{F}}_q$-точки и эндоморфизмы над $\overline{\mathbb{F}}_q$. Под порядком кривой будем понимать число $\mathbb{F}_q$-точек. Кольцо эндоморфизмов $\mathrm{End}(E)$ изоморфно либо порядку в некотором мнимоквадратичном поле, либо порядку в некоторой алгебре кватернионов над $\mathbb{Q}$ [7, Corollary III.9.4 и Theorem V.3.1]. В последнем случае кривая E называется суперсингулярной, и такие кривые нас интересовать не будут. В первом случае $\mathrm{End}(E) \cong \mathcal{O}_D$ для некоторого D, удовлетворяющего (1); $\mathrm{End}(E) = \langle [1], \alpha \rangle_{\mathbb{Z}}$, где α — некоторый эндоморфизм кривой E. Оказывается [8, Теорема 13.14], что кривая вместе с эндоморфизмом α может быть «поднята» в $\mathbb{C}$ в следующем смысле: существует числовое поле L', кривая E', определённая над ним, эндоморфизм α' кривой E', идеал $\mathfrak{B}' \subset \mathcal{O}_{L'}$, лежащий над p (то есть $\mathfrak{B}' \cap \mathbb{Z} = p\mathbb{Z}$), и редукция E' по модулю $\mathfrak{B}'$, изоморфная E, причём при этой редукции α' переходит в α. Поскольку $\alpha \notin \{[n] : n \in \mathbb{Z}\}$, то и $\alpha' \notin \{[n] : n \in \mathbb{Z}\}$, так что $\mathrm{End}(E') \supsetneq \mathbb{Z}$ и E' обладает комплексным умножением на некоторый порядок в некотором мнимоквадратичном поле. Согласно свойствам редукции [8, Теорема 13.12], она индуцирует изоморфизм $\mathrm{End}(E')$ с подкольцом в $\mathrm{End}(E)$. Поскольку редукция α' есть α, то $\mathrm{End}(E') \cong \mathrm{End}(E) \cong \mathcal{O}_D$.

В $\mathrm{End}(E)$ есть эндоморфизм Фробениуса $Fr : (x, y) \mapsto (x^q, y^q)$ и дуальный к нему эндоморфизм $\widehat{Fr}$, причём $Fr \circ \widehat{Fr} = [q]$ [7, Theorem III.6.2 и Proposition 2.11] и $[|E(\mathbb{F}_q)|] = [|\operatorname{Ker}([1] - Fr)|] = ([1] - Fr) \circ ([1] - \widehat{Fr})$ (первое равенство следует из того, что Fr оставляет неподвижными точки $\mathbb{F}_q$ и только их, второе — [7, Theorem III.4.10, Corollary III.5.5, Theorem III.6.2]). Обозначим элемент $\mathcal{O}_D \cong \mathrm{End}(E)$, соответствующий Fr, через π, а элемент, соответствующий $\widehat{Fr}$, через $\overline{\pi}$; тогда $\pi\overline{\pi} = q$ и $(1-\pi)(1-\overline{\pi}) = |E(\mathbb{F}_q)|$. В частности, при $\pi \notin \mathbb{R}$ из этих равенств легко видеть, что $\overline{\pi}$ — действительно комплексное сопряжение к π; если $\pi \in \mathbb{R}$, то $\pi \in \mathbb{R} \cap \mathcal{O}_D = \mathbb{Z}$, следовательно, $Fr = [\pi]$, а в таком случае $\widehat{Fr} = Fr$ [7, Theorem III.6.2], так что и в этом случае $\overline{\pi}$ совпадает с комплексным сопряжением к π.

Поскольку $\pi \in \mathcal{O}_D$, то существуют $u, v \in \mathbb{Z}$, такие, что $\pi = (u + v\sqrt{D})/2$. Тогда $\overline{\pi} = (u - v\sqrt{D})/2$ и $q = \pi\overline{\pi} = (u^2 - Dv^2)/4$, т. е. $4q = u^2 + |D|v^2$. Порядок кривой E при этом равен $1 - \pi - \overline{\pi} + \pi\overline{\pi} = q + 1 - u$; в силу [7, Exercise 5.10] из несуперсингулярности следует, что $(q, u) = 1$.

Подытожим вышесказанное: если E — несуперсингулярная эллиптическая кривая над $\mathbb{F}_q$, то найдутся число D, числовое поле L' и кривая E' над ним, такие, что

— E' обладает комплексным умножением на $\mathcal{O}_D$;
— существует редукция E', изоморфная E;
— порядок E равен $q + 1 - u$, где $u \in \mathbb{Z}$ такое, что для некоторого $v \in \mathbb{Z}$ выполнено равенство $4q = u^2 + |D|v^2$.

1.2. Базовый алгоритм

Для построения таких кривых E реализуем следующую схему, подробности которой будут описаны позже:

1) Выберем числа $q = p^n$, p простое, и $\hat{u}, \hat{v}, D \in \mathbb{Z}$ так, чтобы D удовлетворяло (1) и выполнялись следующие условия:

$$4q = \hat{u}^2 + |D|\hat{v}^2; \tag{4}$$

$$\gcd(\hat{u}, q) = 1, \tag{5}$$

а также чтобы порядок поля q и порядок будущей кривой $q+1-\hat{u}$ удовлетворяли условиям, нужным для конкретных приложений.

2) Вычислим многочлен $H_D[j](x)$.
3) Редуцируем многочлен $H_D[j](x)$ по модулю p; получим некоторый многочлен над $\mathbb{F}_p \subset \mathbb{F}_q$, который, как будет показано, разлагается на линейные множители над $\mathbb{F}_q$. Вычислим какой-нибудь из его корней и построим эллиптическую кривую E'' над $\mathbb{F}_q$ с j-инвариантом, равным вычисленному корню.
4) Кривая E'' обладает комплексным умножением на $\mathcal{O}_D$. Изоморфизм не меняет кольца комплексного умножения, но может изменить число $\mathbb{F}_q$-точек. В дальнейшем будет показано, как построить кривую, изоморфную E'', с числом точек $q + 1 - \hat{u}$.

Под $\left(\frac{a}{p}\right)$, где $a \in \mathbb{Z}$, p — простое, будем понимать символ Кронекера, который при нечётном p равен символу Лежандра, а при $p = 2$ определён только в случае $a \equiv 0, 1 \pmod 4$ и равен

$$\left(\frac{a}{2}\right) = \begin{cases} 1, & \text{если } a \equiv 1 \pmod 8, \\ -1, & \text{если } a \equiv 5 \pmod 8, \\ 0, & \text{если } a \equiv 0 \pmod 4. \end{cases}$$

При $b \in \mathbb{N}$ символ Кронекера $\left(\frac{a}{b}\right)$ определим по мультипликативности.

Условия (4) и (5) накладывают довольно сильные ограничения на q и p. В частности, справедлива следующая лемма.

Лемма 1. Пусть $d < 0$ удовлетворяет условию (2) или (3), $D = df^2$. Пусть для $q = p^n$ и некоторых целых u, v выполнены условия $4q = u^2 + |D|v^2$, $\gcd(q, u) = 1$. Тогда справедливы следующие утверждения:

1)
$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = 1; \tag{6}$$

2) $p \nmid f$;
3) $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$, где $\mathfrak{p} \neq \overline{\mathfrak{p}}$ — простые идеалы $\mathcal{O}$;
4) $\dfrac{u + v\sqrt{D}}{2} \in \mathcal{O}_D$;
5) $\dfrac{u + v\sqrt{D}}{2}\mathcal{O} = \mathfrak{p}^n$ или $\dfrac{u + v\sqrt{D}}{2}\mathcal{O} = \overline{\mathfrak{p}}^n$.

Доказательство. Из равенства $4q = u^2 + |D|v^2$ и условия $p \nmid u$ легко видеть, что $p \nmid D$ и $p \nmid \hat{v}$; кроме того, редукция равенства по модулю p даёт $u^2 - Dv^2 \equiv \equiv 0 \pmod p$, откуда $D \equiv (uv^{-1})^2 \pmod p$. Для доказательства первого утверждения остаётся заметить, что $D = df^2$.

Второе утверждение очевидным образом следует из $p \nmid D$.

Третье утверждение следует из первого в силу хорошо известного факта из теории квадратичных полей (например, [9, Предложения 13.1.3 и 13.1.4]).

Для доказательства четвёртого утверждения рассмотрим по модулю 2 равенство $4q = u^2 + |D|v^2$. Если D чётно, то u чётно, $\mathcal{O}_D = \mathbb{Z}\left[(D + \sqrt{D})/2\right] = \mathbb{Z}\left[(\sqrt{D})/2\right]$ и $(u + v\sqrt{D})/2 = u/2 + v\sqrt{D}/2 \in \mathcal{O}_D$. Если же D нечётно, то $u \equiv v \pmod 2$, $\mathcal{O}_D = \mathbb{Z}\left[(D + \sqrt{D})/2\right] = \mathbb{Z}\left[(1 + \sqrt{D})/2\right]$ и $(u + v\sqrt{D})/2 = (u - v)/2 + v(1 + \sqrt{D})/2 \in \mathcal{O}_D$.

Заметим, что $\frac{u+v\sqrt{D}}{2}\mathcal{O} \cdot \frac{u-v\sqrt{D}}{2}\mathcal{O} = q\mathcal{O} = p^n\mathcal{O} = \mathfrak{p}^n\overline{\mathfrak{p}}^n$. Поскольку $p \nmid u$, то $\mathfrak{p}\overline{\mathfrak{p}} = p\mathcal{O} \nmid \frac{u \pm v\sqrt{D}}{2}\mathcal{O}$. Теперь последнее утверждение следует из единственности разложения на простые идеалы в кольце $\mathcal{O}$. ■

Перейдём к вопросам реализации.

Действия на первом этапе зависят от требований к q и порядку кривой.

Если q фиксировано, то будем осуществлять перебор целых D, удовлетворяющих (1). Для каждого D сначала проверим необходимое условие (6); если оно нарушено, перейдём к следующему D. Пусть D удовлетворяет (6). Применим алгоритм Корначиа [10], который решает уравнение $x^2 + |D|y^2 = m$, при $m = 4q$. Если решения не существует, перейдём к следующему D. Если решение найдено, то проверим, удовлетворяет ли $q + 1 \pm x$ требованиям на порядок кривой.

Если же q не фиксировано, то вместо метода, описанного в предыдущем абзаце, эффективнее фиксировать D, удовлетворяющее (1), после чего случайным образом выбирать $\hat{u}, \hat{v}$, вычислять q из (4) и $q + 1 \pm \hat{u}$ и проверять, что они удовлетворяют нужным условиям. В [11] и [12] предлагаются улучшения этого метода, по существу заключающиеся в том, что если указанные параметры выбирать не совсем случайно, то можно гарантировать отсутствие (или снизить вероятность существования) малых простых делителей у $q = (\hat{u}^2 + |D|\hat{v}^2)/4$ и $q+1 \pm \hat{u}$. Так, если ограничиться нечётным p и требованием нечётности и простоты одного из чисел $q + 1 \pm u$ (как это делает [12]), то легко видеть, что $D \equiv 5 \pmod 8$, $\hat{u}$ и $\hat{v}$ должны быть нечётными; в [12] предлагается начать с $\hat{u} = 210\hat{u}_0 + 1$, $\hat{v} = 210\hat{v}_0 + 105$, $\hat{u}_0, \hat{v}_0$ — случайным образом выбранные натуральные числа, после чего (если выбранные $\hat{u}$ и $\hat{v}$ не подошли) прибавлять к $\hat{u}$ попеременно 106 и $104 = 210 - 106$. Заметим, что $210 = 105 \cdot 2 = 2 \cdot 3 \cdot 5 \cdot 7$. При таком выборе $(\hat{u}^2+|D|\hat{v}^2)/4$ и одно из $q+1\pm u$ не делится на 2, 3, 5, 7. Метод из [11] использует больше малых простых делителей и более громоздкий, поэтому здесь не приводится. Сравнение производительности методов есть в [12].

На втором этапе вычисляем многочлен $H_D[j](x)$. Для этого перечислим все $h = |\mathcal{H}_D|$ приведённых форм, вычислим их корни $\tau_1, \ldots, \tau_h$, найдём с достаточно высокой точностью значения $j(\tau_1), \ldots, j(\tau_h)$ как комплексные числа. По ним приближённо вычислим коэффициенты многочлена $H_D[j](x)$. Если точность вычислений такова, что погрешность в коэффициентах меньше 0,5, то коэффициенты, являющиеся целыми числами, могут быть однозначно восстановлены по вычисленным приближениям.

Если M — числовое поле, $\mathfrak{C} \subset \mathcal{O}_M$ — простой идеал, $z \in \mathcal{O}_M$, то через $R_{\mathfrak{C}}(z)$ будем обозначать редукцию z по модулю идеала $\mathfrak{C}$ (таким образом, $R_{\mathfrak{C}}$ — отображение из $\mathcal{O}_M$ в конечное поле). Отображение $R_{\mathfrak{C}}$ также действует на многочленах из $\mathcal{O}_M[x]$ покоэффициентно.

Для реализации третьего этапа надо показать, что многочлен $R_{p\mathbb{Z}}(H_D[j](x))$ разлагается на линейные множители над $\mathbb{F}_q$, а также построить эллиптическую кривую по её j-инварианту.

По лемме 1 $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$. Пусть $\mathfrak{B} \subset \mathcal{O}_L$ — простой идеал, лежащий над $\mathfrak{p}$. Поскольку $\mathfrak{B} \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, то

$$R_{p\mathbb{Z}}(H_D[j](x)) = R_{\mathfrak{B}}(H_D[j](x)) = \prod_{i=1}^{h}(x - R_{\mathfrak{B}}(j(\mathfrak{a}_i))) \tag{7}$$

и многочлен $R_{p\mathbb{Z}}(H_D[j](x))$ раскладывается на линейные множители над полем $\mathcal{O}_L/\mathfrak{B}$. Таким образом, остаётся доказать следующую теорему.

Теорема 1.

$$\mathcal{O}_L/\mathfrak{B} \subset \mathbb{F}_q. \tag{8}$$

Доказательство. Через $\left(\frac{L/K}{\mathfrak{C}}\right)$, где $\mathfrak{C}$ — простой идеал $\mathcal{O}_L$, лежащий над простым идеалом $\mathfrak{c} \subset \mathcal{O}$, неразветвлённым в L, будем обозначать символ Артина [5, §5] (который определён для любого расширения Галуа $K \subset L$, но здесь понадобится только для конкретных полей K и L, определённых выше), а именно такой единственный ([5, Lemma 5.19]) элемент $\sigma \in \mathrm{Gal}(L/K)$, что $\sigma(\alpha) \equiv \alpha^{Norm(\mathfrak{c})} \pmod{\mathfrak{C}}$ для любого $\alpha \in \mathcal{O}_L$. Поскольку $\mathrm{Gal}(L/K) \cong \mathcal{H}_D$ абелева, то символ Артина зависит только от $\mathfrak{c}$ [5, Corollary 5.21] и для него правомерно обозначение $\left(\frac{L/K}{\mathfrak{c}}\right)$. Если $\mathfrak{b} = \mathfrak{c}_1^{s_1} \dots \mathfrak{c}_k^{s_k}$ — дробный идеал $\mathcal{O}$ и все $\mathfrak{c}_i$ — простые, неразветвлённые в L, то определим $\left(\frac{L/K}{\mathfrak{b}}\right) = \left(\frac{L/K}{\mathfrak{c}_1}\right)^{s_1} \cdot \ldots \cdot \left(\frac{L/K}{\mathfrak{c}_k}\right)^{s_k}$. Отображение $\left(\frac{L/K}{\cdot}\right)$ задаёт гомоморфизм из группы таких дробных идеалов $\mathcal{O}$, в разложение которых на простые не входят простые идеалы, разветвлённые в L, в группу $\mathrm{Gal}(L/K)$. Этот гомоморфизм называется отображением Артина.

Через $P_{K,\mathbb{Z}}(f)$ [5, §9] будем обозначать подгруппу дробных идеалов $\mathcal{O}$, порождённую главными идеалами вида $\alpha\mathcal{O}$, $\alpha \in \mathcal{O}$, $\alpha \equiv a \pmod{f\mathcal{O}}$ для некоторого $a \in \mathbb{Z}$, $\gcd(a, f) = 1$. Согласно [5, §9], поле L классов кольца $\mathcal{O}_D$ — это единственное абелево расширение K, такое, что

— все простые идеалы $\mathcal{O}$, разветвлённые в L, делят $f\mathcal{O}$ (и, следовательно, все идеалы из $P_{K,\mathbb{Z}}(f)$ неразветвлены в L: если $\alpha \equiv a \pmod{f\mathcal{O}}$, то $\gcd(\alpha\mathcal{O}, f\mathcal{O}) = \gcd(a\mathcal{O}, f\mathcal{O}) = \gcd(a, f)\mathcal{O} = \mathcal{O}$, так что идеал $\alpha\mathcal{O}$ взаимно прост с $f\mathcal{O}$);
— ядро отображения Артина есть группа $P_{K,\mathbb{Z}}(f)$.

Положим $\hat{\pi} = (\hat{u} + \hat{v}\sqrt{D})/2$; из леммы 1 следует, что либо $\mathfrak{p}^n = \hat{\pi}\mathcal{O}$, либо $\mathfrak{p}^n = \overline{\hat{\pi}}\mathcal{O}$. В обоих случаях идеал $\mathfrak{p}^n$ главный и лежит в $P_{K,\mathbb{Z}}(f)$ (поскольку $\hat{\pi} = (\hat{u} + \hat{v}\sqrt{D})/2 \equiv \equiv (\hat{u} - f\hat{v}d)/2 \pmod{f\mathcal{O}}$, $\overline{\hat{\pi}} = (\hat{u} - \hat{v}\sqrt{D})/2 \equiv (\hat{u} + f\hat{v}d)/2 \pmod{f\mathcal{O}}$, по определению $P_{K,\mathbb{Z}}(f)$, лемме 1 и равенству (4)), следовательно, лежит в ядре отображения Артина. Отсюда получаем, что $\left(\frac{L/K}{\mathfrak{p}}\right)^n = Id$. Иными словами, n-кратное возведение в степень $\mathrm{Norm}(\mathfrak{p}) = p$, то есть возведение в степень $p^n = q$, действует на $\mathcal{O}_L/\mathfrak{B}$ тривиально, что возможно только в том случае, когда $\mathcal{O}_L/\mathfrak{B} \subset \mathbb{F}_q$. ■

Используя формулы из [7, Proposition A.1.1], легко убедиться, что при $j \in \mathbb{F}_q$ или $j \in \mathbb{C}$ следующие кривые, определённые соответственно над $\mathbb{F}_q$ или над $\mathbb{C}$, имеют j-инвариант, равный j:

— над полем характеристики, равной 0 или не меньшей 5, при $j \neq 0$ и $j \neq 1728$: $y^2 = x^3 + 3cx + 2c$, где $c = \dfrac{j}{1728 - j}$;
— над полем характеристики, равной 0 или не меньшей 5, при $j = 0$: $y^2 = x^3 + 1$;
— над полем характеристики, равной 0 или не меньшей 5, при $j = 1728$: $y^2 = x^3 + x$;
— над полем $\mathbb{F}_q$ характеристики 2 при $j \in \mathbb{F}_q^*$: $y^2 + xy = x^3 + j^{-1}$;
— над полем $\mathbb{F}_q$ характеристики 3 при $j \in \mathbb{F}_q^*$: $y^2 = x^3 + x^2 - j^{-1}$.

Неуказанные случаи $j = 0$ для полей характеристик 2 и 3 задают суперсингулярные кривые [7, Exercise 5.7, Theorem 4.1], поэтому нам не встретятся.

На четвёртом этапе утверждается, что построенная к этому моменту кривая E'' обладает комплексным умножением на $\mathcal{O}_D$ (и, в частности, несуперсингулярна). Докажем это.

Из (7) и построения кривой E'' следует, что её j-инвариант равен $R_{\mathfrak{B}}(j(\mathfrak{a}))$, где $\mathfrak{a}$ — некоторый собственный дробный идеал $\mathcal{O}_D$. Поскольку $j(\mathfrak{a}) \in \mathcal{O}_L$, то в силу [13, §4.3] существует некоторое конечное расширение L' поля L, кривая E', определённая над L', с j-инвариантом, равным $j(\mathfrak{a})$, и идеал $\mathfrak{B}' \subset \mathcal{O}_{L'}$, лежащий над $\mathfrak{B}$, редукция по которому уравнения кривой задаёт кривую без особых точек (уже над конечным полем).

