МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. Ломоносова

На правах рукописи

ГРЕЧНИКОВ ЕВГЕНИЙ АЛЕКСАНДРОВИЧ

ОЦЕНКИ ЧИСЛА РЕШЕНИЙ ТЕОРЕТИКО-ЧИСЛОВЫХ УРАВНЕНИЙ, ИСПОЛЬЗУЕМЫХ В КРИПТОГРАФИИ

01.01.06 – Математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2012

Работа выполнена на кафедре теории чисел Механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	кандидат физико-математических наук, доцент Черепнёв Михаил Алексеевич
Официальные оппоненты:	Цфасман Михаил Анатольевич, доктор физико-математических наук, профессор (Институт проблем передачи информации РАН, заведующий Сектором алгебры и теории чисел)
	Осипов Денис Васильевич, кандидат физико-математических наук, старший научный сотрудник (Математический институт им. В. А. Стеклова РАН, отдел алгебры и теории чисел)
Ведущая организация:	ФГУП «НИИ Автоматики»

Защита диссертации состоится 30 ноября 2012 г. в 16 ч. 45 м. на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М. В. Ломоносова по адресу: 119991, Москва, ГСП-1, Ленинские горы, д.1, МГУ, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 30 октября 2012 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор Иванов Александр Олегович

Общая характеристика работы

Актуальность темы

Одной из важных областей теории чисел является изучение конечных полей. Ещё Гаусс доказал, что в поле вычетов по любому простому модулю существует примитивный элемент g, для которого степени g^x при различных целых x пробегают все ненулевые элементы поля. Степени g^x можно легко вычислить, но для обратной задачи дискретного логарифмирования — нахождения x по значению g^x — неизвестно эффективного алгоритма решения, на чём основаны некоторые криптографические схемы. Это привлекает внимание исследователей к изучению свойств возведения в степень в конечном поле. В частности, известно[1], что задача универсальной подделки ГОСТ Р 34.10-94 может быть сведена к решению уравнения

$$g^x \equiv x \pmod{p}, \quad x \in \{0, \ldots, p-1\}, \tag{1}$$

где p — нечётное простое число. Это уравнение можно рассматривать при различных дополнительных ограничениях на g и на x. Хронологически изучение этого уравнения началось с вопроса о существовании решений при каком-либо примитивном g; этот вопрос получил название проблемы Бризолиса[2]. Если наложить дополнительное ограничение и рассматривать только примитивные корни x в качестве решений, то их количество асимптотически вычислено в 1995 году[3], а также независимо в 1999 году[4], что даёт положительный ответ на проблему Бризолиса при всех достаточно больших p. Окончательно (то есть для всех p) проблему Бризолиса решила M. Campbell[5] в 2003 году (а именно, такие решения существуют при всех $p > 3$). M. Campbell не касается вопроса явного построения решений (1); М. А. Черепнёв[6] строит конструкции при некоторых ограничениях на p, а также улучшает ранее известные оценки и доказывает существование решений при некоторых g, не являющихся первообразными корнями.

Очевидно, что число решений с примитивными g и x даёт нижнюю оценку числа решений при более слабых ограничениях. Гипотетические асимптотические равенства для чисел решений при различных наборах ограничений выдвинул J. Holden[7] в 2002 году. В частности, усреднённое по всем (в том

[1] Черепнёв М. А. Криптографические протоколы. Изд-во механико-математического факультета МГУ, 2006.

[2] Guy R. K. Unsolved Problems in Number Theory. Springer-Verlag, 1994.

[3] Zhang W. P. On a problem of Brizolis // Pure Appl. Math. 1995. Vol. 11. Pp. 1–3.

[4] Cobeli C., Zaharescu A. An exponential congruence with solutions in primitive roots // Rev. Roumaine Math. Pures Appl. 1999. Vol. 44. Pp. 15-22.

[5] Campbell M. E. On fixed points for discrete logarithms. Master's thesis, University of California at Berkeley, 2003.

[6] Черепнёв М. А. Некоторые эффективные оценки для числа решений задачи Бризолиса // Современные проблемы математики и механики, т.IV «Математика», выпуск 3. Изд-во Московского университета. 2009. С. 125–129.

[7] Holden J. Fixed points and two-cycles of the discrete logarithm // ANTS. 2002. Pp. 405–415

числе непримитивным) g число решений (1) без дополнительных ограничений на x гипотетически есть $1 + o(1)$ при $p \to \infty$. Эта гипотеза оказалась трудной и в общем случае пока не доказана; в 2006 году J. Holden и P. Moree[8] доказали гипотезу для множества p положительной плотности (среди всех простых). В 2008 году С. В. Конягин, И. Е. Шпарлинский и Ж. Бургейн[9] доказали гипотезу для множества p плотности 1. В ещё не опубликованной работе тех же авторов доказана верхняя оценка $O(1)$; работа доступна на arxiv.org как arXiv:1103.0567. Усреднённое по примитивным g число решений (1) без дополнительных ограничений на x гипотетически есть также $1 + o(1)$ при $p \to \infty$.

Другим важным объектом в теории конечных полей являются уравнения от двух переменных, задаваемые многочленами. Здесь теория чисел тесно связана с алгебраической геометрией.

Более конкретно, рассмотрим уравнение

$$y^2 \equiv f(x) \pmod{p}, \quad x, y \in \mathbb{F}_p, f \in \mathbb{F}_p[x], 2 \nmid \deg f. \tag{2}$$

Если многочлен f делится на квадрат какого-либо многочлена, то это уравнение очевидной заменой переменных сводится к уравнению того же вида с многочленом меньшей степени. Далее будем считать, что f свободен от квадратов.