Поскольку j-инвариант кривой E' равен сингулярному значению, то E' обладает комплексным умножением на $\mathcal{O}_D$. Поскольку j-инвариант редукции равен редукции j-инварианта (ибо j-инвариант есть рациональная функция от коэффициентов уравнения, задающего кривую), а $\mathfrak{B}' \cap \mathcal{O}_L = \mathfrak{B}$, то $R_{\mathfrak{B}'}(j(\mathfrak{a})) = R_{\mathfrak{B}}(j(\mathfrak{a}))$, т. е. j-инвариант редукции кривой E' по модулю $\mathfrak{B}'$ равен j-инварианту кривой E''. Поскольку две кривые изоморфны, если и только если их j-инварианты совпадают [7, Proposition III.1.4], то E'' изоморфна редукции E'. Теперь из леммы 1 и свойств редукции [8, Теорема 13.12] следует, что E'' несуперсингулярна и $\mathrm{End}(E'') \cong \mathrm{End}(E') \cong \mathcal{O}_D$.

Таким образом, на четвёртом этапе мы начинаем с кривой E'', которая определена над $\mathbb{F}_q$ и имеет комплексное умножение на $\mathcal{O}_D$. Как было показано, порядок кривой E'' равен $q+1-u$, где $4q = u^2 + |D|v^2$ и $\gcd(q,u) = 1$, но u, v необязательно совпадают с $\hat{u}, \hat{v}$. Пусть $\pi = (u + v\sqrt{D})/2 \in \mathcal{O}_D \subset \mathcal{O}$. В силу леммы 1 либо $\pi\mathcal{O} = \mathfrak{p}^n$, либо $\pi\mathcal{O} = \overline{\mathfrak{p}}^n$. То же самое верно и для $\hat{\pi}\mathcal{O}$. Следовательно, $\pi\mathcal{O} = \hat{\pi}\mathcal{O}$ либо $\pi\mathcal{O} = \overline{\hat{\pi}}\mathcal{O}$. Поскольку норма идеала $\pi\mathcal{O}_D \subset \mathcal{O}_D$ равна q и взаимно проста с кондуктором f порядка $\mathcal{O}_D$, то $\pi\mathcal{O}_D = \pi\mathcal{O} \cap \mathcal{O}_D$ [5, Proposition 7.20]. Аналогично $\hat{\pi}\mathcal{O}_D = \hat{\pi}\mathcal{O} \cap \mathcal{O}_D$. Таким образом, либо $\pi\mathcal{O}_D = \hat{\pi}\mathcal{O}_D$, либо $\pi\mathcal{O}_D = \overline{\hat{\pi}}\mathcal{O}_D$, т. е. в кольце $\mathcal{O}_D$ число π ассоциировано либо с $\hat{\pi}$, либо с $\overline{\hat{\pi}}$.

Хорошо известно (см., например, [9, Предложение 13.1.5]), что единицы в кольце $\mathcal{O}_D$ суть $\{\pm 1\}$ при $D \notin \{-3, -4\}$, $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$ при $D = -3$, где $\zeta_3 = e^{2\pi i/3} = (-1+\sqrt{-3})/2$, и $\{\pm 1, \pm i\}$ при $D = -4$.

Если $D \notin \{-3, -4\}$, то $\pi = \pm\hat{\pi}$ либо $\pi = \pm\overline{\hat{\pi}}$, что соответствует $u = \pm\hat{u}$. Таким образом, в этом случае $|E''(\mathbb{F}_q)| = q+1\pm\hat{u}$. Если $|E''(\mathbb{F}_q)| = q+1-\hat{u}$, то кривая E'' является искомой, иначе следует сконструировать другую кривую по уравнению E'' следующим образом. Если $p \neq 2$, то нормальная форма Вейерштрасса уравнения кривой имеет вид $y^2 = f(x)$, где f — многочлен степени 3 со старшим коэффициентом 1, и тогда кривая $y^2 = c^3 f(x/c)$, где c — квадратичный невычет из $\mathbb{F}_q$, имеет нужный порядок (как легко видеть из формулы в [14]). Если же $p = 2$, то нормальная форма Вейерштрасса имеет вид $y^2 + xy = x^3 + a_2x^2 + a_6$, и тогда кривая $y^2 + xy = x^3 + (a_2+\gamma)x^2 + a_6$, где $Tr_{\mathbb{F}_q/\mathbb{F}_2}\gamma = 1$, имеет нужный порядок [14].

Если $D = -3$, то в соответствии с описанной выше процедурой можно вычислить $H_{-3}[j](x) = x$, единственный корень $j = 0$. Формула (6) в этом случае означает $\left(\dfrac{-3}{p}\right) = 1$, откуда $p \equiv 1 \pmod 3$, в частности, $p > 3$. Любая кривая вида $y^2 = x^3 + b$, $b \neq 0$, имеет j-инвариант, равный нулю [7, Proposition A.1.1], и все кривые такого вида $\overline{\mathbb{F}}_q$-изоморфны между собой (поскольку у них одинаковый j-инвариант).

Обозначим через χ единственный мультипликативный характер $\mathbb{F}_q$ порядка 2 и положим $S_2(b) = \sum\limits_{x \in \mathbb{F}_q} \chi(x^3 + b)$. Легко видеть, что порядок кривой $y^2 = x^3 + b$ равен $q + 1 + S_2(b)$. Поскольку $p \equiv 1 \pmod 3$, то и $q \equiv 1 \pmod 3$; в этом случае, согласно

но [15] (где рассматривается только случай $q = p$, когда χ есть символ Лежандра, но рассуждения переносятся на общий случай тривиальным образом), существуют $k, l \in \mathbb{Z}$, такие, что для произвольного кубического невычета $c \in \mathbb{F}_q^*$ справедливы равенства $S_2(1) = 2k$, $S_2(c^2) = -k \pm 3l$, $S_2(c^{-2}) = -k \mp 3l$ и $q = k^2 + 3l^2$. Кроме того, $S_2(b) = \chi(t)S_2(bt^3)$ для любого $t \in \mathbb{F}_q^*$.

Построенная на третьем этапе кривая E'' имеет вид $y^2 = x^3 + 1$; тогда $u = -S_2(1) = -2k$, $q = k^2 + 3l^2$, $l = \pm\frac{S_2(c^2) - S_2(c^{-2})}{6}$, где c — произвольный кубический невычет в $\mathbb{F}_q$; отсюда в силу $|\pi|^2 = q$ имеем $\pi = -k \pm l\sqrt{-3}$. В случае необходимости сделаем замену c на c^{-1} и представим π в виде $-k - l\sqrt{-3}$, где $l = (S_2(c^2) - S_2(c^{-2}))/6$.

Либо $\hat{\pi}$, либо $\overline{\hat{\pi}}$ равно произведению π на какую-то из единиц кольца $\mathcal{O}_{-3}$; в обоих случаях $\hat{u} = 2\operatorname{Re}\hat{\pi}$ равно удвоенной вещественной части произведения π на какую-то из единиц. Таким образом, для $\hat{u}$ возможны шесть вариантов:

— $\hat{u} = 2\operatorname{Re}\hat{\pi} = \pm 2\operatorname{Re}\pi = \pm 2k$. В этом случае ищем кривую с $q + 1 \pm 2k$ точек, и кривая $y^2 = x^3 + 1$ либо $y^2 = x^3 + g^3$, где g — квадратичный невычет в $\mathbb{F}_q$, является искомой;

— $\hat{u} = 2\operatorname{Re}\hat{\pi} = \pm 2\operatorname{Re}(\zeta_3\pi) = \pm(k + 3l)$. В этом случае ищем кривую с $q + 1 \pm (k + 3l)$ точек, и кривая $y^2 = x^3 + c^2$ либо $y^2 = x^3 + c^2g^3$ является искомой;

— $\hat{u} = 2\operatorname{Re}\hat{\pi} = \pm 2\operatorname{Re}(\zeta_3^2\pi) = \pm(k - 3l)$. В этом случае ищем кривую с $q + 1 \pm (k - 3l)$ точек, и кривая $y^2 = x^3 + c^{-2}$ либо $y^2 = x^3 + c^{-2}g^3$ является искомой.

Если $D = -4$, то аналогично имеем $H_{-4}[j](x) = x - 1728$, единственный корень $j = 1728$. Формула (6) в этом случае означает $\left(\dfrac{-4}{p}\right) = 1$, откуда $p \equiv 1 \pmod 4$, в частности по-прежнему $p > 3$. Любая кривая вида $y^2 = x^3 + bx$, $b \neq 0$, имеет j-инвариант, равный 1728 [7, Proposition A.1.1], и все кривые такого вида $\overline{\mathbb{F}}_q$-изоморфны между собой (поскольку имеют одинаковый j-инвариант).

Положим $S_1(b) = \sum\limits_{x \in \mathbb{F}_q} \chi(x)\chi(x^2 + b)$, где, как и раньше, χ — единственный мультипликативный характер $\mathbb{F}_q$ порядка 2. Легко видеть, что порядок кривой $y^2 = x^3 + bx$ равен $q + 1 + S_1(b)$. Поскольку $p \equiv 1 \pmod 4$, то и $q \equiv 1 \pmod 4$; в этом случае, согласно [16], существуют $k, l \in \mathbb{Z}$, такие, что k нечётно, $S_1(1) = 2k$, $S_1(b) = \pm 2l$ для любого квадратичного невычета b и $S_1(b) = \chi(t)S_1(bt^2)$ для любого $t \in \mathbb{F}_q^*$.

Построенная на третьем этапе кривая E'' имеет вид $y^2 = x^3 + x$; тогда $u = -S_1(1) = -2k$, $q = k^2 + l^2$. Поскольку $|\pi|^2 = q$, то $\pi = -k \pm li$.

Аналогично предыдущему случаю есть четыре варианта для $\hat{u}$, а именно $\pm 2\operatorname{Re}\pi = \pm 2k$ и $\pm 2\operatorname{Re}(i\pi) = \pm 2l$. Если $\hat{u} = \pm 2k$, то кривая $y^2 = x^3 + x$ либо $y^2 = x^3 + g^2x$, где g — квадратичный невычет в $\mathbb{F}_q$, имеет нужное число точек. Если $\hat{u} = \pm 2l$, то кривая $y^2 = x^3 + gx$ либо $y^2 = x^3 + g^3x$ имеет нужное число точек.

1.3. Некоторые известные оптимизации метода

Коэффициенты многочлена $H_D[j]$ растут достаточно быстро с ростом $|D|$. Например, $H_{-40}[j](x) = x^2 - 425692800x + 9103145472000$. Поэтому представляет интерес поиск других функций, сингулярные значения которых лежат в L, но имеют меньшую высоту характеристического многочлена.

Пусть $z \in \mathbb{H}$, $q = e^{2\pi i z}$. Введём вслед за [6] функции

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) = q^{\frac{1}{24}} \sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{3n^2+n}{2}},$$

$$\mathfrak{f}(z) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{z+1}{2}\right)}{\eta(z)}, \quad \mathfrak{f}_1(z) = \frac{\eta\left(\frac{z}{2}\right)}{\eta(z)}, \quad \mathfrak{f}_2(z) = \sqrt{2}\frac{\eta(2z)}{\eta(z)}, \tag{9}$$

$$\gamma_2(z) = \frac{\mathfrak{f}^{24}-16}{\mathfrak{f}^8} = \frac{\mathfrak{f}_1^{24}+16}{\mathfrak{f}_1^8} = \frac{\mathfrak{f}_2^{24}+16}{\mathfrak{f}_2^8}, \quad j(z) = \gamma_2(z)^3.$$

Пусть N — натуральное число. Назовём вслед за [17] N-системой набор форм $(A_1, B_1, C_1), \ldots, (A_h, B_h, C_h)$, такой, что

— набор $\{\mathfrak{h}(A_i, B_i, C_i) : 1 \leqslant i \leqslant h\}$ является полной системой представителей группы $\mathcal{H}_D$;

— справедливы соотношения $\gcd(A_i, N) = 1$; $B_i \equiv B_j \pmod{2N}$.

Отметим, что для любой формы (A_i, B_i, C_i) выполнено $B_i \equiv D \pmod 2$, так что из первого условия автоматически следует, что $B_i \equiv B_j \pmod 2$ для любых i, j.

По известному набору форм, удовлетворяющему первому условию (например, полному набору приведённых форм), можно построить N-систему. Соответствующий алгоритм приведён в [17, доказательство Proposition 3]. (Предполагаем известным разложение N на простые множители.)

1) Сначала добьёмся выполнения условия $\gcd(A_i, N) = 1$ при всех i.

Ясно, что достаточно уметь добиваться условия $\gcd(A_i, N_0 l) = 1$ в предположении, что $\gcd(A_i, N_0) = 1$, где l — очередной простой делитель N, не делящий N_0.

Число l не может делить каждое из трёх чисел A_i, $A_i + N_0 B_i + N_0^2 C_i$, $l^2 A_i + l N_0 B_i + N_0^2 C_i$, потому что иначе числа A_i, B_i, C_i имели бы общий делитель l и форма (A_i, B_i, C_i) не была бы примитивной.

— Если $l \nmid A_i$, то условие $\gcd(A_i, N_0 l) = 1$ выполнено.

— Если $l \nmid A_i + N_0 B_i + N_0^2 C_i$, то в форме $A_i x^2 + B_i xy + C_i y^2$ сделаем замену переменных $x = x'$, $y = N_0 x' + y'$ (очевидно, определитель матрицы этой замены равен 1); получим эквивалентную форму с коэффициентом при x'^2, равным $A_i + N_0 B_i + N_0^2 C_i$, дальше будем работать с ней вместо (A_i, B_i, C_i).

— Если $l \nmid l^2 A_i + l N_0 B_i + N_0^2 C_i$, то найдём $a, b \in \mathbb{Z}$, такие, что $al - bN_0 = 1$, и сделаем замену переменных $x = lx' + by'$, $y = N_0 x' + ay'$ (очевидно, определитель матрицы этой замены равен 1); получим эквивалентную форму с коэффициентом при x'^2, равным $l^2 A_i + l N_0 B_i + N_0^2 C_i$, дальше будем работать с ней вместо (A_i, B_i, C_i).

2) Остаётся обеспечить условие $B_i \equiv B_1 \pmod{2N}$ при всех i. Замена переменных $x = x' + ay'$, $y = y'$ переводит форму (A_i, B_i, C_i) в эквивалентную форму $(A_i, B_i + 2aA_i, C_i + aB_i + a^2 A_i)$; поскольку $\gcd(A_i, N) = 1$, то применение этого преобразования с $a = A_i^{-1}(B_1 - B_i)/2 \bmod N$ решает задачу.

Теорема 2 (Theorem 1 из [17]). Пусть $\alpha \in \mathbb{H}$ — корень формы

$$(A, B, C), \quad 2 \nmid A, \quad 32 \mid B,$$

дискриминант которой равен $B^2 - 4AC = D = -4m$, $m \in \mathbb{N}$. Пусть $g(\alpha)$ определено следующими формулами:

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}(\alpha)^2\right)^3, \text{ если } m \equiv 1 \pmod 8,$$

$$\begin{aligned}
\mathfrak{f}(\alpha)^3, &\text{ если } m \equiv 3 \pmod 8,\\
\left(\frac{1}{2}\mathfrak{f}(\alpha)^4\right)^3, &\text{ если } m \equiv 5 \pmod 8,\\
\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}(\alpha)\right)^3, &\text{ если } m \equiv 7 \pmod 8,\\
\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}_1(\alpha)^2\right)^3, &\text{ если } m \equiv 2 \pmod 4,\\
\left(\left(\frac{2}{A}\right)\frac{1}{2\sqrt{2}}\mathfrak{f}_1(\alpha)^4\right)^3, &\text{ если } m \equiv 4 \pmod 8.
\end{aligned}$$

Тогда $g(\alpha) \in \mathcal{O}_L$.

Если $\alpha_1 = \alpha, \ldots, \alpha_h$ — корни элементов 16-системы, то сингулярные значения $g(\alpha_i)$ образуют полный набор различных сопряжённых чисел над $\mathbb{Q}$.

Теорема 3 (Theorem 2 из [17]). Пусть $\alpha \in \mathbb{H}$ — корень формы

$$(A, B, C), \quad 3 \nmid A, \quad 3 \mid B$$

дискриминанта $B^2 - 4AC = D$. Тогда

$$\mathbb{Q}(\gamma_2(\alpha)) = \begin{cases} \mathbb{Q}(j(\alpha)), & 3 \nmid D, \\ \mathbb{Q}(j(3\alpha)), & 3 \mid D. \end{cases}$$

Более того, в случае $3 \nmid D$, если $\alpha_1 = \alpha, \ldots, \alpha_h$ — корни элементов 3-системы, то сингулярные значения $\gamma_2(\alpha_i)$ образуют полный набор различных сопряжённых чисел над $\mathbb{Q}$. Кроме того, числа $\gamma_2(\alpha_i)$ целые алгебраические.

Введём вслед за [18] при простых p_1, p_2 функцию

$$\mathfrak{m}_{p_1,p_2}(z) = \frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta(z)\eta\left(\frac{z}{p_1 p_2}\right)}$$

и обозначим $s = \dfrac{24}{\gcd(24, (p_1-1)(p_2-1))}$.

Теорема 4 (Theorems 3.2, 3.3, Corollary 3.1 из [18]). Пусть D удовлетворяет (1), $N = p_1 p_2$, p_1 и p_2 — простые числа, удовлетворяющие следующему условию:

1) $\left(\dfrac{D}{p_1}\right), \left(\dfrac{D}{p_2}\right) \neq -1$ при $p_1 \neq p_2$,

либо 2*а*) $\left(\dfrac{D}{p}\right) = 1$ при $p_1 = p_2 = p$, либо 2*б*) $p | f$ при $p_1 = p_2 = p$.

Тогда существует форма (A_1, B_1, C_1), такая, что $\gcd(A_1, N) = 1$ и $N \mid C_1$. Пусть $\alpha_1 \in \mathbb{H}$ — её корень. Сингулярное значение $\mathfrak{m}^s_{p_1,p_2}(\alpha_1)$ лежит в L. Все сопряжённые над K значения к $\mathfrak{m}^s_{p_1,p_2}(\alpha_1)$ суть $\mathfrak{m}^s_{p_1,p_2}(\alpha_i)$, где α_i пробегает корни элементов N-системы. Числа $\mathfrak{m}^s_{p_1,p_2}(\alpha_i)$ являются целыми алгебраическими.

Если выполнено условие 1 или 2*а*, то $\mathfrak{m}^s_{p_1,p_2}(\alpha_i)$ являются единицами (т. е. $\mathfrak{m}^{-s}_{p_1,p_2}(\alpha_i)$ также целые алгебраические).

Если p_1 и p_2 удовлетворяют более сильному условию

— $\left(\dfrac{D}{p_1}\right), \left(\dfrac{D}{p_2}\right) \neq -1$ и $p_1, p_2 \nmid f$ при $p_1 \neq p_2$;

— $\left(\dfrac{D}{p}\right) = 1$ или $p \mid f$ при $p_1 = p_2 = p \neq 2$;

— либо $\left(\dfrac{D}{2}\right) = 1$, либо $2 \mid f$ и $D \not\equiv 4 \pmod{32}$ при $p_1 = p_2 = 2$,

то комплексное сопряжение переставляет числа $\mathfrak{m}^s_{p_1,p_2}(\alpha_i)$.

Далее понадобятся более точные утверждения. Формулировки теорем 2, 3, 4 дают неполную информацию о действии автоморфизмов из $\mathrm{Gal}(L/K)$ на сингулярных значениях. Однако их доказательства из [17, 18] предоставляют эту информацию.

Утверждение 1 [17]. Пусть θ — функция, описанная в формулировке одной из теорем 2, 3, 4 (в последней достаточно выполнения слабого условия на p_1, p_2), $\mathfrak{a}, \mathfrak{b}$ — два элемента N-системы из формулировок тех же теорем, α — корень $\mathfrak{a}$, β — корень $\mathfrak{b}$, $\Omega : \mathcal{H}_D \to \mathrm{Gal}(L/K)$ — канонический изоморфизм. Тогда

$$\theta(\alpha)^{\Omega(\mathfrak{h}(\mathfrak{a})\mathfrak{h}(\mathfrak{b})^{-1})} = \theta(\beta).$$

Для $\theta = j$ эта формула также верна, что уже упоминалось выше.

Утверждение 1 удобнее использовать в виде формулы, задающей действие конкретного элемента $\mathrm{Gal}(L/K)$ на сингулярных значениях. Напомним, что $\mathfrak{h}$ сюръективно, а N-система по определению содержит представителей всех классов $\mathcal{H}_D$.

Следствие. Пусть θ, N-система и $\mathfrak{a}$ такие же, как в предыдущем утверждении, и $\mathfrak{c} \in \mathcal{H}_D$. Тогда существует форма $\mathfrak{b}$, принадлежащая этой N-системе и такая, что

$$\mathfrak{h}(\mathfrak{b}) = \mathfrak{h}(\mathfrak{a})\mathfrak{c}^{-1}.$$

Если β — корень $\mathfrak{b}$, то

$$\theta(\alpha)^{\Omega(\mathfrak{c})} = \theta(\beta). \tag{10}$$

В дальнейшем при использовании функции $\mathfrak{m}^s_{p_1,p_2}$ будем предполагать, что p_1 и p_2 удовлетворяют сильному условию теоремы; легко видеть, что для любого D такие p_1, p_2 всегда можно найти.

Объединяя теоремы 2 и 3, получаем, что если в дополнение к условиям теоремы 2 выполнены условия $3 \nmid D$, $3 \nmid A$, $3 \mid B$, то в заключении теоремы 2 в выражениях для $g(\alpha)$ можно убрать возведение в куб. Например, рассмотрим случай $m \equiv 3 \pmod 8$. Согласно (9),

$$\mathfrak{f}(\alpha) = \frac{\left(\mathfrak{f}(\alpha)^3\right)^3 \gamma_2(\alpha)}{\left(\mathfrak{f}(\alpha)^3\right)^8 - 16}. \tag{11}$$

Поскольку $\mathfrak{f}(\alpha)^3 \in L$ и $\gamma_2(\alpha) \in L$, то и $\mathfrak{f}(\alpha) \in L$. Из утверждения 1 следует, что любой автоморфизм из $\mathrm{Gal}(L/K)$ переводит $\mathfrak{f}(\alpha)^3$ в $\mathfrak{f}(\alpha')^3$ и $\gamma_2(\alpha)$ в $\gamma_2(\alpha')$, где α' зависит только от автоморфизма; из (11) следует, что $\mathfrak{f}(\alpha)$ переходит в $\mathfrak{f}(\alpha')$. Наконец, $\mathfrak{f}(\alpha)$ — целое алгебраическое, например, как кубический корень из целого алгебраического числа $\mathfrak{f}(\alpha)^3$. В остальных случаях формулы несколько сложнее, но принцип одинаков.

Пусть θ и $\alpha_* = \{\alpha_1, \ldots, \alpha_h\}$ — соответственно функция и набор корней, заданные в условии одной из теорем 2–4. Введём многочлен от одной переменной

$$H_D[\theta, \alpha_*](x) = \prod_{i=1}^{h} (x - \theta(\alpha_i)).$$

Если θ — функция, заданная в условии теоремы 2 или 3, то многочлен $H_D[\theta, \alpha_*]$ имеет целые коэффициенты. Если же $\theta = \mathfrak{m}^s_{p_1,p_2}$, то нужно привлечь утверждение 1, из

которого легко видеть, что $H_D[\theta, \alpha_*]$ инвариантен относительно $\mathrm{Gal}(L/K)$ и, следовательно, лежит в $K[x]$; теперь из теоремы 4 следует, что и в этом случае $H_D[\theta, \alpha_*]$ имеет целые коэффициенты.

Например, $H_{-40}[\gamma_2, \alpha_*](x) = x^2 - 780x + 20880$, $H_{-40}[g, \alpha_*](x) = x^2 - x - 1$, где $g(\alpha) = \left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}_1(\alpha)^2$, $H_{-40}[\mathfrak{m}_{5,7}, \alpha_*](x) = x^2 - x - 1$, $H_{-40}[\mathfrak{m}_{11,13}, \alpha_*](x) = x^2 \pm 2x + 1$. (В первых трёх примерах многочлен не зависит от набора α_*, в последнем в зависимости от α_* есть два варианта.) Последний пример демонстрирует, что значения $\mathfrak{m}^s_{p_1,p_2}(\alpha_i)$ могут и не быть попарно различными, так что в общем случае $H_D[\mathfrak{m}^s_{p_1,p_2}, \alpha_*]$ есть некоторая степень минимального многочлена.

Поскольку для рассматриваемых функций многочлен $H_D[\theta, \alpha_*]$, как и $H_D[j]$, имеет целые коэффициенты, то его можно вычислять путём построения достаточно точных приближений к сингулярным значениям $\theta(\alpha_i)$ с последующим перемножением скобок вида $x - \theta(\alpha_i)$ и восстановлением целых коэффициентов многочлена путём округления вычисленных приближений. Поскольку $\theta(\alpha_i) \in \mathcal{O}_L$, то $\theta(\alpha_i)$ имеет представителя в $\mathcal{O}_L/\mathfrak{B} \subset \mathbb{F}_q$ (теорема 1), так что редукция уравнения $H_D[\theta, \alpha_*](x) = 0$ по модулю p разлагается на линейные множители над $\mathbb{F}_q$. Остаётся по значению редукции $\theta(\alpha_i)$ в $\mathbb{F}_q$ вычислить j-инвариант нужной эллиптической кривой, равный $R_{\mathfrak{B}}(j(\alpha))$. Для функции γ_2 и степеней $\mathfrak{f}$ из теоремы 2 ответ дают формулы (9). Для функций $\mathfrak{m}^s_{p_1,p_2}$ ситуация более сложная. В этом случае существует многочлен $\Phi_{p_1,p_2}(x, y) \in \mathbb{Z}[x, y]$, такой, что выполнено тождество $\Phi_{p_1,p_2}(\mathfrak{m}^s_{p_1,p_2}(z), j(z)) = 0$ [18]; подставляя в это тождество значение $z = \alpha_i$ и редуцируя по модулю $\mathfrak{B}$ (поскольку $\mathfrak{B} \cap \mathbb{Z} = p\mathbb{Z}$, то для редукции достаточно привести многочлен Φ_{p_1,p_2} по модулю p), получаем полиномиальное уравнение над $\mathbb{F}_q$ на $R_{\mathfrak{B}}(j(\alpha))$, из которого можно найти несколько вариантов для $R_{\mathfrak{B}}(j(\alpha))$. Правильный вариант можно выбрать, рассмотрев все варианты, построив для каждого эллиптическую кривую и проверив, что её порядок равен $q + 1 - m$. Если, как, например, нужно в криптографических приложениях, $q + 1 - m$ делится на большое простое число, то простой тест, проверяющий, что случайно выбранная точка кривой после умножения на $q+1-m$ переходит в нуль, хорошо отсеивает неверные альтернативы. Следует отметить, что совпадающий порядок кривой не гарантирует, что кольцо эндоморфизмов есть в точности $\mathcal{O}_D$, но столь тонкие различия часто неважны для приложений; более подробно этот вопрос разобран в [18].

2. Свойства изоморфизма Ω

Мы определили группу $\mathcal{H}_D$ как фактор-группу группы $I(\mathcal{O}_D)$ собственных дробных идеалов порядка $\mathcal{O}_D$ по подгруппе главных идеалов $P(\mathcal{O}_D)$.

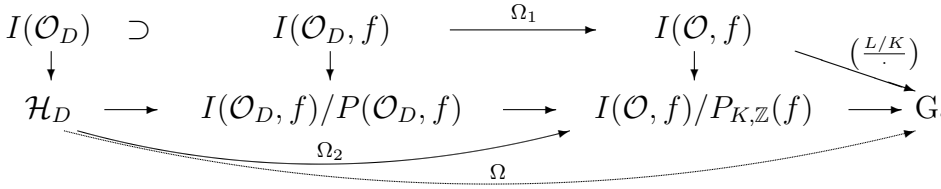
Напомним, что идеал $\mathfrak{a} \subset \mathcal{O}_D$ взаимно прост с f, если $\mathfrak{a} + f\mathcal{O}_D = \mathcal{O}_D$. Согласно [5, Lemma 7.18], это условие эквивалентно $\gcd(\mathrm{Norm}(\mathfrak{a}), f) = 1$, и все такие идеалы собственные. Обозначим подгруппу, порождённую ими в $I(\mathcal{O}_D)$, через $I(\mathcal{O}_D, f)$. Обозначим подгруппу в $P(\mathcal{O}_D)$, порождённую главными идеалами $\alpha\mathcal{O}_D$ с $\gcd(\mathrm{Norm}(\alpha), f) = 1$, через $P(\mathcal{O}_D, f)$. Включение $I(\mathcal{O}_D, f) \subset I(\mathcal{O}_D)$ индуцирует изоморфизм $I(\mathcal{O}_D, f)/P(\mathcal{O}_D, f) \cong \mathcal{H}_D$ [5, Proposition 7.19].

Идеал $\mathfrak{a} \subset \mathcal{O}$ взаимно прост с f тогда и только тогда, когда выполнено условие $\gcd(\mathrm{Norm}(\mathfrak{a}), f) = 1$ [5, Lemma 7.18]. Обозначим группу дробных идеалов $\mathcal{O}$, порождённую такими идеалами, через $I(\mathcal{O}, f)$. Напомним, что $P_{K,\mathbb{Z}}(f)$ обозначает подгруппу идеалов $\mathcal{O}$, порождённую главными идеалами вида $\alpha\mathcal{O}$, где $\alpha \in \mathcal{O}$, $\alpha \equiv a \pmod{f\mathcal{O}}$ для $a \in \mathbb{Z}$, такого, что $\gcd(a, f) = 1$. В соответствии с [5, Proposition 7.20] формула $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}$

задаёт изоморфизм групп $\Omega_1 : I(\mathcal{O}_D, f) \to I(\mathcal{O}, f)$, сохраняющий норму. Кроме того [5, Proposition 7.22], Ω_1 индуцирует изоморфизм $I(\mathcal{O}_D, f)/P(\mathcal{O}_D, f) \cong I(\mathcal{O}, f)/P_{K,\mathbb{Z}}(f)$.

Таким образом, получили изоморфизм $\Omega_2 : \mathcal{H}_D \to I(\mathcal{O}, f)/P_{K,\mathbb{Z}}(f)$. Отображение Артина $I(\mathcal{O}, f) \to \mathrm{Gal}(L/K)$, которое будем обозначать $\left(\frac{L/K}{\cdot}\right)$, индуцирует изоморфизм $I(\mathcal{O}, f)/P_{K,\mathbb{Z}}(f) \to \mathrm{Gal}(L/K)$, композиция которого с Ω_2, согласно [5, §9], есть канонический изоморфизм Ω, который фигурирует в утверждении 1.

Подытожим: существует коммутативная диаграмма



(12)

где вертикальные стрелки обозначают проекции группы на фактор-группу, а стрелки во второй строке обозначают изоморфизмы.

Теорема 5. Пусть (A, B, C) — форма, такая, что $\gcd(A, D) = 1$. Пусть $q \mid D$ такое, что выполнен один из двух наборов условий:

— $|q|$ — нечётное простое число, $q \equiv 1 \pmod 4$;
— $q \in \{-4, \pm 8\}$, $D/q \equiv 0 \pmod 4$ или $D/q \equiv 1 \pmod 4$.

Тогда

1) $\sqrt{q} \in L$;
2) $\mathfrak{a} = \left\langle A, (-B + \sqrt{D})/2 \right\rangle_{\mathbb{Z}} \in I(\mathcal{O}_D, f)$, $\mathrm{Norm}(\mathfrak{a}) = A$;
3) $\left(\frac{L/K}{\Omega_1(\mathfrak{a})}\right)(\sqrt{q}) = \left(\frac{q}{A}\right)\sqrt{q}$, где $\left(\frac{L/K}{\cdot}\right)$ обозначает отображение Артина, введённое при доказательстве теоремы 1, а $\left(\frac{q}{A}\right)$ есть символ Кронекера, определённый на с. 21.

Доказательство. Первое утверждение следует из [19, Theorem 2.2.23 и (2.2.8)].

По [5, Theorem 7.7] $\mathfrak{a}$ является собственным идеалом $\mathcal{O}_D$. Его норма по определению равна $|\mathcal{O}_D/\mathfrak{a}|$; легко видеть, что в каждом смежном классе по $\mathfrak{a}$ существует единственное целое число из $0, \ldots, A-1$, так что $\mathrm{Norm}(\mathfrak{a}) = A$. Поскольку $\gcd(A, f) = 1$, то $\mathfrak{a}$ взаимно прост с f.

Докажем третье утверждение. Запишем $\Omega_1(\mathfrak{a}) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$, где $\mathfrak{p}_i$ — простые идеалы $\mathcal{O}$ (не обязательно различные). Поскольку $A = \mathrm{Norm}(\mathfrak{a}) = \mathrm{Norm}(\mathfrak{p}_1) \cdot \ldots \cdot \mathrm{Norm}(\mathfrak{p}_s)$ и символ Кронекера мультипликативен по нижнему аргументу, достаточно доказать, что для каждого простого $\mathfrak{p} \mid \Omega_1(\mathfrak{a})$ выполнено равенство с символом Артина

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt{q}) = \left(\frac{q}{\mathrm{Norm}(\mathfrak{p})}\right)\sqrt{q}. \tag{13}$$

Поскольку левая часть есть образ $\sqrt{q}$ под действием некоторого автоморфизма, то она должна быть равна $\pm\sqrt{q}$.

Пусть $\mathfrak{p}$ — простой идеал, $\mathfrak{p} \mid \Omega_1(\mathfrak{a})$, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, p нечётно. Пусть простой идеал $\mathfrak{B} \subset \mathcal{O}_L$ лежит над $\mathfrak{p}$. Поскольку $\gcd(A, D) = 1$ и $q \mid D$, то $2\sqrt{q} \notin \mathfrak{B}$ и, следовательно, $\sqrt{q} \not\equiv -\sqrt{q} \pmod{\mathfrak{B}}$. По определению

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt{q}) \equiv \sqrt{q}^{\mathrm{Norm}(\mathfrak{p})} = q^{\frac{\mathrm{Norm}(\mathfrak{p})-1}{2}}\sqrt{q} \pmod{\mathfrak{B}}.$$

Если идеал $p\mathcal{O}$ простой (т. е. $\mathfrak{p} = p\mathcal{O}$), то $\mathrm{Norm}(\mathfrak{p}) = p^2$ и правая часть (13) равна $\sqrt{q}$. С другой стороны, $q^{\frac{\mathrm{Norm}(\mathfrak{p})-1}{2}} = (q^{p-1})^{\frac{p+1}{2}} \equiv 1 \pmod{p}$, так что левая часть (13) сравнима с $\sqrt{q}$ по модулю $\mathfrak{B}$ и, следовательно, равна $\sqrt{q}$, так что равенство (13) выполнено.

Если идеал $p\mathcal{O}$ не простой, то $\mathrm{Norm}(\mathfrak{p}) = p$ и правая часть (13) равна $\left(\frac{q}{p}\right)\sqrt{q}$. С другой стороны, $q^{\frac{\mathrm{Norm}(\mathfrak{p})-1}{2}} = q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$, так что левая часть (13) сравнима с $\left(\frac{q}{p}\right)\sqrt{q}$ по модулю $\mathfrak{B}$, следовательно, равна $\left(\frac{q}{p}\right)\sqrt{q}$, что доказывает (13) и в этом случае.

Пусть теперь $\mathfrak{p} \mid \Omega_1(\mathfrak{a})$, $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$, простой идеал $\mathfrak{B} \subset \mathcal{O}_L$ лежит над $\mathfrak{p}$. В этом случае $2 \mid A$, следовательно, по условию $2 \nmid D$ и q нечётно. Поскольку $B^2 - 4AC = D$, то $D \equiv B^2 \equiv 1 \pmod{8}$. Следовательно, $d \equiv 1 \pmod{8}$ и идеал $2\mathcal{O}$ не простой [9, Предложение 13.1.4], так что $\mathrm{Norm}(\mathfrak{p}) = 2$. Таким образом, правая часть (13) равна $\left(\frac{q}{2}\right)\sqrt{q}$. Для вычисления левой части (13) рассмотрим $\left(\frac{L/K}{\mathfrak{p}}\right)\left(\frac{1+\sqrt{q}}{2}\right)$. Это выражение должно быть равно $(1 \pm \sqrt{q})/2$, и два возможных значения различны по модулю $\mathfrak{B}$. По определению

$$\left(\frac{L/K}{\mathfrak{p}}\right)\left(\frac{1+\sqrt{q}}{2}\right) \equiv \left(\frac{1+\sqrt{q}}{2}\right)^2 = \frac{q-1}{4} + \frac{1+\sqrt{q}}{2} \pmod{\mathfrak{B}}.$$

Если $\left(\frac{q}{2}\right) = 1$, то $q \equiv 1 \pmod{8}$, $(q-1)/4$ чётно и, следовательно, лежит в $\mathfrak{B}$; если $\left(\frac{q}{2}\right) = -1$, то $q \equiv 5 \pmod{8}$, $(q-1)/4$ нечётно и, следовательно, сравнимо с $-1 \equiv 1$ по модулю $\mathfrak{B}$. В обоих случаях

$$\left(\frac{L/K}{\mathfrak{p}}\right)\left(\frac{1+\sqrt{q}}{2}\right) \equiv \frac{1+\left(\frac{q}{2}\right)\sqrt{q}}{2} \pmod{\mathfrak{B}},$$

откуда следует (13). ■

Лемма 2. Пусть $d < 0$ удовлетворяет одному из условий (2) и (3). Тогда d может быть единственным с точностью до порядка множителей способом представлен в виде произведения $d = q_1^* \cdot \ldots \cdot q_t^*$, где все q_i^* попарно взаимно просты, $q^* = (-1)^{\frac{q-1}{2}} q$, если $q > 0$ — нечётное простое, и $q^* \in \{-4, \pm 8\}$, если $q = 2$.

Доказательство. Единственность такого представления очевидна, нужно доказать его существование.

В случае (2) разложение числа d на простые множители имеет вид $d = -q_1 \cdot \ldots \cdot q_t$, где q_i — различные нечётные простые; поскольку $q_i^* = \pm q_i$, то $d = \pm q_1^* \cdot \ldots \cdot q_t^*$; наконец, поскольку $d \equiv 1 \pmod{4}$ и $q_i^* \equiv 1 \pmod{4}$ для всех i, то заключение леммы выполнено.

В случае (3) разложение числа $d/4$ на простые множители имеет вид либо $d/4 = -q_1 \cdot \ldots \cdot q_{t-1}$, либо $d/4 = -2q_1 \cdot \ldots \cdot q_{t-1}$, где в обоих вариантах q_i — различные нечётные простые. Если $d/4$ нечётно, то, как и в предыдущем случае, $d/4 = \pm q_1^* \cdot \ldots \cdot q_{t-1}^*$, но теперь в силу (3) $d/4 \not\equiv 1 \pmod{4}$, так что в правой части должен быть знак минус, и после умножения на 4 получаем заключение леммы с $q_t^* = -4$. Наконец, если $d/4$ чётно, то $d/4 = \pm 2q_1^* \cdot \ldots \cdot q_{t-1}^*$, и, выбирая знак $q_t^* = \pm 8$ подходящим образом, получаем заключение леммы. ■

Легко видеть, что числа q_i^* из леммы 2 удовлетворяют условию теоремы 5 и, следовательно, $K\left(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}\right)\subset L$. Поле $K\left(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}\right)$ зависит только от поля K (которое определяет d, но не f) и называется полем родов (*genus field*) для K. Далее будем обозначать $K\left(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}\right)=K_G$.

3. Кольцо целых поля родов

Итак, введены в рассмотрение поля $K=\mathbb{Q}\left(\sqrt{d}\right)$ и $K_G=K\left(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}\right)$. Далее понадобится знание кольца целых в K_G.

Пусть q_i^* взяты из условия леммы 2, тогда выполнен один из следующих трёх случаев:

1) все $|q_i|$ — нечётные простые;
2) $q_t^*=\pm 8$;
3) $q_t^*=-4$.

Построим в каждом из этих случаев фундаментальный базис поля K_G; поскольку $d=q_1^*\cdot\ldots\cdot q_t^*$, то $\sqrt{d}\in\mathbb{Q}(\sqrt{q_1^*},\ldots,\sqrt{q_t^*})$ и, следовательно, $K_G=\mathbb{Q}(\sqrt{q_1^*},\ldots,\sqrt{q_t^*})$.

Лемма 3. Пусть M — числовое поле, $p\in\mathbb{Z}$ — такое простое число, что идеал $p\mathbb{Z}$ неразветвлён в M. Пусть также $c\in M$ такое, что $pc^2\in\mathcal{O}_M$. Тогда $c\in\mathcal{O}_M$.

Доказательство. Предположим, что $c\notin\mathcal{O}_M$. Тогда идеал $c\mathcal{O}_M$ дробный, и его разложение на простые имеет вид $\mathfrak{q}_1^{s_1}\cdot\ldots\cdot\mathfrak{q}_m^{s_m}$, где все $\mathfrak{q}_i$ попарно различны и $s_1<0$. Но степень $\mathfrak{q}_1$ в разложении идеала $p\mathcal{O}_M$ не превосходит 1 в силу неразветвлённости $p\mathbb{Z}$, а степень $\mathfrak{q}_1$ в разложении идеала $c^2\mathcal{O}_M$ не больше -2, следовательно, степень идеала $\mathfrak{q}_1$ в разложении $pc^2\mathcal{O}_M$ отрицательна, что противоречит тому, что $pc^2\in\mathcal{O}_M$. ■

Теорема 6. Пусть $\tilde{q}_1,\ldots,\tilde{q}_r$ — такие попарно различные целые числа, что $|\tilde{q}_i|$ — нечётные простые и $\tilde{q}_i\equiv 1\pmod 4$. Обозначим $\alpha_i=(1+\sqrt{\tilde{q}_i})/2$ и $\tilde{\alpha}_i=(1-\sqrt{\tilde{q}_i})/2$. Тогда

1) числа $\alpha_1^{s_1}\ldots\alpha_r^{s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^r$, образуют фундаментальный базис поля $\mathbb{Q}(\sqrt{\tilde{q}_1},\ldots,\sqrt{\tilde{q}_r})$;
2) числа $\tilde{\alpha}_1^{s_1}\alpha_1^{1-s_1}\ldots\tilde{\alpha}_r^{s_r}\alpha_r^{1-s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^r$, образуют фундаментальный базис поля $\mathbb{Q}(\sqrt{\tilde{q}_1},\ldots,\sqrt{\tilde{q}_r})$.

Доказательство. Доказательство проведём индукцией по r. При $r=0$ утверждение тривиально. Предположим, что утверждение доказано для полей $M_i=\mathbb{Q}(\sqrt{\tilde{q}_1},\ldots,\sqrt{\tilde{q}_i})$ при $i=1,\ldots,r-1$.

Лемма 4. Пусть $p\in\mathbb{Z}$ — простое число, не делящее ни одно из чисел $\tilde{q}_1,\ldots,\tilde{q}_{r-1}$. Тогда идеал $p\mathbb{Z}$ неразветвлён в M_{r-1}.

Доказательство. Достаточно проверить, что для всех $1\leqslant i\leqslant r-1$ никакой из идеалов поля M_{i-1}, делящих $p\mathcal{O}_{M_{i-1}}$, неразветвлён в $M_i=M_{i-1}(\sqrt{\tilde{q}_i})$.

Пусть $\mathfrak{p}$ — простой идеал кольца целых поля M_{i-1}, такой, что $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$. Расширение $M_{i-1}\subset M_i$ порождается элементом α_i; из индуктивного предположения следует, что $(1,\alpha_i)$ образуют базис $\mathcal{O}_{M_i}/\mathcal{O}_{M_{i-1}}$. Единственный нетривиальный автоморфизм M_i над M_{i-1} переводит этот базис в $(1,\tilde{\alpha}_i)$. В соответствии с [20, Предложения III.8 и III.14] для доказательства неразветвлённости $\mathfrak{p}$ достаточно проверить, что $\mathfrak{p}$ не делит $\det\begin{pmatrix}1 & \alpha_i\\ 1 & \tilde{\alpha}_i\end{pmatrix}^2=(\alpha_i-\tilde{\alpha}_i)^2=\tilde{q}_i$. Поскольку p не делит $\tilde{q}_i$, это свойство выполнено. ■

Применим лемму 4 к $p=|\tilde{q}_r|$. Разложение идеала $\tilde{q}_r\mathcal{O}_{M_{r-1}}$ на простые идеалы не содержит квадратов. В частности, $\sqrt{\tilde{q}_r}\notin M_{r-1}$, поскольку иначе было бы $(\tilde{q}_r\mathcal{O}_{M_{r-1}})=$

$= (\sqrt{\tilde{q}_r}\mathcal{O}_{M_{r-1}})^2$. Следовательно, $(1, \alpha_r)$ образуют базис M_r над M_{r-1}. Пусть $a + b\alpha_r$ — целое алгебраическое число и $a, b \in M_{r-1}$. Число $a + b(1 - \alpha_r)$ — сопряжённое к $a + b\alpha_r$ и потому тоже является целым алгебраическим. Следовательно, их сумма $x = 2a + b$ и произведение $y = a^2 + ab + b^2(1 - \tilde{q}_r)/4$ также являются целыми алгебраическими и, следовательно, лежат в $\mathcal{O}_{M_{r-1}}$. Далее, $x^2 - 4y = \tilde{q}_r b^2 \in \mathcal{O}_{M_{r-1}}$. Из леммы 3 следует, что $b \in \mathcal{O}_{M_{r-1}}$. Следовательно, $2a \in \mathcal{O}_{M_{r-1}}$, $a^2 + ab \in \mathcal{O}_{M_{r-1}}$, $2a^2 = 2(a^2 + ab) - 2a \cdot b \in \mathcal{O}_{M_{r-1}}$. Применяя леммы 4 и 3 к $p = 2$, получаем $a \in \mathcal{O}_{M_{r-1}}$. Таким образом, если $a + b\alpha_r$ — целое алгебраическое и $a, b \in M_{r-1}$, то $a, b \in \mathcal{O}_{M_{r-1}}$; обратное утверждение очевидно, следовательно, $(1, \alpha_r)$ образуют базис кольца целых M_r над $\mathcal{O}_{M_{r-1}}$, что доказывает индуктивный переход для набора $\alpha_1^{s_1} \dots \alpha_r^{s_r}$. Для доказательства второго утверждения теоремы достаточно заметить, что $(1 - \alpha_r, \alpha_r) = \big((1 - \sqrt{\tilde{q}_r})/2, (1 + \sqrt{\tilde{q}_r})/2\big)$ также образуют базис кольца целых M_r над $\mathcal{O}_{M_{r-1}}$. ■

Теорема 7. Пусть $\tilde{q}_1, \dots, \tilde{q}_{r-1}$ такие же, как в теореме 6, и $\tilde{q}_r = \pm 8$. Обозначим $\alpha_r = \sqrt{\tilde{q}_r/4}$. Тогда следующие множества образуют фундаментальные базисы поля $\mathbb{Q}(\sqrt{\tilde{q}_1}, \dots, \sqrt{\tilde{q}_r})$:

1) числа $\alpha_1^{s_1} \dots \alpha_r^{s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0, 1\}^r$;
2) числа $\tilde{\alpha}_1^{s_1} \alpha_1^{1-s_1} \dots \tilde{\alpha}_{r-1}^{s_{r-1}} \alpha_{r-1}^{1-s_{r-1}} \alpha_r^{s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0, 1\}^r$.

Доказательство. Положим $M = \mathbb{Q}(\sqrt{\tilde{q}_1}, \dots, \sqrt{\tilde{q}_{r-1}})$. Применим лемму 4 к $p = 2$ и теорему 6. Идеал $2\mathbb{Z}$ неразветвлён в M, следовательно, как было показано ранее, $\sqrt{\tilde{q}_r} \notin M$ и $(1, \sqrt{\tilde{q}_r})$ образуют базис $M(\sqrt{\tilde{q}_r})$ над M.

Пусть $a + b\alpha_r$ — целое алгебраическое число и $a, b \in M$. Число $a - b\alpha_r$ — сопряжённое к $a + b\alpha_r$ и потому тоже является целым алгебраическим. Следовательно, их сумма $2a$ и произведение $a^2 \mp 2b^2$ также являются целыми алгебраическими и, следовательно, лежат в $\mathcal{O}_M$. Далее, $(2a)^2 - 4(a^2 \mp 2b^2) = \pm 2(2b)^2 \in \mathcal{O}_M$, по лемме 3 отсюда следует, что $2b \in \mathcal{O}_M$. Теперь $2(a^2 \mp 2b^2) \pm (2b)^2 = 2a^2 \in \mathcal{O}_M$ и, повторно применяя лемму 3, находим $a \in \mathcal{O}_M$. Наконец, $a^2 - (a^2 \mp 2b^2) = \pm 2b^2 \in \mathcal{O}_M$, и третье применение леммы 3 даёт $b \in \mathcal{O}_M$. Таким образом, $(1, \alpha_r)$ образуют базис кольца целых поля $M(\sqrt{q_r^*})$ над $\mathcal{O}_M$, и применение теоремы 6 завершает доказательство. ■

Теорема 8. Пусть $\tilde{q}_1, \dots, \tilde{q}_{r-1}$ такие же, как в теореме 6, и $\tilde{q}_r = -4$. Обозначим $\alpha_r = \sqrt{\tilde{q}_r/4} = i$. Тогда следующие множества образуют фундаментальные базисы поля $\mathbb{Q}(\sqrt{\tilde{q}_1}, \dots, \sqrt{\tilde{q}_r})$:

1) числа $\alpha_1^{s_1} \dots \alpha_r^{s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0, 1\}^r$;
2) числа $\tilde{\alpha}_1^{s_1} \alpha_1^{1-s_1} \dots \tilde{\alpha}_{r-1}^{s_{r-1}} \alpha_{r-1}^{1-s_{r-1}} \alpha_r^{s_r}$, когда набор (s_i) пробегает всевозможные наборы из $\{0, 1\}^r$.

Доказательство. Положим $M = \mathbb{Q}(\sqrt{\tilde{q}_1}, \dots, \sqrt{\tilde{q}_{r-1}})$. Равенство $2 = -i(1 + i)^2$ показывает, что идеал $2\mathbb{Z}$ разветвлён в любом поле, содержащем i. Согласно лемме 4 и теореме 6, $2\mathbb{Z}$ неразветвлён в M. Следовательно, $i \notin M$.

Пусть $a + bi$ — целое алгебраическое число и $a, b \in M$. Число $a - bi$ — сопряжённое к $a + bi$ и потому тоже является целым алгебраическим. Следовательно, их сумма $2a$ и произведение $a^2 + b^2$ также являются целыми алгебраическими и, следовательно, лежат в $\mathcal{O}_M$. Далее, $2(a^2 + b^2) + 2a \cdot 2b = 2(a + b)^2 \in \mathcal{O}_M$ и по леммам 4 и 3, применённым к $p = 2$, и теореме 6 $a + b \in \mathcal{O}_M$. Теперь $2a - (a + b) = a - b \in \mathcal{O}_M$, $(a + b)(a - b) = a^2 - b^2 \in \mathcal{O}_M$, $2a^2 \in \mathcal{O}_M$, $2b^2 \in \mathcal{O}_M$; снова применяя леммы 4 и 3 и теорему 6, получаем $a, b \in \mathcal{O}_M$. Таким образом, $(1, \alpha_t)$ образуют базис кольца целых поля $M(\sqrt{\tilde{q}_r})$ над $\mathcal{O}_M$, и применение теоремы 6 завершает доказательство. ■

Поскольку в каждом случае из теорем следует, что $[K_G : \mathbb{Q}] = 2^t$, то $\sqrt{q_j^*} \notin \mathbb{Q}(\dots, \sqrt{q_{j-1}^*}, \sqrt{q_{j+1}^*}, \dots)$ для любого $1 \leqslant j \leqslant t$. Следовательно, в $\mathrm{Gal}(K_G/\mathbb{Q})$ есть t элементов τ_j, действующих следующим образом:

$$\tau_j\left(\sqrt{q_j^*}\right) = -\sqrt{q_j^*}, \quad \tau_j\left(\sqrt{q_i^*}\right) = \sqrt{q_i^*} \text{ при } i \neq j. \tag{14}$$

Положим $\tau'_\mu = \tau_1^{\mu_1} \dots \tau_t^{\mu_t} \in \mathrm{Gal}(K_G/\mathbb{Q})$ при $\mu \in \{0,1\}^t$; сравнивая действие τ'_μ на $\sqrt{q_i^*}$, легко видеть, что все τ'_μ различны. Получаем $2^t = |\mathrm{Gal}(K_G/\mathbb{Q})|$ различных элементов $\mathrm{Gal}(K_G/\mathbb{Q})$, которые, таким образом, исчерпывают эту группу.

Предыдущие теоремы задают $\mathbb{Z}$-базис $\mathcal{O}_{K_G}$. Нас также будут интересовать пересечение $\mathcal{O}_{K_G}$ с $\mathbb{R}$ (являющееся, очевидно, кольцом целых в поле $K_G \cap \mathbb{R}$) и пересечение $\mathcal{O}_{K_G}$ с $i\mathbb{R}$ (являющееся, очевидно, $\mathbb{Z}$-модулем). Среди q_i^* есть отрицательные числа. Обозначив через u число положительных среди q_i^*, $0 \leqslant u < t$, можно без ограничения общности считать, что $q_1^* > 0, \dots, q_u^* > 0, q_{u+1}^* < 0, \dots, q_t^* < 0$.

Комплексное сопряжение действует на $\sqrt{q_i^*}$ так же, как и композиция $\tau_{u+1} \dots \tau_t$. Поскольку $K_G \cap \mathbb{R}$ — это максимальное подполе K_G, инвариантное относительно комплексного сопряжения, то $\mathrm{Gal}((K_G \cap \mathbb{R})/\mathbb{Q})$ изоморфна фактор-группе $\mathrm{Gal}(K_G/\mathbb{Q})$ по подгруппе, порождённой комплексным сопряжением. Выбирая в качестве представителя смежного класса элемент с $\mu_t = 0$, получаем, что $\mathrm{Gal}((K_G \cap \mathbb{R})/\mathbb{Q})$ состоит из автоморфизмов

$$\tau_\lambda = \tau_{\lambda_1,\dots,\lambda_{t-1}} = \tau'_{\lambda_1,\dots,\lambda_{t-1},0} = \tau_1^{\lambda_1} \dots \tau_{t-1}^{\lambda_{t-1}} \tag{15}$$

при $\lambda \in \{0,1\}^{t-1}$, различных при разных λ.

В дальнейшем из двух значений $\sqrt{d}$ будем выбирать то, которое соответствует произведению $\sqrt{q_1^*} \cdot \ldots \cdot \sqrt{q_t^*}$, где значения отдельных корней такие же, как при вычислении α_i и $\tilde{\alpha}_i$.

Теорема 9. Пусть $q_1^*, \dots, q_t^*$ такие же, как в лемме 2, нечётные, занумерованные так, что $q_i^* > 0$ при $1 \leqslant i \leqslant u$ и $q_i^* < 0$ при $u < i \leqslant t$, где u — некоторое число от 0 до $t-1$ включительно; $K_G = \mathbb{Q}(\sqrt{q_1^*}, \dots, \sqrt{q_t^*})$; τ_λ заданы формулой (15). Тогда

1) числа

$$\beta_{s_1,\dots,s_{t-1}} = \beta_{s_1,\dots,s_{t-1}}(q_1^*, \dots, q_t^*) = \\ = \left(\prod_{i=1}^{u} \tilde{\alpha}_i^{s_i} \alpha_i^{1-s_i}\right)\left(\left(\prod_{i=u+1}^{t-1} \tilde{\alpha}_i^{s_i} \alpha_i^{1-s_i}\right)\alpha_t + \left(\prod_{i=u+1}^{t-1} \tilde{\alpha}_i^{1-s_i} \alpha_i^{s_i}\right)\tilde{\alpha}_t\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют фундаментальный базис поля $K_G \cap \mathbb{R}$;

2) числа

$$\beta^*_{s_1,\dots,s_{t-1}} = \beta^*_{s_1,\dots,s_{t-1}}(q_1^*, \dots, q_t^*) = \\ = \left(\prod_{i=1}^{u} (-\tilde{\alpha}_i)^{s_i} \alpha_i^{1-s_i}\right)\left(\left(\prod_{i=u+1}^{t-1} (-\tilde{\alpha}_i)^{s_i} \alpha_i^{1-s_i}\right)\alpha_t - \left(\prod_{i=u+1}^{t-1} \tilde{\alpha}_i^{1-s_i} (-\alpha_i)^{s_i}\right)\tilde{\alpha}_t\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют базис $\mathbb{Z}$-модуля $\mathcal{O}_{K_G} \cap i\mathbb{R}$;

3) для любых $\eta, \nu \in \{0,1\}^{t-1}$ справедливо равенство

$$\sum_{\mu \in \{0,1\}^{t-1}} (-1)^{\mu_1 + \dots + \mu_{t-1}} \tau_\mu\left(\beta_{\eta_1,\dots,\eta_{t-1}} \beta^*_{\nu_1,\dots,\nu_{t-1}}\right) = \begin{cases} \sqrt{d}, & \text{если } \eta = \nu, \\ 0, & \text{иначе.} \end{cases}$$

Доказательство. Обозначим элемент базиса из п. 2 теоремы 6, соответствующий набору $(s_1, \ldots, s_t)$, через $\beta'_{s_1,\ldots,s_t}$.

Число из $\mathcal{O}_{K_G}$ попадает в пересечение $K_G \cap \mathbb{R}$ тогда и только тогда, когда оно инвариантно относительно комплексного сопряжения. Легко видеть, что комплексное сопряжение переводит $\beta'_{s_1,\ldots,s_t}$ в $\beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_t}$. Таким образом, для инвариантности $\mathbb{Z}$-линейной комбинации $\beta'_{s_1,\ldots,s_t}$ необходимо и достаточно, чтобы для каждого набора (s_i) коэффициенты при $\beta'_{s_1,\ldots,s_t}$ и $\beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_t}$ совпадали. Теперь из теоремы 6 следует, что $\{\beta'_{s_1,\ldots,s_{t-1},0} + \beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_{t-1},1}\}$ образуют требуемый фундаментальный базис. Из определения β' легко видеть, что эта сумма равна $\beta_{s_1,\ldots,s_{t-1}}$, что доказывает первое утверждение теоремы.

Число из $\mathcal{O}_{K_G}$ попадает в пересечение $K_G \cap i\mathbb{R}$ тогда и только тогда, когда оно меняет знак под действием комплексного сопряжения. Аналогично предыдущему получаем, что $\{\beta'_{s_1,\ldots,s_{t-1},0} - \beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_{t-1},1}\}$ образуют требуемый $\mathbb{Z}$-базис. Из определения β' легко видеть, что эта разность равна $\pm\beta^*_{s_1,\ldots,s_{t-1}}$, что доказывает второе утверждение теоремы.

Наконец, третье утверждение проверяется прямой выкладкой. А именно, легко видеть, что

$$\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\right) =$$
$$= \left(\prod_{i=1}^{u} \tilde{\alpha}_i^{\mu_i\oplus\eta_i}\alpha_i^{1-(\mu_i\oplus\eta_i)}\right)\left(\left(\prod_{i=u+1}^{t-1} \tilde{\alpha}_i^{\mu_i\oplus\eta_i}\alpha_i^{1-(\mu_i\oplus\eta_i)}\right)\alpha_t + \left(\prod_{i=u+1}^{t-1} \tilde{\alpha}_i^{1-(\mu_i\oplus\eta_i)}\alpha_i^{\mu_i\oplus\eta_i}\right)\tilde{\alpha}_t\right),$$
$$\tau_\mu\left(\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) = \left(\prod_{i=1}^{u}(-1)^{\nu_i}\tilde{\alpha}_i^{\mu_i\oplus\nu_i}\alpha_i^{1-(\mu_i\oplus\nu_i)}\right)\times$$
$$\times\left(\left(\prod_{i=u+1}^{t-1}(-1)^{\nu_i}\tilde{\alpha}_i^{\mu_i\oplus\nu_i}\alpha_i^{1-(\mu_i\oplus\nu_i)}\right)\alpha_t - \left(\prod_{i=u+1}^{t-1}(-1)^{\nu_i}\tilde{\alpha}_i^{1-(\mu_i\oplus\nu_i)}\alpha_i^{\mu_i\oplus\nu_i}\right)\tilde{\alpha}_t\right).$$

Подставим эти формулы в произведение $\tau_\mu(\beta_{\eta_1,\ldots,\eta_{t-1}})\tau_\mu(\beta^*_{\nu_1,\ldots,\nu_{t-1}})$, получим формулу вида $(a+b)(c-d)$, в которой раскроем скобки, получив четыре слагаемых $ac+bc-ad-bd$. Под δ_{ij} будем понимать символ Кронекера: $\delta_{ii} = 1, \delta_{ij} = 0$ при $i \neq j$. Заметим, что

$$\sum_{\mu_i=0}^{1}(-1)^{\mu_i}(-1)^{\nu_i}\tilde{\alpha}_i^{(\mu_i\oplus\eta_i)+(\mu_i\oplus\nu_i)}\alpha_i^{1-(\mu_i\oplus\eta_i)+1-(\mu_i\oplus\nu_i)} =$$
$$= (-1)^{\nu_i}\left(\tilde{\alpha}_i^{\eta_i+\nu_i}\alpha_i^{2-(\eta_i+\nu_i)} - \tilde{\alpha}_i^{2-(\eta_i+\nu_i)}\alpha_i^{\eta_i+\nu_i}\right) = \delta_{\eta_i\nu_i}\left(\alpha_i^2 - \tilde{\alpha}_i^2\right) = \delta_{\eta_i\nu_i}\sqrt{q_i^*},$$
$$\sum_{\mu_i=0}^{1}(-1)^{\mu_i}(-1)^{\nu_i}\tilde{\alpha}_i^{1-(\mu_i\oplus\eta_i)+(\mu_i\oplus\nu_i)}\alpha_i^{(\mu_i\oplus\eta_i)+1-(\mu_i\oplus\nu_i)} =$$
$$= (-1)^{\nu_i}\left(\tilde{\alpha}_i^{1-\eta_i+\nu_i}\alpha_i^{1+\eta_i-\nu_i} - \tilde{\alpha}_i^{1+\eta_i-\nu_i}\alpha_i^{1-\eta_i+\nu_i}\right) = \delta_{\eta_i+\nu_i,1}\left(\alpha_i^2 - \tilde{\alpha}_i^2\right) = \delta_{\eta_i+\nu_i,1}\sqrt{q_i^*}$$

и перестановка α_i и $\tilde{\alpha}_i$ даёт ещё два рассматриваемых произведения, которые совпадают с предыдущими, умноженными на (-1).

Таким образом,

$$\sum_{\mu\in\{0,1\}^{t-1}}(-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) =$$
$$= \left(\prod_{i=1}^{u}\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)\left(\alpha_t^2\prod_{i=u+1}^{t-1}\delta_{\eta_i\nu_i}\sqrt{q_i^*} + \tilde{\alpha}_t\alpha_t\prod_{i=u+1}^{t-1}\delta_{\eta_i+\nu_i,1}\sqrt{q_i^*} -\right.$$
$$\left. -\alpha_t\tilde{\alpha}_t\prod_{i=u+1}^{t-1}\left(-\delta_{\eta_i+\nu_i,1}\sqrt{q_i^*}\right) - \tilde{\alpha}_t^2\prod_{i=u+1}^{t-1}\left(-\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)\right).$$

Знак произведения $q_1^* \cdot \ldots \cdot q_t^*$ определяется чётностью количества отрицательных множителей, которых ровно $t-u$. Таким образом, из условия $q_1^* \ldots q_t^* < 0$ следует, что $t-u$ нечётно и $\prod\limits_{i=u+1}^{t-1}(-1) = (-1)^{t-u-1} = 1$;

$$\sum_{\mu\in\{0,1\}^{t-1}} (-1)^{\mu_1+\ldots+\mu_{t-1}} \tau_\mu \left(\beta_{\eta_1,\ldots,\eta_{t-1}} \beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) =$$
$$= \left(\prod_{i=1}^{u} \delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)(\alpha_t^2 - \tilde{\alpha}_t^2)\left(\prod_{i=u+1}^{t-1} \delta_{\eta_i\nu_i}\sqrt{q_i^*}\right) = \sqrt{q_t^*}\prod_{i=1}^{t-1}\delta_{\eta_i\nu_i}\sqrt{q_i^*}.$$

Теорема доказана. ■

Теорема 10. Пусть $q_2^*, \ldots, q_t^*$ такие же, как в теореме 9, и $q_1^* = 8$. Пусть q_i^* занумерованы так, что $q_i^* > 0$ при $1 \leqslant i \leqslant u$ и $q_i^* < 0$ при $u < i \leqslant t$, где u — некоторое число от 1 до $t-1$ включительно; $K_G = \mathbb{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$; τ_λ заданы формулой (15). Тогда

1) числа

$$\beta_{s_1,\ldots,s_{t-1}} = \beta_{s_1,\ldots,s_{t-1}}(q_1^*, \ldots, q_t^*) = \sqrt{2}^{s_1}\left(\prod_{i=2}^{u}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i}\right)\times$$
$$\times\left(\left(\prod_{i=u+1}^{t-1}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i}\right)\alpha_t + \left(\prod_{i=u+1}^{t-1}\tilde{\alpha}_i^{1-s_i}\alpha_i^{s_i}\right)\tilde{\alpha}_t\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют фундаментальный базис поля $K_G \cap \mathbb{R}$;

2) числа

$$\beta^*_{s_1,\ldots,s_{t-1}} = \beta^*_{s_1,\ldots,s_{t-1}}(q_1^*, \ldots, q_t^*) = \sqrt{2}^{1-s_1}\left(\prod_{i=2}^{u}(-\tilde{\alpha}_i)^{s_i}\alpha_i^{1-s_i}\right)\times$$
$$\times\left(\left(\prod_{i=u+1}^{t-1}(-\tilde{\alpha}_i)^{s_i}\alpha_i^{1-s_i}\right)\alpha_t - \left(\prod_{i=u+1}^{t-1}\tilde{\alpha}_i^{1-s_i}(-\alpha_i)^{s_i}\right)\tilde{\alpha}_t\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют базис $\mathbb{Z}$-модуля $\mathcal{O}_{K_G} \cap i\mathbb{R}$;

3) для любых $\nu, \eta \in \{0,1\}^{t-1}$ справедливо равенство

$$\sum_{\mu\in\{0,1\}^{t-1}} (-1)^{\mu_1+\ldots+\mu_{t-1}} \tau_\mu \left(\beta_{\eta_1,\ldots,\eta_{t-1}} \beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) = \begin{cases}\sqrt{d}, & \text{если } \eta = \nu,\\ 0, & \text{иначе.}\end{cases}$$

Доказательство аналогично доказательству теоремы 9. При вычислении выражения из третьего утверждения теоремы по сравнению с теоремой 9 возникает дополнительный множитель

$$\sum_{\mu_1=0}^{1}(-1)^{\mu_1}\left((-1)^{\mu_1}\sqrt{2}\right)^{\eta_1}\left((-1)^{\mu_1}\sqrt{2}\right)^{1-\nu_1} = \sqrt{2}^{1+\eta_1-\nu_1}\left(1+(-1)^{\eta_1+\nu_1}\right) = 2\sqrt{2}\delta_{\eta_1\nu_1}.$$ ■

Теорема 11. Пусть $q_1^*, \ldots, q_{t-1}^*$ такие же, как в теореме 9, и $q_t^* \in \{-4, -8\}$. Пусть q_i^* занумерованы так, что $q_i^* > 0$ при $1 \leqslant i \leqslant u$ и $q_i^* < 0$ при $u < i \leqslant t$, где u — некоторое число от 0 до $t-2$ включительно; $K_G = \mathbb{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$; τ_λ заданы формулой (15). Тогда

1) числа

$$\beta_{s_1,\ldots,s_{t-1}} = \beta_{s_1,\ldots,s_{t-1}}(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) = \left(\prod_{i=1}^{u}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i}\right)\times$$
$$\times\left(\left(\prod_{i=u+1}^{t-2}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i}\right)\alpha_{t-1}\alpha_t^{s_{t-1}} + \left(\prod_{i=u+1}^{t-2}\tilde{\alpha}_i^{1-s_i}\alpha_i^{s_i}\right)\tilde{\alpha}_{t-1}(-\alpha_t)^{s_{t-1}}\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют фундаментальный базис поля $K_G \cap \mathbb{R}$;

2) числа

$$\beta^*_{s_1,\ldots,s_{t-1}} = \beta^*_{s_1,\ldots,s_{t-1}}(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) = \left(\prod_{i=1}^{u}(-\tilde{\alpha}_i)^{s_i}\alpha_i^{1-s_i}\right)\times$$
$$\times\left(\left(\prod_{i=u+1}^{t-2}(-\tilde{\alpha}_i)^{s_i}\alpha_i^{1-s_i}\right)\alpha_{t-1}\alpha_t^{1-s_{t-1}} - \left(\prod_{i=u+1}^{t-2}\tilde{\alpha}_i^{1-s_i}(-\alpha_i)^{s_i}\right)\tilde{\alpha}_{t-1}(-\alpha_t)^{1-s_{t-1}}\right),$$

когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют базис $\mathbb{Z}$-модуля $\mathcal{O}_{K_G} \cap i\mathbb{R}$;

3) для любых $\eta,\nu \in \{0,1\}^{t-1}$ справедливо равенство

$$\sum_{\mu\in\{0,1\}^{t-1}}(-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) = \begin{cases}\sqrt{d}, & \text{если } \eta=\nu,\\ 0, & \text{иначе.}\end{cases}$$

Доказательство. Обозначим элемент базиса из п. 2 теоремы 8, соответствующий набору $(s_1,\ldots,s_t)$, через $\beta'_{s_1,\ldots,s_t}$.

Число из кольца целых поля K_G попадает в пересечение этого поля с $\mathbb{R}$ тогда и только тогда, когда оно инвариантно относительно комплексного сопряжения. Легко видеть, что комплексное сопряжение переводит $\beta'_{s_1,\ldots,s_t}$ в $(-1)^{s_t}\beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_{t-1},s_t}$. Следовательно, для инвариантности линейной комбинации $\beta'_{s_1,\ldots,s_t}$ с коэффициентами из $\mathbb{Z}$ необходимо и достаточно, чтобы для каждого набора (s_i) коэффициенты при $\beta'_{s_1,\ldots,s_t}$ и $\beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_{t-1},s_t}$ отличались друг от друга умножением на $(-1)^{s_t}$. Теперь из теоремы 8 следует, что $\{\beta'_{s_1,\ldots,s_{t-2},0,s_t} + (-1)^{s_t}\beta'_{s_1,\ldots,s_u,1-s_{u+1},\ldots,1-s_{t-2},1,s_t}\}$ образуют требуемый фундаментальный базис. Из определения β' легко видеть, что эта сумма равна $\beta_{s_1,\ldots,s_{t-2},s_t}$, что доказывает первое утверждение теоремы.

Доказательство второго утверждения аналогично первому.

Третье утверждение доказывается явной выкладкой. Аналогично доказательству теоремы 9 находим

$$\sum_{\mu\in\{0,1\}^{t-1}}(-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) =$$
$$= \left(\prod_{i=1}^{u}\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)\alpha_t^{\eta_{t-1}+1-\nu_{t-1}}\left(\sqrt{q_{t-1}^*}\prod_{i=u+1}^{t-2}\delta_{\eta_i\nu_i}\sqrt{q_i^*} + \right.$$
$$\left. +(-1)^{\nu_{t-1}+\eta_{t-1}}(-\sqrt{q_{t-1}^*})\prod_{i=u+1}^{t-2}\left(-\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)\right).$$

Поскольку $q_1^* \dots q_t^* < 0$, то количество отрицательных среди q_i^*, то есть $t-u$, нечётно и, следовательно, $\prod\limits_{i=u+1}^{t-2}(-1) = (-1)^{t-u-2} = -1$. Тогда

$$\sum_{\mu\in\{0,1\}^{t-1}} (-1)^{\mu_1+\dots+\mu_{t-1}} \tau_\mu\left(\beta_{\eta_1,\dots,\eta_{t-1}}\beta^*_{\nu_1,\dots,\nu_{t-1}}\right) =$$
$$= \left(\prod_{i=1}^{t-2}\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)(1+(-1)^{\nu_{t-1}+\eta_{t-1}})\alpha_t^{1+\eta_{t-1}-\nu_{t-1}} = \delta_{\eta_{t-1}\nu_{t-1}}\left(\prod_{i=1}^{t-2}\delta_{\eta_i\nu_i}\sqrt{q_i^*}\right)2\alpha_t.$$

Теорема доказана. ■

Теорема 12. Пусть $q_1^*, \dots, q_{t-1}^*$ нечётные положительные, $q_t^* = -4$ или $q_t^* = -8$. Тогда

1) числа $\beta_{s_1,\dots,s_{t-1}} = \beta_{s_1,\dots,s_{t-1}}(q_1^*,\dots,q_t^*) = \prod\limits_{i=1}^{t-1}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i}$, когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют фундаментальный базис поля $K_G\cap\mathbb{R}$;
2) числа $\beta^*_{s_1,\dots,s_{t-1}} = \beta^*_{s_1,\dots,s_{t-1}}(q_1^*,\dots,q_t^*) = \left(\prod\limits_{i=1}^{t-1}(-\tilde{\alpha}_i)^{s_i}\alpha_i^{1-s_i}\right)\sqrt{q_t^*}$, когда набор (s_i) пробегает всевозможные наборы из $\{0,1\}^{t-1}$, образуют базис $\mathbb{Z}$-модуля $\mathcal{O}_{K_G}\cap i\mathbb{R}$;
3) для любых $\eta,\nu\in\{0,1\}^{t-1}$ справедливо равенство

$$\sum_{\mu\in\{0,1\}^{t-1}} (-1)^{\mu_1+\dots+\mu_{t-1}} \tau_\mu\left(\beta_{\eta_1,\dots,\eta_{t-1}}\beta^*_{\nu_1,\dots,\nu_{t-1}}\right) = \begin{cases}\sqrt{d}, & \text{если } \eta=\nu,\\ 0, & \text{иначе.}\end{cases}$$

Доказательство. Очевидно, что в условиях теоремы $K_G = M(\sqrt{q_t^*})$, где $M\subset\mathbb{R}$. Следовательно, $K_G\cap\mathbb{R} = M$, $K_G\cap i\mathbb{R} = \sqrt{q_t^*}\cdot M$. Первые два утверждения следуют из теоремы 6, третье доказывается выкладкой, аналогичной доказательству теоремы 9. ■

Будем обозначать $\beta_\mu = \beta_{\mu_1,\dots,\mu_{t-1}}$ при $\mu\in\{0,1\}^{t-1}$. Множество $\{\beta_\mu\}$ образует фундаментальный базис поля $K_G\cap\mathbb{R}$, которое в дальнейшем будем обозначать $\mathcal{M}$.

Пусть z — произвольный элемент $\mathcal{O}_{K_G}$. Поскольку $z\in K_G$, то и $\overline{z}\in K_G$, так что $z+\overline{z} = 2\operatorname{Re} z\in K_G\cap\mathbb{R}$ и $z-\overline{z} = 2i\operatorname{Im} z\in K_G\cap i\mathbb{R}$. Более того, z и, следовательно, $\overline{z}$ являются целыми алгебраическими, а потому $2\operatorname{Re} z$ и $2i\operatorname{Im} z$ также являются целыми алгебраическими. Таким образом, $2\operatorname{Re} z = \sum\limits_\mu b_\mu\beta_\mu$ и $2i\operatorname{Im} z = \sum\limits_\mu b'_\mu\beta^*_\mu$. Здесь и далее, если явным образом не указано множество значений параметра, записанного греческой буквой, подразумевается $\{0,1\}^{t-1}$. Опишем, как по приближённому значению таких сумм находить наборы чисел b_μ и b'_μ. Числа β_μ образуют базис вещественного поля $\mathcal{M}$, базис β^*_μ чисто мнимый и становится базисом того же поля $\mathcal{M}$ после деления, например, на $\sqrt{q_t^*}\in K_G$, $q_t^*<0$. Таким образом, можно найти точное выражение для z по приближённому значению, если уметь решать задачу восстановления целых коэффициентов разложения вещественного числа, заданного с некоторой точностью, по вещественному базису.

Дальнейший план изложения таков.

— Выделим в $\mathcal{O}_{K_G}[x]$ делитель многочлена $H_D[\theta,\alpha_*]$ степени $h/2^{t-1}$, который будем рассматривать вместо многочлена $H_D[\theta,\alpha_*]$. Это позволит уменьшить число вычисляемых коэффициентов и их величину. Этому посвящён п. 4.
— Оценим сверху все сопряжённые числа к коэффициентам рассматриваемого многочлена (п. 5).

— Основная идея для восстановления коэффициентов — использовать рациональные приближения к элементам базиса с одним и тем же знаменателем достаточной точности в зависимости от оценки из п. 5. Построению таких приближений для случая β_μ и β_μ^* посвящён п. 6.
— Далее в п. 7 опишем, как при помощи этих рациональных приближений точно определить коэффициенты рассматриваемого многочлена, вычисленные по определению с некоторой точностью.

4. Делитель многочлена $H_D[\theta, \alpha_*](x)$

Пусть $\tilde{\mathfrak{a}} \in \mathcal{H}_D$. Выберем форму (A, B, C) так, чтобы $\mathfrak{h}(A, B, C) = \tilde{\mathfrak{a}}$ и $\gcd(A, D) = 1$; это возможно, поскольку $\mathfrak{h}$ зависит только от класса эквивалентности формы, а в каждом классе эквивалентных форм, согласно [5, Lemma 2.25, Lemma 2.3], есть представитель (A, B, C) с $\gcd(A, D) = 1$. Определим отображение $\varphi : \mathcal{H}_D \to \{\pm 1\}^t$ следующей формулой:

$$\varphi(\tilde{\mathfrak{a}}) = \left(\left(\frac{q_1^*}{A} \right), \ldots, \left(\frac{q_t^*}{A} \right) \right).$$

Это определение корректно, поскольку отображение Артина зависит только от класса идеала в $I(\mathcal{O}, f)/P_{K,\mathbb{Z}}(f)$, из теоремы 5 следует, что $\left(\frac{q_i^*}{A} \right)$ не меняется при замене формы (A, B, C) на эквивалентную с сохранением условия $\gcd(A, D) = 1$.

Теорема 13. Образ отображения φ совпадает с группой $\{(\varepsilon_1, \ldots, \varepsilon_t) \in \{\pm 1\}^t : \prod_i \varepsilon_i = 1\}$ с покомпонентным умножением. Отображение φ является гомоморфизмом групп. Поле инвариантов $L^{\Omega(\operatorname{Ker}\varphi)} = \{x \in L : \tau(x) = x \text{ для всех } \tau \in \Omega(\operatorname{Ker}\varphi)\}$ есть $K(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$.

Доказательство. То, что φ является гомоморфизмом, следует из п. 3 теоремы 5 и того, что отображение Артина является гомоморфизмом.

Проверим, что для любого элемента из образа φ произведение его компонент равно 1. Рассмотрим идеал $\mathfrak{a}$, определённый, как в теореме 5, для формы (A, B, C). Тогда

$$\left(\frac{q_i^*}{A} \right) = \frac{1}{\sqrt{q_i^*}} \left(\frac{L/K}{\Omega_1(\mathfrak{a})} \right) (\sqrt{q_i^*})$$

и, перемножая эти равенства по всем i, с учётом леммы 2 находим

$$\left(\frac{q_1^*}{A} \right) \cdot \ldots \cdot \left(\frac{q_t^*}{A} \right) = \frac{1}{\sqrt{d}} \left(\frac{L/K}{\Omega_1(\mathfrak{a})} \right) (\sqrt{d}).$$

Но $\sqrt{d} \in K$, а $\left(\frac{L/K}{\Omega_1(\mathfrak{a})} \right)$, будучи элементом $\operatorname{Gal}(L/K)$, оставляет на месте элементы K.

Проверим, что подгруппа $\Omega(\operatorname{Ker}\varphi)$ оставляет на месте элементы $\sqrt{q_i^*}$. Пусть $\varphi(\tilde{\mathfrak{a}}) = (1, \ldots, 1)$, $\mathfrak{a}$ — представитель $\tilde{\mathfrak{a}}$ из п. 2 теоремы 5. Тогда

$$\left(\frac{L/K}{\Omega_1(\mathfrak{a})} \right) (\sqrt{q_i^*}) = \sqrt{q_i^*},$$

то есть образ $\Omega_1(\mathfrak{a})$ при отображении Артина, равный $\Omega(\tilde{\mathfrak{a}})$ в силу коммутативности диаграммы (12), действует на $\sqrt{q_i^*}$ тривиально, что и требовалось доказать.

Таким образом,

$$\operatorname{Im}\varphi \subset \left\{(\varepsilon_1,\ldots,\varepsilon_t)\in\{\pm1\}^t : \prod_i \varepsilon_i = 1\right\}, \quad K(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) \subset L^{\Omega(\operatorname{Ker}\varphi)}.$$

В силу теории Галуа $\operatorname{Gal}(L^{\Omega(\operatorname{Ker}\varphi)}/K) \cong \operatorname{Gal}(L/K)/\Omega(\operatorname{Ker}\varphi) \cong \mathcal{H}_D/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$, в частности $[L^{\Omega(\operatorname{Ker}\varphi)} : K] = |\operatorname{Im}\varphi| \leqslant 2^{t-1}$. В п. 3 доказано, что $[K(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) : \mathbb{Q}] = 2^t$. Отсюда $[K(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) : K] = 2^{t-1}$. Поскольку $[K(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) : K] \leqslant [L^{\Omega(\operatorname{Ker}\varphi)} : K] = |\operatorname{Im}\varphi| \leqslant 2^{t-1}$, это возможно только когда $|\operatorname{Im}\varphi| = 2^{t-1}$ и $K(\sqrt{q_1^*},\ldots,\sqrt{q_t^*}) = L^{\Omega(\operatorname{Ker}\varphi)}$. ■

Будем вычислять вместо многочлена $H_D[\theta,\alpha_*]$ его делитель

$$\hat{H}_D[\theta,\alpha_*](x) = \prod_{i:\varphi(\mathfrak{h}(A_i,B_i,C_i))=(1,\ldots,1)} (x-\theta(\alpha_i)), \tag{16}$$

где набор $\{(A_i,B_i,C_i)\}$ является N-системой, соответствующей функции θ (т. е. удовлетворяющей условию той из теорем 2–4, которая применима к θ), а α_i — корень формы (A_i,B_i,C_i).

Главная возникающая здесь трудность состоит в том, что $\hat{H}_D[\theta,\alpha_*]$ не инвариантен относительно $\operatorname{Gal}(L/K)$. Из формулы (10) и того, что φ — гомоморфизм, легко видеть, что автоморфизмы из $\Omega(\operatorname{Ker}\varphi)$ оставляют на месте $\hat{H}_D[\theta,\alpha_*](x)$; таким образом, его коэффициенты лежат в K_G. По теоремам 2–4 все числа $\theta(\alpha)$ целые алгебраические, так что коэффициенты $\hat{H}_D[\theta,\alpha_*]$ тоже целые алгебраические. Следовательно, для использования многочлена $\hat{H}_D[\theta,\alpha_*]$ в методе комплексного умножения нужно уметь восстанавливать целое алгебраическое число из K_G по его достаточно точному комплексному приближению. После получения представления коэффициентов $\hat{H}_D[\theta,\alpha_*]$ в виде точного разложения по базису $\mathcal{O}_{K_G}$ дальнейшие действия для генерации эллиптической кривой точно такие же, как и в исходном варианте.

Следует отметить, что поле родов для генерации эллиптических кривых уже рассматривалось в 1993 г. в [4], где трудность восстановления точного значения z одного коэффициента многочлена $\hat{H}_D[\theta,\alpha_*]$ по приближённому значению преодолевается следующим образом: приближённо вычисляются все сопряжённые значения к z, после чего z ищется в виде разложения по некоторой системе образующих $\mathcal{O}_{K_G}$ с неопределёнными целыми коэффициентами b_i; поскольку целые коэффициенты инвариантны относительно $\operatorname{Gal}(K_G/K)$, то все числа, сопряжённые к z, тоже выражаются через b_i, откуда можно приближённо найти систему линейных уравнений на b_i. Отметим, что этот подход требует вычисления $\theta(\alpha_i)$ для корней всех форм N-системы и всех сопряжённых многочленов к $\hat{H}_D[\theta,\alpha_*]$. Тем самым получается экономия не в количестве коэффициентов, а только в их величине.

В предлагаемом подходе требуется вычисление только многочлена $\hat{H}_D[\theta,\alpha_*]$; в частности, достаточно вычислить $\theta(\alpha_i)$ только для таких корней форм $\mathfrak{a}$, для которых $\varphi(\mathfrak{h}(\mathfrak{a})) = (1,\ldots,1)$. Из теоремы 13 очевидным образом следует, что таких корней в 2^{t-1} раз меньше, чем размер N-системы.

5. Оценка коэффициентов многочлена $\hat{H}_D[\theta,\alpha_*]$

В теоремах 9–12 доказано, что каждый коэффициент многочлена $\hat{H}_D[\theta,\alpha_*]$ представляется в виде $\frac{1}{2}\left(\sum_\mu b_\mu\beta_\mu + \sum_\mu b'_\mu\beta^*_\mu\right)$, где $b_\mu, b'_\mu \in \mathbb{Z}$, $\beta_\mu \in \mathbb{R}$, $\beta^*_\mu \in i\mathbb{R}$. Оценим

величины b_μ и b'_μ. Для этого сначала получим оценку на максимум модуля всех сопряжённых, т. е.

$$\left|\frac{1}{2}\tau'_\lambda\left(\sum_\mu b_\mu\beta_\mu+\sum_\mu b'_\mu\beta^*_\mu\right)\right|\leqslant T_0.$$

Отметим, что многочлен $\hat{H}_D[j,\alpha_*]$ не зависит от набора α_*, так что правомерно короткое обозначение $\hat{H}_D[j]=\hat{H}_D[j,\alpha_*]$.

Для получения теоретических оценок применим метод из [21].

Наряду с многочленом $\hat{H}_D[j]$ будем рассматривать также при $\varphi_0\in\{0,1\}^t$ многочлены

$$\hat{H}_{D,\varphi_0}[j](x)=\prod_{i:\varphi(\mathfrak{h}(A_i,B_i,C_i))=\varphi_0}(x-j(\alpha_i)),\tag{17}$$

где, как и раньше, (A_i,B_i,C_i) пробегает представителей всех классов форм, а α_i — корень (A_i,B_i,C_i).

По определению $\hat{H}_D[j]=\hat{H}_{D,(1,\ldots,1)}[j]$. По тем же причинам, что и для $\hat{H}_D[j]$, при всех φ_0 многочлен $\hat{H}_{D,\varphi_0}[j]$ лежит в $\mathcal{O}_{K_G}[x]$. Более того, если $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$ — автоморфизм, соответствующий классу идеалов $\mathfrak{b}\in\mathcal{H}_D$, то в силу следствия из утверждения 1 $\hat{H}_{D,\varphi_0}[j]^\sigma=\hat{H}_{D,\varphi_0\varphi(\mathfrak{b})^{-1}}[j]$. Поскольку любой автоморфизм поля K_G продолжается до элемента из $\mathrm{Gal}(L/\mathbb{Q})$, то для любого $\tau\in\mathrm{Gal}(K_G/\mathbb{Q})$ найдётся $\varphi_0=\varphi_0(\tau)$ (фиксируем одно из продолжений), такое, что $\hat{H}_{D,\varphi_1}[j]^\tau=\hat{H}_{D,\varphi_1\varphi_0(\tau)}[j]$ для любого $\varphi_1\in\{\pm1\}^t$.

Теорема 14. Каждый коэффициент многочлена $\hat{H}_{D,\varphi_0}[j]$ по модулю не превосходит

$$\exp\left(c_5h+c_1N\left(\ln^2N+4\gamma\ln N+c_6+\frac{\ln N+\gamma+1}{N}\right)\right)\leqslant$$
$$\leqslant\exp\left(c_1N\ln^2N+c_2N\ln N+c_3N+c_1\ln N+c_4\right)=T_0,$$

где $N=\sqrt{|D|/3}$; $\gamma=0{,}577...$ — константа Эйлера; $c_1=\sqrt{3}\pi=5{,}441...$; $c_2=18{,}587...$; $c_3=17{,}442...$; $c_4=11{,}594...$; $c_5=3{,}011...$; $c_6=2{,}566...$ Асимптотическая верхняя оценка

$$T_0=\exp\mathrm{O}\left(\sqrt{|D|}\ln^2|D|\right)$$

также выполняется для других функций θ.

Доказательство. Будем следовать [21, Section 4].

В произведении из (17) можно считать, что (A_i,B_i,C_i) — приведённые формы (поскольку замена формы на эквивалентную соответствует некоторому $SL_2(\mathbb{Z})$-преобразованию корня формы, а j инвариантен относительно таких преобразований). Оценим для приведённой формы (A,B,C) значение $j\left((-B+\sqrt{D})/(2A)\right)$. Аргумент функции j находится в области $\{z\in\mathbb{H}:|z|\geqslant1,|\operatorname{Re}z|\leqslant1/2\}$. Следовательно, $\operatorname{Im}z\geqslant\sqrt{3}/2$ и $|q|=|\mathrm{e}^{2\pi iz}|\leqslant\mathrm{e}^{-\pi\sqrt{3}}$. Далее,

$$j(z)=\frac{1}{q}+744+\sum_{m=1}^{\infty}c_mq^m,$$

где коэффициенты ряда Фурье, согласно [22], оцениваются как $|c_m|\leqslant\dfrac{e^{4\pi\sqrt{m}}}{\sqrt{2}m^{3/4}}$. Следовательно,

$$\left|j\left(\frac{-B+\sqrt{D}}{2A}\right)-\frac{1}{q}\right|\leqslant744+\sum_{m=1}^{\infty}\frac{e^{4\pi\sqrt{m}}}{\sqrt{2}m^{3/4}}e^{-\pi\sqrt{3}m}=k_1=2114{,}566...$$

и $\left|j\left((-B+\sqrt{D})/(2A)\right)\right| \leqslant 1/|q|+k_1 \leqslant k_2/|q|$, где $k_2 = 1+k_1e^{-\pi\sqrt{3}} = 10{,}163...$

Перенумеруем приведённые формы так, чтобы $\{(A_i,B_i,C_i) : 1 \leqslant i \leqslant \deg \hat{H}_D[j]\}$ — все приведённые формы, по которым вычисляется произведение (17), — были расположены в порядке возрастания $|1/q_i| = e^{\pi\sqrt{|D|}/A_i}$. Тогда коэффициент при x^k многочлена $\hat{H}_{D,\varphi_0}[j]$ по модулю не превосходит

$$C^k_{\deg \hat{H}_D[j]} \prod_{i=k+1}^{\deg \hat{H}_D[j]} \frac{k_2}{|q_i|} \leqslant (2k_2)^{h/2^{t-1}} \prod_{i=1}^{h/2^{t-1}} e^{\pi\sqrt{|D|}/A_i}.$$

Следовательно, логарифм любого коэффициента $\hat{H}_{D,\varphi_0}[j]$ не превосходит

$$\frac{h}{2^{t-1}}\ln(2k_2) + \pi\sqrt{|D|}\sum_{i=1}^{h/2^{t-1}}\frac{1}{A_i} \leqslant h\ln(2k_2) + \pi\sqrt{|D|}\sum_{i=1}^{h}\frac{1}{A_i}.$$

Оценка для последней суммы, вычисленная в [21, Theorem 1.2], завершает доказательство для j. Оценки для других функций θ следуют из доказанной оценки и [23, Proposition 3]. ■

На практике будем использовать эвристические, но более точные оценки.

В [23] в качестве эвристической оценки сверху, достаточно близкой к точному значению, для логарифмов модулей коэффициентов многочлена $H_D[j]$ предлагается сумма

$$\pi\sqrt{|D|}\sum_{(A,B,C)}\frac{1}{A},$$

где сумма берётся по всем приведённым формам. Там же в качестве аналогичной оценки, соответствующей θ вместо j, предлагается эта же сумма, умноженная на некоторую константу, зависящую только от выбранного инварианта θ, а именно на отношение степеней $\deg_j \Phi/\deg_\theta \Phi$, где многочлен от двух переменных Φ связывает функции θ и j так, что $\Phi(\theta(z), j(z)) = 0$.

Тривиальные изменения рассуждений из [23] применительно к многочлену $\hat{H}_D[j]$ дают эвристическую оценку

$$\ln T_0 \sim \pi\sqrt{|D|}\max_{\varepsilon\in\{\pm1\}^t}\sum_{(A,B,C):\varphi(\mathfrak{h}(A,B,C))=\varepsilon}\frac{1}{A} \tag{18}$$

при использовании инварианта j. При использовании других функций θ следует умножить оценку на $\deg_j \Phi/\deg_\theta \Phi$.

Пусть $z = \left(\sum_\mu b_\mu\beta_\mu + \sum_\mu b'_\mu\beta^*_\mu\right)/2$ — коэффициент многочлена $\hat{H}_{D,\varphi_0}[j]$, $b_\mu, b'_\mu \in \mathbb{Z}$. Как было отмечено выше, действие группы $\mathrm{Gal}(K_G/\mathbb{Q})$ переводит многочлен $\hat{H}_{D,\varphi_1}[j]$ в многочлен того же вида, поэтому для любого $\lambda \in \{0,1\}^t$ справедливо неравенство

$$|\tau'_\lambda(z)| \leqslant T_0.$$

6. Построение рациональных приближений к базису кольца целых

Для построения совместных приближений существуют различные универсальные алгоритмы, изучению которых посвящена работа [24]; на практике характеристики получаемых приближений существенно различаются для разных алгоритмов, для практических целей, по-видимому, наилучшим является алгоритм скалярных произведений из [24, Chapter 6A]. К сожалению, для универсальных алгоритмов довольно трудно получить теоретические оценки качества. Поэтому мы предлагаем алгоритм, подходящий только для наборов чисел нужного вида, работающий на практике примерно столь же хорошо, сколь и алгоритм скалярных произведений, и допускающий теоретические оценки.

Основная часть следующей теоремы по существу содержится в работе [25]. Основные её отличия от рассуждений в [25] заключаются в явной формулировке (в том числе явных константах), введении функции $\mathfrak{M}$ ([25] оперирует двойственными базисами, что эквивалентно $\mathfrak{M} = 1$) и специализацией для интересующего нас случая ([25] не требует нормальности расширения $M/\mathbb{Q}$ и содержит также обратную теорему).

Теорема 15. Пусть $M \subset \mathbb{R}$ — поле, такое, что $M/\mathbb{Q}$ — расширение Галуа степени m. Пусть $W_1, \dots, W_m$ и $W_1^*, \dots, W_m^*$ — два $\mathbb{Q}$-базиса M и $\mathfrak{M} : \mathrm{Gal}(M/\mathbb{Q}) \to \mathbb{R}$ — функция (необязательно гомоморфизм), такие, что для всех $1 \leqslant l, l' \leqslant m$ выполнено равенство

$$\sum_{\tau \in \mathrm{Gal}(M/\mathbb{Q})} \mathfrak{M}(\tau)\tau(W_l W_{l'}^*) = \begin{cases} 1, & \text{если } l = l', \\ 0, & \text{если } l \neq l'. \end{cases}$$

Обозначим

$$C = \sum_{\substack{\tau \in \mathrm{Gal}(M/\mathbb{Q}) \\ \tau \neq Id}} |\mathfrak{M}(\tau)\tau(W_1)|$$

и при $i = 2, \dots, m$

$$C_i = \sum_{\substack{\tau \in \mathrm{Gal}(M/\mathbb{Q}) \\ \tau \neq Id}} \left| \mathfrak{M}(\tau) \left(\tau(W_i) - W_i \tfrac{\tau(W_1)}{W_1} \right) \right|.$$

Пусть также положительное число Δ и целые числа $\Lambda_1, \dots, \Lambda_m$ таковы, что

$$\sum_{i=1}^m \Lambda_i W_i^* = Z \geqslant 1, \quad \left| \tau \left(\sum_{i=1}^m \Lambda_i W_i^* \right) \right| \leqslant \frac{\Delta}{Z^{\frac{1}{m-1}}} \quad \text{для всех } \tau \in \mathrm{Gal}(M/\mathbb{Q}), \tau \neq Id.$$

Тогда

— справедливо неравенство $|\Lambda_1| \geqslant |\mathfrak{M}(Id)W_1|Z - C\Delta$;
— если $|\Lambda_1| > C\Delta$, то $\mathfrak{M}(Id) \neq 0$ и при всех $i = 2, \dots, m$ справедлива оценка

$$\left| \frac{\Lambda_i}{\Lambda_1} - \frac{W_i}{W_1} \right| \leqslant C_i \frac{\Delta}{|\Lambda_1| \left(\frac{|\Lambda_1| - C\Delta}{|\mathfrak{M}(Id)W_1|} \right)^{\frac{1}{m-1}}}.$$

Доказательство. По условию для каждого $l = 1, \dots, m$ справедливо равенство

$$\begin{aligned} \Lambda_l = \sum_{l'=1}^m \Lambda_{l'} \left(\sum_{\tau \in \mathrm{Gal}(M/\mathbb{Q})} \mathfrak{M}(\tau)\tau\left(W_l W_{l'}^*\right) \right) &= \sum_{\tau \in \mathrm{Gal}(M/\mathbb{Q})} \mathfrak{M}(\tau)\tau(W_l) \left(\sum_{l'=1}^m \Lambda_{l'} \tau(W_{l'}^*) \right) = \\ &= \mathfrak{M}(Id)W_l Z + \sum_{\substack{\tau \in \mathrm{Gal}(M/\mathbb{Q}) \\ \tau \neq Id}} \mathfrak{M}(\tau)\tau(W_l)\tau(Z). \end{aligned} \tag{19}$$

Подставим $l = 1$:

$$\Lambda_1 = \mathfrak{M}(Id)W_1Z + \sum_{\substack{\tau\in\mathrm{Gal}(M/\mathbb{Q})\\ \tau\neq Id}} \mathfrak{M}(\tau)\tau(W_1)\tau(Z). \tag{20}$$

Перенося первое слагаемое из правой части в левую и используя определение C и оценку $\tau(Z)$, находим

$$|\Lambda_1 - \mathfrak{M}(Id)W_1Z| \leqslant \frac{C\Delta}{Z^{\frac{1}{m-1}}} \leqslant C\Delta.$$

Это доказывает первое утверждение теоремы.

Пусть $|\Lambda_1| > C\Delta$. Тогда $|\mathfrak{M}(Id)W_1|Z \geqslant |\Lambda_1| - C\Delta$. Следовательно, $\mathfrak{M}(Id) \neq 0$ и

$$Z \geqslant \frac{|\Lambda_1| - C\Delta}{|\mathfrak{M}(Id)W_1|}. \tag{21}$$

Вычтем из равенства (19) равенство (20), умноженное на W_l/W_1, и воспользуемся определением C_l и оценкой $\tau(Z)$:

$$\left|\Lambda_l - \frac{W_l}{W_1}\Lambda_1\right| \leqslant C_l\frac{\Delta}{Z^{\frac{1}{m-1}}}.$$

Разделим полученное неравенство на $|\Lambda_1|$:

$$\left|\frac{\Lambda_l}{\Lambda_1} - \frac{W_l}{W_1}\right| \leqslant C_l\frac{\Delta}{|\Lambda_1|Z^{\frac{1}{m-1}}}.$$

Применение оценки (21) завершает доказательство. ■

В работе [25] используется знание структуры группы единиц $\mathcal{O}_M^*$ (которое даёт теорема Дирихле) и находится число $\sum\limits_{i=1}^{m}\Lambda_i W_i^*$ как единица специального вида. Это позволяет доказать интересные теоретические результаты, но довольно неудобно с практической точки зрения. Используем другой подход.

Будем строить совместные приближения к элементам поля $\mathcal{M} = K_G \cap \mathbb{R}$, для этого применим теорему 15 к полю $M = \mathcal{M}$. Соответственно $m = [\mathcal{M} : \mathbb{Q}] = 2^{t-1}$, $t \geqslant 2$, и $\mathrm{Gal}(\mathcal{M}/\mathbb{Q})$ состоит из автоморфизмов τ_λ при $\lambda \in \{0,1\}^{t-1}$, определённых в (15).

Наборы, связанные с полем $\mathcal{M}$, удобно нумеровать векторами из множества $\{0,1\}^{t-1}$. Поэтому дальше будем полагать, что заданы два $\mathbb{Q}$-базиса поля $\mathcal{M}$, ω_μ и ω_μ^* при $\mu \in \{0,1\}^{t-1}$, а также функция $\mathfrak{M} : \mathrm{Gal}(\mathcal{M}/\mathbb{Q}) \to \mathbb{R}$, удовлетворяющие следующим условиям:

1) $\omega^*_{0,\ldots,0} = 1$;
2) любой элемент кольца целых $\mathcal{O}_\mathcal{M}$ поля $\mathcal{M}$ разлагается по базису $\{\omega_\mu^*\}$ с целыми коэффициентами;
3) если $\lambda, \lambda' \in \{0,1\}^{t-1}$, то

$$\sum_{\mu\in\{0,1\}^{t-1}} \mathfrak{M}(\tau_\mu)\tau_\mu\left(\omega_\lambda\omega^*_{\lambda'}\right) = \begin{cases} 1, & \text{если } \lambda = \lambda', \\ 0, & \text{если } \lambda \neq \lambda'. \end{cases} \tag{22}$$

Будем называть такую пару $\mathfrak{M}$-парой. Легко видеть, что последнее условие обеспечивает выполнение условия на базисы теоремы 15, применённой к числам

$$\begin{aligned} W_{1+\mu_1+2\mu_2+2^2\mu_3+\ldots+2^{t-2}\mu_{t-1}} &= \omega_\mu, \\ W^*_{1+\mu_1+2\mu_2+2^2\mu_3+\ldots+2^{t-2}\mu_{t-1}} &= \omega^*_\mu. \end{aligned}$$

Заметим, что если $x \in \mathcal{O}_\mathcal{M}$, то $x\beta^*_{0,\ldots,0} \in \mathcal{O}_{K_G} \cap i\mathbb{R}$. Из теорем 9–12 легко видеть, что справедливы следующие следствия. Как и в самих теоремах, для $\sqrt{d}$ выбирается то из двух значений, которое соответствует произведению $\sqrt{q_1^*} \cdot \ldots \cdot \sqrt{q_t^*}$.

Следствие 1. Если

$$\begin{aligned} \omega_{\mu_1,\ldots,\mu_{t-1}} &= \frac{\beta_{\mu_1,\ldots,\mu_{t-1}}}{\beta_{0,\ldots,0}}, \\ \omega^*_{\mu_1,\ldots,\mu_{t-1}} &= \frac{\beta^*_{\mu_1,\ldots,\mu_{t-1}}}{\beta^*_{0,\ldots,0}}, \\ \mathfrak{M}(\tau_{\mu_1,\ldots,\mu_{t-1}}) &= (-1)^{\mu_1+\ldots+\mu_{t-1}} \frac{\tau_{\mu_1,\ldots,\mu_{t-1}}\left(\beta_{0,\ldots,0}\beta^*_{0,\ldots,0}\right)}{\sqrt{d}}, \end{aligned} \tag{23}$$

то условия 1–3 выполнены.

Следствие 2. Если

$$\begin{aligned} \omega_{\mu_1,\ldots,\mu_{t-1}} &= \frac{\beta^*_{\mu_1,\ldots,\mu_{t-1}}}{\beta^*_{0,\ldots,0}}, \\ \omega^*_{\mu_1,\ldots,\mu_{t-1}} &= \frac{\beta_{\mu_1,\ldots,\mu_{t-1}}}{\beta_{0,\ldots,0}}, \\ \mathfrak{M}(\tau_{\mu_1,\ldots,\mu_{t-1}}) &= (-1)^{\mu_1+\ldots+\mu_{t-1}} \frac{\tau_{\mu_1,\ldots,\mu_{t-1}}\left(\beta_{0,\ldots,0}\beta^*_{0,\ldots,0}\right)}{\sqrt{d}}, \end{aligned} \tag{24}$$

то условия 1–3 выполнены.

Помимо базисов W_i, W_i^* и функции $\mathfrak{M}$, в теореме 15 фигурируют набор целых чисел Λ_i и константа Δ. Далее опишем алгоритм построения набора A_μ, такого, что числа $\Lambda_{1+\mu_1+2\mu_2+2^2\mu_3+\ldots+2^{t-2}\mu_{t-1}} = A_{\mu_1,\ldots,\mu_{t-1}}$ удовлетворяют условию теоремы 15 с некоторым Δ.

Пусть $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq (0,\ldots,0)$. Положим $\delta_\lambda = (q_1^*)^{\lambda_1} \ldots (q_{t-1}^*)^{\lambda_{t-1}} (q_t^*)^{\lambda_{u+1} \oplus \ldots \oplus \lambda_{t-1}}$. Если δ_λ чётно, положим $g_\lambda = \sqrt{\delta_\lambda}/2$, в противном случае — $g_\lambda = (1+\sqrt{\delta_\lambda})/2$. Тогда $g_\lambda \in \mathcal{O}_\mathcal{M}$.

Будем использовать цепные дроби. Напомним, что для любого числа $X \in \mathbb{R}$ определена последовательность его полных частных $X_0, X_1, X_2, \ldots$ и неполных частных $a_0, a_1, a_2, \ldots$ следующим образом: $X_0 = X$, $a_n = \lfloor X_n \rfloor$, $X_{n+1} = 1/(X_n - a_n)$, причём последовательность конечна (т. е. X_n не определено при некотором n) тогда и только тогда, когда $X \in \mathbb{Q}$. Кроме того, определена последовательность подходящих дробей $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots$ к X вместе с формальным выражением $\frac{P_{-1}}{Q_{-1}}$ следующим образом: $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1, P_{n+1} = a_{n+1}P_n + P_{n-1}, Q_{n+1} = a_{n+1}Q_n + Q_{n-1}$. Хорошо известно (например, [26, Теорема 9 и Теорема 12]), что при $n \geqslant 0$

$$\left| X - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n Q_{n+1}}, \text{ если } X_{n+2} \text{ определено ;} \tag{25}$$

$$Q_n \geqslant 2^{\frac{n-1}{2}}. \tag{26}$$

Будем рассматривать случай квадратичных иррациональностей; воспользуемся некоторыми результатами из [27, §II.10], собранными в следующем утверждении.

Утверждение 2. Пусть a, b, c — целые числа, взаимно простые в совокупности, и $\delta = b^2 - ac > 0$ не равно полному квадрату. Корни уравнения $ax^2 + 2bx + c = 0$ будем называть иррациональностями определителя δ.

Пусть $X = (-b + \sqrt{\delta})/a$ — иррациональность определителя δ. Тогда все полные частные X тоже являются иррациональностями определителя δ и имеют вид $X_n = (x_n + \sqrt{\delta})/y_n$, где $x_n, y_n \in \mathbb{Z}$ определены единственным образом. Если $a_n = \lfloor X_n \rfloor$ — неполные частные для X и $y_{-1} = -c = (\delta - b^2)/a \in \mathbb{Z}$, то справедливы следующие формулы:

$$\begin{aligned} x_n &= y_{n-1}a_{n-1} - x_{n-1}, \quad n \geqslant 1, \\ \delta &= x_n^2 + y_n y_{n-1}, \quad n \geqslant 0, \\ y_n &= y_{n-2} - a_{n-1}(x_n - x_{n-1}), \quad n \geqslant 1. \end{aligned} \tag{27}$$

Кроме того, при $n \geqslant 0$

$$X_1 \dots X_n = \frac{(-1)^n}{P_{n-1} - Q_{n-1}X}; \quad aP_{n-1}^2 + 2bP_{n-1}Q_{n-1} + cQ_{n-1}^2 = (-1)^n y_n.$$

Назовём число $(x + \sqrt{\delta})/y$, $x, y \in \mathbb{Z}$, приведённым, если $(x + \sqrt{\delta})/y > 1$ и $-1 < (x - \sqrt{\delta})/y < 0$. Число $(x + \sqrt{\delta})/y$ приведённое тогда и только тогда, когда $0 < \sqrt{\delta} - x < y < \sqrt{\delta} + x$. Если X приведённое, то все его полные частные X_n тоже приведённые.

Введём несколько необходимых определений.

Будем параллельно строить цепные дроби для всех чисел g_λ, $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq 0$. Полные частные для g_λ будем обозначать $X_{\lambda,n}$, неполные частные — $a_{\lambda,n}$, числители и знаменатели подходящих дробей — $P_{\lambda,n}$ и $Q_{\lambda,n}$. Величины x_n, y_n из утверждения 2, построенные для $X = g_\lambda$, будем обозначать $x_{\lambda,n}$ и $y_{\lambda,n}$. Пусть σ_λ обозначает единственный нетривиальный автоморфизм поля $\mathbb{Q}(g_\lambda)$.

Если δ_λ нечётно, то по определению g_λ есть иррациональность определителя δ_λ, $x_{\lambda,0} = 1$, $y_{\lambda,0} = 2$, $y_{\lambda,-1} = (\delta_\lambda - 1)/2$. По индукции из (27) легко видеть, что $x_{\lambda,n}$ нечётно при всех n и $y_{\lambda,n}$ чётно при всех n; обозначим $x'_{\lambda,n} = (x_{\lambda,n} - 1)/2 \in \mathbb{Z}$ и $y'_{\lambda,n} = y_{\lambda,n}/2 \in \mathbb{Z}$. Квадратный трёхчлен $ax^2 + 2bx + c$, где a, b, c определены утверждением 2, имеет старший коэффициент 2 и корни g_λ, $\sigma_\lambda(g_\lambda)$. Следовательно, последнее равенство утверждения 2 можно переписать как $2(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda)\sigma_\lambda(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda) = (-1)^n y_{\lambda,n} = (-1)^n 2y'_{\lambda,n}$.

Если δ_λ чётно, то по определению g_λ есть иррациональность определителя $\delta_\lambda/4$, $x_{\lambda,0} = 0$, $y_{\lambda,0} = 1$, $y_{\lambda,-1} = \delta_\lambda/4$. Обозначим $x'_{\lambda,n} = x_{\lambda,n}$ и $y'_{\lambda,n} = y_{\lambda,n}$. Квадратный трёхчлен $ax^2 + 2bx + c$, где a, b, c определены утверждением 2, имеет старший коэффициент 1 и корни g_λ, $\sigma_\lambda(g_\lambda)$. Следовательно, последнее равенство утверждения 2 можно переписать как $(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda)\sigma_\lambda(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda) = (-1)^n y_{\lambda,n} = (-1)^n y'_{\lambda,n}$.

В обоих случаях

$$X_{\lambda,n} = \frac{g_\lambda + x'_{\lambda,n}}{y'_{\lambda,n}},$$

$$(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda)\sigma_\lambda(P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda) = (-1)^n y'_{\lambda,n}. \tag{28}$$

Утверждение 2 даёт эффективный способ последовательного построения чисел $x'_{\lambda,n}$, $y'_{\lambda,n}$, $a_{\lambda,n} = \lfloor X_{\lambda,n} \rfloor$, а по ним $P_{\lambda,n}$ и $Q_{\lambda,n}$. Для алгоритма понадобятся числа $x'_{\lambda,n}$, $y'_{\lambda,n}$ и

$$z_{\lambda,n} = (X_{\lambda,1} \dots X_{\lambda,n})^{-1} = (-1)^n (P_{\lambda,n-1} - Q_{\lambda,n-1}g_\lambda) \in \mathcal{O}_\mathcal{M}. \tag{29}$$

Отсюда и из (28) следует, что для любого $n \geqslant 0$

$$z_{\lambda,n}\sigma_\lambda(z_{\lambda,n}) = (-1)^n y'_{\lambda,n}. \tag{30}$$

Числа A_μ будем получать, пересчитывая разложение произведения целых алгебраических чисел $\prod\limits_{\lambda\neq 0}((-1)^{n_\lambda}\sigma_\lambda(z_{\lambda,n_\lambda})) = \sum\limits_\mu A_\mu\omega^*_\mu$ по базису ω^*_μ. В силу условия 2 $\mathfrak{M}$-пары и (29) числа A_μ будут целыми.

На каждом шаге алгоритм увеличивает ровно одно из чисел n_λ. На $\sum\limits_\mu A_\mu\omega^*_\mu$ этот переход действует умножением на

$$\frac{(-1)^{n+1}\sigma_\lambda\left(z_{\lambda,n+1}\right)}{(-1)^n\sigma_\lambda\left(z_{\lambda,n}\right)} = \frac{y'_{\lambda,n+1}/z_{\lambda,n+1}}{y'_{\lambda,n}/z_{\lambda,n}} = \frac{X_{\lambda,n+1}y'_{\lambda,n+1}}{y'_{\lambda,n}} = \frac{g_\lambda + x'_{\lambda,n+1}}{y'_{\lambda,n}}.$$

Таким образом, нужно переходить от набора чисел A_μ к набору чисел A'_μ, такому, что

$$\sum_\mu A'_\mu\omega^*_\mu = \left(\sum_\xi A_\xi\omega^*_\xi\right)\frac{g_\lambda + x_\lambda}{y_\lambda},$$

где $x_\lambda = x'_{\lambda,n_{\lambda+1}}$ и $y_\lambda = y'_{\lambda,n_\lambda}$. Поскольку $\{\omega^*_\mu\}$ образуют $\mathbb{Q}$-базис поля $\mathcal{M}$ и числа g_μ лежат в этом поле, то в самом начале можно предвычислить такие $c_{\mu\xi\eta} \in \mathbb{Q}$, что

$$\omega^*_\xi g_\eta = \sum_\mu c_{\mu\xi\eta}\omega^*_\mu.$$

Зная числа $c_{\mu\xi\eta}$, можем вычислить

$$\left(\sum_\xi A_\xi\omega^*_\xi\right)\frac{g_\lambda + x_\lambda}{y_\lambda} = \frac{1}{y_\lambda}\left(\sum_\xi A_\xi\sum\nolimits_\mu c_{\mu\xi\lambda}\omega^*_\mu + \sum_\xi A_\xi\omega^*_\xi x_\lambda\right) = \sum_\mu\frac{\sum_\xi A_\xi c_{\mu\xi\lambda} + A_\mu x_\lambda}{y_\lambda}\omega^*_\mu.$$

Теперь можно предъявить алгоритм.

Алгоритм построения совместных приближений. Входные данные — набор δ_λ, g_λ, $c_{\mu\xi\eta}$, введённых выше, а также порог $N_0 > 0$. Выходные данные — целые числа A_μ, такие, что $|A_{0,\ldots,0}| \geqslant N_0$ и $A_\mu/A_{0,\ldots,0}$ — приближение к $\omega_\mu/\omega_{0,\ldots,0}$ для каждого $\mu \in \{0,1\}^{t-1}$.

Алгоритм в процессе работы хранит набор из 2^{t-1} целых чисел A_μ, а также вспомогательные наборы целых неотрицательных чисел x_λ, натуральных чисел $(y_\lambda, \tilde{y}_\lambda)$ и вещественных положительных чисел $(z_\lambda, \tilde{z}_\lambda)$, где $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq (0,\ldots,0)$. Эти наборы имеют следующий смысл: если после некоторого числа итераций на шаге 3 (см. ниже) значение λ было выбрано n_λ раз, то в определённых выше обозначениях $x_\lambda = x'_{\lambda,n_\lambda}$, $(y_\lambda, \tilde{y}_\lambda) = (y'_{\lambda,n_\lambda}, y'_{\lambda,n_\lambda-1})$, $(z_\lambda, \tilde{z}_\lambda) = (z_{\lambda,n_\lambda}, z_{\lambda,n_\lambda-1})$, $\sum\limits_\mu A_\mu\omega^*_\mu = \prod\limits_{\lambda\neq 0}((-1)^{n_\lambda}\sigma_\lambda(z_{\lambda,n_\lambda}))$.

Действия алгоритма.

1) *Инициализация.* Присвоить начальные значения: $A_{0,\ldots,0} := 1$; $A_\lambda := 0$; $x_\lambda := 0$; $(y_\lambda, \tilde{y}_\lambda) := (1, \lfloor\delta_\lambda/4\rfloor)$; $(z_\lambda, \tilde{z}_\lambda) := (1, g_\lambda)$ для всех $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq (0,\ldots,0)$.
2) *Итерации.* Пока $|A_{0,\ldots,0}| < N_0$, повторять следующие шаги.
3) Выбрать некоторое λ, такое, что $z_\lambda = \max\limits_{\mu\neq(0,\ldots,0)} z_\mu$.
4) Вычислить $a = \lfloor(g_\lambda + x_\lambda)/y_\lambda\rfloor$.
5) Присвоить $(z_\lambda, \tilde{z}_\lambda) := (\tilde{z}_\lambda - az_\lambda, z_\lambda)$.

6) Запомнить $x = x_\lambda$, присвоить $x_\lambda := ay_\lambda - x_\lambda - 4\{\delta_\lambda/4\}$, после чего присвоить $(y_\lambda, \tilde{y}_\lambda) := (\tilde{y}_\lambda - a(x_\lambda - x), y_\lambda)$. (Как будет показано, новое значение x_λ всегда целое неотрицательное, а новое значение y_λ натуральное.)

7) Вычислить $A'_\mu = \left(\sum\limits_\xi A_\xi c_{\mu\xi\lambda} + A_\mu x_\lambda\right)/\tilde{y}_\lambda$ для всех μ. (Как было показано, $A'_\mu \in \mathbb{Z}$ для всех μ.) Присвоить $A_\mu := A'_\mu$.

Доказательство следующей теоремы есть в [28].

Теорема 16. Алгоритм завершается за $\mathrm{O}(\ln N_0)$ шагов. В процессе его работы всегда выполнены неравенства $0 \leqslant x_\lambda < \sqrt{\delta_\lambda} - g_\lambda$; $0 < y_\lambda < \sqrt{\delta_\lambda}$; $Z = \sum\limits_\mu A_\mu \omega^*_\mu \geqslant 1$; $\left|\tau_\lambda\left(\sum\limits_\mu A_\mu \omega^*_\mu\right)\right| \leqslant \dfrac{\sqrt{|d|}^m}{Z^{\frac{1}{m-1}}}$ при $\lambda \neq (0, \ldots, 0)$.

Доказательство. Начнём с оценок величин $x'_{\lambda,n}$, $y'_{\lambda,n}$.

Лемма 5. Пусть $\lambda \in \{0,1\}^{t-1}, \lambda \neq 0$; $n \geqslant 1$ — целое число. Тогда

$$0 \leqslant x'_{\lambda,n} < \sqrt{\delta_\lambda} - g_\lambda, \quad 0 < y'_{\lambda,n} < \sqrt{\delta_\lambda}, \quad -1 < \sigma_\lambda(X_{\lambda,n}) < 0.$$

Доказательство. Будем отдельно рассматривать случаи чётного и нечётного δ_λ.

Пусть δ_λ нечётно. По определению $X_{\lambda,1} = 1/(g_\lambda - \lfloor g_\lambda \rfloor)$. Очевидно, что $X_{\lambda,1} > 1$. Кроме того, $\sigma_\lambda(X_{\lambda,1}) = 1/(1 - g_\lambda - \lfloor g_\lambda \rfloor)$ и, поскольку $g_\lambda > 1$, получаем $-1 < \sigma_\lambda(X_{\lambda,1}) < 0$. Следовательно, в силу утверждения 2 все полные частные для g_λ, начиная с $X_{\lambda,1}$, являются приведёнными иррациональностями определителя δ_λ, т. е. $0 < \sqrt{\delta_\lambda} - x_{\lambda,n} < y_{\lambda,n} < \sqrt{\delta_\lambda} + x_{\lambda,n}$ при $n \geqslant 1$. Поскольку в этом случае $x'_{\lambda,n} = (x_{\lambda,n} - 1)/2$ и $y'_{\lambda,n} = (y_{\lambda,n})/2$, получаем заявленные оценки.

Пусть δ_λ чётно. Как и в предыдущем случае, $X_{\lambda,1} = 1/(g_\lambda - \lfloor g_\lambda \rfloor) > 1$. Кроме того, $\sigma_\lambda(X_{\lambda,1}) = -1/(g_\lambda + \lfloor g_\lambda \rfloor)$ и, поскольку $g_\lambda > 1$, получаем $-1 < \sigma_\lambda(X_{\lambda,1}) < 0$. Следовательно, в силу утверждения 2 все полные частные для g_λ, начиная с $X_{\lambda,1}$, являются приведёнными иррациональностями определителя $\delta_\lambda/4$, т. е. $0 < \sqrt{\delta_\lambda}/2 - x_{\lambda,n} < y_{\lambda,n} < \sqrt{\delta_\lambda}/2 + x_{\lambda,n}$ при $n \geqslant 1$. Поскольку в этом случае $x'_{\lambda,n} = x_{\lambda,n}$ и $y'_{\lambda,n} = y_{\lambda,n}$, получаем заявленные оценки. ■

Поскольку $X_{\lambda,n} = (g_\lambda + x'_{\lambda,n})/y'_{\lambda,n}$, немедленно получаем

Следствие. При $n \geqslant 1$ справедлива оценка

$$X_{\lambda,n} < \sqrt{\delta_\lambda}. \tag{31}$$

Напомним, что n_λ при $\lambda \neq 0$ обозначает количество выборов λ на шаге 3 алгоритма.

Неравенство $Z = \prod\limits_{\lambda \neq 0} ((-1)^{n_\lambda} \sigma_\lambda(z_{\lambda,n_\lambda})) \geqslant 1$ немедленно следует из последнего неравенства леммы 5 и определения $z_{\lambda,n_\lambda} = 1/(X_{\lambda,1} \cdot \ldots \cdot X_{\lambda,n_\lambda})$.

Лемма 6.

$$\frac{\max\limits_{\mu \neq (0,\ldots,0)} z_{\mu,n_\mu}}{\min\limits_{\mu \neq (0,\ldots,0)} z_{\mu,n_\mu}} \leqslant \sqrt{|d|}.$$

Доказательство. Перед итерациями левая часть равна 1, так что неравенство верно. Допустим, что после некоторого числа итераций неравенство верно, и предположим, что на очередной итерации алгоритм выбрал значение λ на шаге 3, т. е. $z_{\lambda,n_\lambda} = \max\limits_{\mu \neq (0,\ldots,0)} z_{\mu,n_\mu}$. Обозначим $n'_\lambda = n_\lambda + 1$ и $n'_\mu = n_\mu$ при $\mu \neq \lambda$, $\mu \neq (0, \ldots, 0)$. Очевидно, $X_{\lambda,n'_\lambda} > 1$, так что $z_{\lambda,n'_\lambda} < z_{\lambda,n_\lambda}$. Возможны два случая:

1) $z_{\lambda,n'_\lambda} \geqslant \min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu}$. В этом случае $\min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu} = \min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu}$, следовательно, $\dfrac{\max\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu}}{\min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu}} \leqslant \dfrac{\max\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu}}{\min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu}} \leqslant \sqrt{|d|}$.
2) $z_{\lambda,n'_\lambda} < \min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu}$. В этом случае $\min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu} = z_{\lambda,n'_\lambda}$; используя (31), находим $\dfrac{\max\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu}}{\min\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n'_\mu}} \leqslant \dfrac{z_{\lambda,n_\lambda}}{z_{\lambda,n'_\lambda}} = X_{\lambda,n_\lambda+1} < \sqrt{\delta_\lambda} \leqslant \sqrt{|d|}$.

Лемма доказана. ■

Напомним, что σ_λ — автоморфизм поля $\mathbb{Q}(g_\lambda) \subset \mathcal{M}$. Заметим, что при любых λ и μ отображение τ_μ можно ограничить на поле $\mathbb{Q}(g_\lambda)$. Поскольку

$$\tau_\mu\left(\sqrt{(q_1^*)^{\lambda_1}\ldots(q_{t-1}^*)^{\lambda_{t-1}}(q_t^*)^{\lambda_{u+1}\oplus\ldots\oplus\lambda_{t-1}}}\right) =$$
$$= ((-1)^{\mu_1}\sqrt{q_1^*})^{\lambda_1}\ldots((-1)^{\mu_{t-1}}\sqrt{q_{t-1}^*})^{\lambda_{t-1}}\sqrt{q_t^*}^{\lambda_{u+1}\oplus\ldots\oplus\lambda_{t-1}} =$$
$$= (-1)^{\sum\limits_{i=1}^{t-1}\lambda_i\mu_i}\sqrt{(q_1^*)^{\lambda_1}\ldots(q_{t-1}^*)^{\lambda_{t-1}}(q_t^*)^{\lambda_{u+1}\oplus\ldots\oplus\lambda_{t-1}}},$$

то $\tau_\mu|_{\mathbb{Q}(g_\lambda)}$ действует тождественно при $\sum\limits_{i=1}^{t-1}\lambda_i\mu_i \equiv 0 \pmod 2$ и совпадает с σ_λ в противном случае.

Обозначим $\max\limits_{\mu\neq(0,\ldots,0)} z_{\mu,n_\mu} = \varepsilon$. Тогда по лемме (6) для всех $\lambda \neq (0,\ldots,0)$ справедлива двусторонняя оценка $\dfrac{\varepsilon}{\sqrt{|d|}} \leqslant z_{\lambda,n_\lambda} \leqslant \varepsilon$. Из (29), (30) и леммы 5 следует, что $1 \leqslant z_{\lambda,n_\lambda}\,|\sigma_\lambda(z_{\lambda,n_\lambda})| < \sqrt{\delta_\lambda} \leqslant \sqrt{|d|}$. Следовательно, $\dfrac{1}{\varepsilon} \leqslant |\sigma_\lambda(z_{\lambda,n_\lambda})| \leqslant \dfrac{|d|}{\varepsilon}$. По построению $Z = \prod\limits_{\lambda\neq0}|\sigma_\lambda(z_{\lambda,n_\lambda})| \leqslant \left(\dfrac{|d|}{\varepsilon}\right)^{m-1}$, откуда $\varepsilon \leqslant \dfrac{|d|}{Z^{\frac{1}{m-1}}}$.

Пусть $\lambda \neq 0$. Тогда условие $\sum\limits_{i=1}^{t-1}\lambda_i\mu_i \equiv 0 \pmod 2$, рассматриваемое как уравнение на $\mu \in \{0,1\}^{t-1}$, имеет ровно $n/2$ решений, одно из которых нулевое. Получим

$$\left|\tau_\lambda\left(\sum_\mu A_\mu\omega_\mu^*\right)\right| = \prod_{\substack{2|\sum\limits_i\lambda_i\mu_i,\\ \mu\neq0}}\left|\sigma_\mu\left(z_{\mu,n_\mu}\right)\right|\cdot\prod_{2\nmid\sum\limits_i\lambda_i\mu_i}\left|z_{\mu,n_\mu}\right| \leqslant \left(\frac{|d|}{\varepsilon}\right)^{\frac{m}{2}-1}\varepsilon^{\frac{m}{2}} = |d|^{\frac{m}{2}-1}\varepsilon \leqslant \frac{\sqrt{|d|}^m}{Z^{\frac{1}{m-1}}}.$$

Остаётся доказать, что алгоритм завершает работу за $\mathrm{O}(\ln N_0)$ итераций. Доказанная часть теоремы позволяет применить теорему 15, согласно которой в процессе работы алгоритма всегда выполнено неравенство $|A_{0,\ldots,0}| \geqslant |\mathfrak{M}(Id)\omega_{0,\ldots,0}|Z - C\sqrt{|d|}^m$, где константы $\mathfrak{M}(Id)\omega_{0,\ldots,0} \neq 0$ и $C\sqrt{|d|}^m$ зависят только от базисов.

В силу (30) $Z = \prod\limits_{\lambda\neq0}\dfrac{y'_{\lambda,n_\lambda}}{z_{\lambda,n_\lambda}} \geqslant \left(\prod_{\lambda\neq0} z_{\lambda,n_\lambda}\right)^{-1}$, откуда в силу (29), (25) и (26)

$$Z \geqslant \left(\prod_{\lambda\neq0}\left|P_{\lambda,n_\lambda-1} - Q_{\lambda,n_{\lambda-1}}g_\lambda\right|\right)^{-1} \geqslant \prod_{\lambda\neq0} Q_{\lambda,n_\lambda} \geqslant \prod_{\lambda\neq0} 2^{\frac{n_\lambda-1}{2}} = 2^{\frac{\sum\limits_{\lambda\neq0} n_\lambda-(m-1)}{2}}.$$

Сумма $\sum\limits_{\lambda\neq 0} n_\lambda$ есть общее число итераций алгоритма. Таким образом, после $\mathrm{O}(\ln N_0)$ итераций алгоритма достигается неравенство $Z \geqslant \dfrac{N_0 + C\sqrt{|d|}^m}{|\mathfrak{M}(Id)\omega_{0,\dots,0}|}$, из которого следует, что $|A_{0,\dots,0}| \geqslant N_0$, что и требовалось доказать. ■

7. Вычисление элемента поля родов по приближённому значению

Восстановим числа $b_\mu \in \mathbb{Z}$ по приближённому значению числа $\sum\limits_\mu b_\mu\beta_\mu$, а также числа $b'_\mu \in \mathbb{Z}$ — по приближённому значению $\sum\limits_\mu b'_\mu\beta^*_\mu$. В п. 5 получены априорные оценки

$$\left|\tau_\lambda\left(\sum_\mu b_\mu\beta_\mu\right)\right| \leqslant T_0, \quad \left|\tau_\lambda\left(\sum_\mu b'_\mu\beta^*_\mu\right)\right| \leqslant T_0, \tag{32}$$

где T_0 — некоторое выражение, зависящее только от D. В п. 6 построен набор совместных приближений к числам $\beta_\mu/\beta_{0,\dots,0}$ и $\beta^*_\mu/\beta^*_{0,\dots,0}$ с точностью, зависящей от параметра N_0.

Построенные приближения удовлетворяют теореме 16, которую и будем использовать. (Можно доказать, что любые совместные приближения Λ_i к базису W_i, удовлетворяющие оценке вида $\left|\dfrac{\Lambda_i}{\Lambda_1} - \dfrac{W_i}{W_1}\right| \leqslant \dfrac{C'_i}{|\Lambda_1|^{1+\alpha}}$, также удовлетворяют последней оценке из теоремы 16 с показателем α вместо $1/(m-1)$ и некоторой константой в числителе.)

Продолжим использовать базисы ω_μ, ω^*_μ и функцию $\mathfrak{M}$, определённые в (23) для задачи поиска b_μ и в (24) для задачи поиска b^*_μ. Легко видеть, что при таком определении помимо свойств 1–3 $\mathfrak{M}$-пар выполнено следующее свойство:

$2'$. Если $x \in \mathcal{O}_\mathcal{M}$, то $\omega_\xi x$ разлагается по базису $\{\omega_\mu\}$ с целыми коэффициентами.

Для определённости будем работать с числами b_μ; нахождение чисел b'_μ полностью аналогично.

Пусть $X_\eta \in \mathcal{O}_\mathcal{M}$ — линейно независимый над $\mathbb{Q}$ набор из $m = 2^{t-1}$ чисел. Например, можно взять $X_\eta = \beta_\eta$; или $X_{0,\dots,0} = 1$ и $X_\eta = g_\eta$ при $\eta \neq (0,\dots,0)$, где g_η определены в предыдущем пункте. В силу условия $2'$

$$\omega_\xi X_\eta = \sum_\mu x_{\mu\xi\eta}\omega_\mu, \tag{33}$$

где $x_{\mu\xi\eta} \in \mathbb{Z}$. (Выбор $X_\eta = g_\eta$ удобен тем, что коэффициенты $x_{\mu\xi\eta}$ совпадают с рассмотренными в предыдущем пункте коэффициентами $c_{\mu\xi\eta}$ с перестановкой β_μ и β^*_μ. Выбор $X_\eta = \beta_\eta$ приводит к несколько меньшим по абсолютной величине числам.)

Зададимся точностью $\varepsilon > 0$ и вычислим $\sum\limits_\xi b_\xi\beta_\xi$ с точностью ε, т. е. найдём число γ, такое, что $\left|\sum\limits_\xi b_\xi\beta_\xi - \gamma\right| < \varepsilon$. Разделив это неравенство на $\beta_{0,\dots,0}$ и умножив на X_η, получим

$$\left|\sum_\xi b_\xi\omega_\xi X_\eta - \frac{\gamma X_\eta}{\beta_{0,\dots,0}}\right| \leqslant \frac{\varepsilon|X_\eta|}{|\beta_{0,\dots,0}|},$$

$$\left|\sum_\mu\left(\sum_\xi b_\xi x_{\mu\xi\eta}\right)\omega_\mu - \frac{\gamma X_\eta}{\beta_{0,\dots,0}}\right| \leqslant \frac{\varepsilon|X_\eta|}{|\beta_{0,\dots,0}|}. \tag{34}$$

Обозначим $B_{\mu\eta} = \sum\limits_{\xi} b_\xi x_{\mu\xi\eta} \in \mathbb{Z}$. Тогда для произвольного μ' из (22) следует, что

$$B_{\mu'\eta} = \sum_{\mu} B_{\mu\eta} \sum_{\lambda} \mathfrak{M}(\tau_\lambda)\tau_\lambda(\omega_\mu\omega^*_{\mu'}) = \sum_{\lambda} \mathfrak{M}(\tau_\lambda)\tau_\lambda(\omega^*_{\mu'})\tau_\lambda\left(\sum_{\mu} B_{\mu\eta}\omega_\mu\right),$$

$$\sum_{\mu'} A_{\mu'} B_{\mu'\eta} = \sum_{\lambda} \mathfrak{M}(\tau_\lambda)\tau_\lambda\left(\sum_{\mu'} A_{\mu'}\omega^*_{\mu'}\right)\tau_\lambda\left(\sum_{\mu} B_{\mu\eta}\omega_\mu\right). \tag{35}$$

Слагаемое с $\lambda = 0$ будем рассматривать отдельно; в этом случае (34) даёт приближённое значение последнего сомножителя и оценку погрешности приближения. При $\lambda \neq 0$ оценку второго сомножителя даёт теорема 16. Найдём оценку последнего сомножителя: $\tau_\lambda\left(\sum\limits_{\mu} B_{\mu\eta}\omega_\mu\right) = \tau_\lambda\left(\sum\limits_{\xi} b_\xi \sum\limits_{\mu} x_{\mu\xi\eta}\omega_\mu\right) = \tau_\lambda\left(\sum\limits_{\xi} b_\xi\omega_\xi\right)\tau_\lambda(X_\eta)$, откуда и из (32) следует, что $\left|\tau_\lambda\left(\sum\limits_{\mu} B_{\mu\eta}\omega_\mu\right)\right| \leqslant T_0\left|\tau_\lambda(X_\eta)\right|$. Таким образом, из (35), (34) и теоремы 16 следует, что

$$\left|\sum_{\mu'} A_{\mu'} B_{\mu'\eta} - \mathfrak{M}(Id)Z\frac{\gamma X_\eta}{\beta_{0,\ldots,0}}\right| \leqslant |\mathfrak{M}(Id)Z|\,\frac{\varepsilon|X_\eta|}{|\beta_{0,\ldots,0}|} + \sum_{\lambda\neq 0}|\mathfrak{M}(\tau_\lambda)|\frac{\sqrt{|d|}^m}{Z^{\frac{1}{m-1}}}T_0|\tau_\lambda(X_\eta)|, \tag{36}$$

где, как и раньше, $Z = \sum\limits_{\mu} A_\mu\omega^*_\mu$.

Второе слагаемое представляет из себя отношение некоторой константы и $Z^{\frac{1}{m-1}}$. Поскольку $A_{0,\ldots,0} = \Lambda_1$, неравенство (21) показывает, что можно выбрать порог N_0 в алгоритме так, чтобы было выполнено неравенство

$$Z > \left(4\sum_{\lambda\neq 0}|\mathfrak{M}(\tau_\lambda)\tau_\lambda(X_\eta)|\sqrt{|d|}^m T_0\right)^{m-1}, \tag{37}$$

а тогда второй член в правой части (36) меньше $1/4$.

Выбрав такой порог N_0 и построив совместные приближения A_μ, вычислим Z. Выберем ε так, чтобы для всех η было выполнено неравенство

$$\varepsilon < \frac{1}{4}\frac{|\beta_{0,\ldots,0}|}{|\mathfrak{M}(Id)X_\eta|Z}. \tag{38}$$

Тогда первый член в правой части (36) также будет меньше $1/4$, а следовательно, левая часть (36) меньше $1/2$. Поскольку $\sum\limits_{\mu'} A_{\mu'} B_{\mu'\eta} \in \mathbb{Z}$, то можно восстановить точное значение этой суммы, округляя $\mathfrak{M}(Id)Z\dfrac{\gamma X_\eta}{\beta_{0,\ldots,0}}$.

Возвращаясь к b_ξ, получаем на них систему линейных уравнений с левой частью

$$\sum_{\mu} A_\mu B_{\mu\eta} = \sum_{\xi}\left(\sum_{\mu} A_\mu x_{\mu\xi\eta}\right) b_\xi. \tag{39}$$

Лемма 7. Матрица $\left(\sum\limits_{\mu} A_\mu x_{\mu\xi\eta}\right)_{\xi,\eta\in\{0,1\}^{t-1}}$ невырождена.

Доказательство. Предположим, что матрица вырождена. Это эквивалентно существованию таких чисел $y_\eta \in \mathbb{Q}$, не равных одновременно нулю, что

$$\sum_\eta \sum_\mu A_\mu x_{\mu\xi\eta} y_\eta = 0. \tag{40}$$

Пусть η фиксировано. Введём квадратные матрицы с элементами $(M_1)_{\mu_1\mu_2} = \tau_{\mu_1}(\omega_{\mu_2})$, $(M_2)_{\mu_1'\mu_2'} = \tau_{\mu_1'}(\omega^*_{\mu_2'})$, $(X)_{\mu_1''\mu_2''} = x_{\mu_1''\mu_2''\eta}$ и квадратные диагональные матрицы M_3 с элементами $\mathfrak{M}(\tau_\mu)$, M_4 с элементами $\tau_\mu(X_\eta)$. Равенство (22) можно интерпретировать как матричное равенство $M_1^T M_3 M_2 = E$, где E — единичная матрица. В частности, M_1, M_2 и M_3 обратимы. Совокупность всех равенств, получающихся из (33) применением различных τ_μ, можно интерпретировать как матричное равенство $M_4 M_1 = M_1 X$. Отсюда $X = M_1^{-1} M_4 M_1$, $X^T = M_1^T M_4 (M_1^T)^{-1} = M_2^{-1} M_3^{-1} M_4 M_3 M_2$. Поскольку любые диагональные матрицы, в том числе M_3 и M_4, коммутируют, то $M_2 X^T = M_4 M_2$. Сравнивая элемент на пересечении первой строки и столбца μ, находим $\sum\limits_\xi \omega^*_\xi x_{\mu\xi\eta} = X_\eta \omega^*_\mu$.

Далее η не фиксировано. Умножим (40) на ω^*_ξ и сложим по всем $\xi \in \{0,1\}^{t-1}$:

$$\sum_\eta \sum_\mu A_\mu X_\eta \omega^*_\mu y_\eta = 0, \quad \left(\sum_\eta X_\eta y_\eta\right)\left(\sum_\mu A_\mu \omega^*_\mu\right) = 0.$$

Но первый множитель не равен нулю, поскольку X_η выбирались линейно независимыми над $\mathbb{Q}$, а $y_\eta \in \mathbb{Q}$ не все равны нулю. Второй множитель не равен нулю по теореме 16. Полученное противоречие доказывает лемму 7. ■

Таким образом, для нахождения $\{b_\mu\}$ остаётся решить заведомо невырожденную систему размером $m \times m$, например стандартным методом Гаусса.

Общая схема предлагаемой модификации метода комплексного умножения такова.

1) Выберем числа $q = p^n$, $\hat{u}, \hat{v}, D \in \mathbb{Z}$ как в шаге 1 базового алгоритма из п. 1.2. Кривая, которую мы построим, будет определена над $\mathbb{F}_q$ и будет иметь порядок $q + 1 - \hat{u}$.
2) Вычислим все примитивные формы, оценку T_0 по формуле (18), порог N_0, такой, чтобы была выполнена оценка (37), с использованием формулы (21). Применим алгоритм нахождения совместных приближений из п. 6.
3) Вычислим необходимую точность ε по формуле (38). Найдём многочлен $\hat{H}_D[j]$ по определению (16) приближённо с точностью ε.
4) Для каждого коэффициента найденного многочлена определим разложение его удвоенной вещественной части по базису β_μ, составив систему линейных уравнений с левой частью (39) с использованием (36) и решив эту систему. Аналогично определим разложение удвоенной мнимой части каждого коэффициента по базису β^*_μ. (Если известно, что коэффициент вещественный, то не нужно вычислять разложение мнимой части и не нужно умножать вещественную часть на 2.)
5) Редуцируем многочлен по модулю любого простого идеала, лежащего над p, в кольце $\mathcal{O}_{K_G}$; получим некоторый многочлен над $\mathbb{F}_q$, который разлагается на линейные множители над $\mathbb{F}_q$. Вычислим какой-нибудь из его корней и построим эллиптическую кривую E'' над $\mathbb{F}_q$ с j-инвариантом, равным вычисленному корню.
6) Если порядок кривой E'' оказался не таким, какой требуется, применим изоморфизм, описанный в п. 1.2.

Как и в исходном методе, в описанной модификации вместо модулярного инварианта j можно использовать другие функции, описанные в п. 1.3. Для этого следует скорректировать оценку T_0 на шаге 2, как описано в п. 5, на шаге 3 вычислить многочлен $\hat{H}_D[\theta, \alpha_*]$, а на шаге 5 после нахождения корня редуцированного многочлена вычислить j-инвариант как функцию от найденного корня, описанную в п. 1.3.

Автор благодарит своего научного руководителя Михаила Алексеевича Черепнёва за постановку задачи, продуктивные обсуждения и полезные замечания, позволившие уточнить и прояснить текст.

ЛИТЕРАТУРА

1. *Koblitz N.* Elliptic curve cryptosystems // Math. Comput. 1987. V. 48. P. 203–209.
2. *Miller V. S.* Uses of elliptic curves in cryptography // LNCS. 1986. V. 218. P. 417–426.
3. *Lenstra H. W.* Factoring integers with elliptic curves // Ann. Math. 1987. V. 126. P. 649–673.
4. *Atkin A. O. L. and Morain F.* Elliptic curves and primality proving // Math. Comput. 1993. V. 61. No. 203. P. 29–68.
5. *Cox D. A.* Primes of the form $x^2 + ny^2$. New York: Wiley, 1989.
6. *Weber H.* Lehrbuch der Algebra. 3rd edition. New York: Chelsea Publishing Company, 1908. V. 3.
7. *Silverman J. H.* The Arithmetic of Elliptic Curves. Springer, 1986.
8. *Ленг С.* Эллиптические функции. М.: Наука, 1984.
9. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.
10. *Cornacchia G.* Su di un metodo per la risoluzione in numeri interi dell' equazione $\sum\limits_{h=0}^{n} C_h x^{n-h} y^h = P$ // Giorn. Mat. Batt. 1908. No. 46. P. 33–90.
11. *Baier H.* Efficient algorithms for generating elliptic curves over finite fields suitable for use in cryptography. Department of Computer Science, Technical University of Darmstadt, 2002.
12. *Konstantinou E., Kontogeorgis A., Stamatiou Y. C., and Zaroliagis C. D.* On the Efficient Generation of Prime-Order Elliptic Curves // J. Cryptol. 2010. V. 23. No. 3. P. 477–503.
13. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper // Abh. Math. Sem. Hansischen Univ. 1941. B. 14. S. 197–272.
14. *Lay G.-J. and Zimmer H. G.* Constructing elliptic curves with given group order over large finite fields // LNCS. 1994. V. 877. P. 250–263.
15. *Von Schrutka L.* Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n + 1$ in ein einfaches und ein dreifaches Quadrat // J. Reine Ang. Math. 1911. B. 140. S. 252–265.
16. *Jacobstahl E.* Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate // J. Reine Ang. Math. 1907. B. 132. S. 238–245.
17. *Schertz R.* Weber's class invariants revisited // J. Théor. Nombr. Bord. 2002. V. 14. No. 1. P. 325–343.
18. *Enge A. and Schertz R.* Constructing elliptic curves over finite fields using double eta-quotients // J. Théor. Nombr. Bord. 2004. V. 16. No. 3. P. 555-568.
19. *Cohn H.* Introduction to the construction of class fields. Cambridge University Press, 1985.
20. *Ленг С.* Алгебраические числа. М.: Мир, 1966.
21. *Enge A.* The complexity of class polynomial computation via floating point approximations // Math. Comput. 2009. V. 78. No. 266. P. 1089–1107.
22. *Brisebarre N. and Philibert G.* Effective lower and upper bounds for the Fourier coefficients of powers of the modular invariant j // J. Raman. Math. Soc. 2005. V. 20. P. 255–282.

23. *Enge A. and Morain F.* Comparing invariants for class fields of imaginary quadratic fields // LNCS. 2002. V. 2369. P. 252–266.
24. *Brentjes A. J.* Multi-dimensional continued fraction algorithms. Amsterdam: Mathematisch Centrum, 1981.
25. *Peck L. G.* Simultaneous rational approximations to algebraic numbers // Bull. Amer. Math. Soc. 1961. V. 67. P. 197–201.
26. *Хинчин А. Я.* Цепные дроби. М.: Наука, 1978.
27. *Венков Б. А.* Элементарная теория чисел. ОНТИ НКТП СССР, 1937.
28. *Гречников Е. А.* Оптимизация метода с комплексным умножением построения эллиптической кривой // Деп. в ВИНИТИ 21.06.11, №305-В2011. М.: МГУ им. М. В. Ломоносова, 2011.