Если f — многочлен третьей степени (свободный от квадратов), то множество решений уравнения (2) вместе с одним «бесконечно удалённым» образует абелеву группу. Рассмотрение всех решений над $\overline{\mathbb{F}}_p$, а не только над $\mathbb{F}_p$, приводит к эллиптической кривой. Теория эллиптических кривых исключительно обширна; её основы прекрасно изложены в книге J. Silverman[10]. В частности, неравенство Хассе устанавливает двустороннюю оценку на число решений уравнения (2) для любого возможного f степени 3 без кратных корней: это число решений (включая «бесконечно удалённое») не может отличаться от $p+1$ по модулю более чем на $2\sqrt{p}$. Теорема Дойринга–Ватерхауза[11,12] применительно к полю $\mathbb{F}_p$ утверждает, что для любого числа в пределах оценки Хассе существует уравнение вида (2) с таким числом решений.

Операция сложения в группе точек эллиптической кривой легко вычислима. Следовательно, операция умножения точки P на целое число $P \mapsto nP$, $n \in \mathbb{Z}$, также эффективно вычислима. Однако для обратной операции дискретного логарифмирования на эллиптической кривой — вычисления n по

[8] Holden J., Moree P. Some heuristics and results for small cycles of the discrete logarithm // Mathematics of computation. 2006. Vol. 75. Pp. 419–449.

[9] Bourgain J., Konyagin S. V., Shparlinski I. E. Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm // Int. Math. Res. Notices. 2008. No. rnn090

[10] Silverman J. H. The Arithmetic of Elliptic Curves. Springer, 1986.

[11] Deuring M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper // Abh. Math. Sem. Hansischen Univ. 1941. Vol. 14. Pp. 197–272.

[12] Waterhouse W. C. Abelian varieties over finite fields // Ann. Sci. École Norm. Sup. 1969. Vol. 2, no. 4. Pp. 521–560.

известным точкам P и nP — в общем случае неизвестно эффективного алгоритма, на чём основаны некоторые криптографические схемы[13,14]. Для этих схем важно, чтобы порядок группы точек был простым числом или, по крайней мере, имел большой простой делитель. Кроме того, в некоторых специальных случаях дискретное логарифмирование всё же возможно[15,16]; их легко запретить дополнительными условиями на порядок группы точек.

Теорема Дойринга–Ватерхауза гарантирует существование эллиптической кривой с нужным порядком, но не содержит способа построения такой кривой. Один из возможных методов построения — случайно выбирать коэффициенты уравнения кривой и подсчитывать число точек с помощью алгоритма Шуфа в цикле, пока вычисленное число точек не удовлетворяет заданным условиям. Следует отметить, что вероятность случайно получить кривую с порядком, делящимся на большое простое число, не слишком велика. Кроме того, сложность алгоритма Шуфа хотя и полиномиальна (по размеру входных данных), но растёт достаточно быстро.

Другой, более эффективный способ построения эллиптических кривых — метод комплексного умножения. Для простых полей первый её вариант описали A. Atkin и F. Morain[17] в 1993 году (в качестве вспомогательного средства для алгоритма проверки простоты), для произвольных конечных полей, включая поля характеристики 2, — G.-J. Lay и H. Zimmer[18] в 1994 году. В дальнейшем этот метод неоднократно улучшали[19,20,21,22].

Если в уравнении (2) f — многочлен нечётной степени $n > 3$ (свободный от квадратов), то множество решений этого уравнения над $\overline{\mathbb{F}}_p$ вместе с одним «бесконечно удалённым» есть гиперэллиптическая кривая рода $\frac{n-1}{2}$. Представим число $\mathbb{F}_p$-точек кривой в виде $p + 1 + N$, или, что эквивалентно, число решений уравнения (2) в виде $p + N$. Оценка Вейля, доказанная средствами

---

[13] Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. 1987. Vol. 48. Pp. 203–209.

[14] Miller V. S. Uses of elliptic curves in cryptography // Advances in Cryptology—CRYPTO '85. Vol. 218 of Lecture Notes in Computer Science. Springer-Verlag, 1986. Pp. 417-426.

[15] Semaev I. A. Evaluation of discrete logarithm in a group of p-torsion points of an elliptic curve in characteristics p // Mathematics of Computation. 1998. Vol. 67. Pp. 353–356.

[16] Menezes A. J., Okamoto T., Vanstone S. A. Reducing elliptic curve logarithms to a finite field // IEEE Trans. Info. Theory. 1993. Vol. 39. Pp. 1639–1646.

[17] Atkin A. O. L., Morain F. Elliptic curves and primality proving // Mathematics of Computation. 1993. Vol. 61, no. 203. Pp. 29–68.

[18] Lay G.-J., Zimmer H. G. Constructing elliptic curves with given group order over large finite fields // ANTS / Ed. by L. M. Adleman, M.-D. A. Huang. Vol. 877 of Lecture Notes in Computer Science. Springer, 1994. Pp. 250–263.

[19] Enge. A., Morain F. Comparing invariants for class fields of imaginary quadratic fields // Algorithmic Number Theory — ANTS-V (Berlin). Vol. 2369 of Lecture Notes in Computer Science. Springer-Verlag, 2002. Pp. 252–266.

[20] Baier. H. Efficient algorithms for generating elliptic curves over finite fields suitable for use in cryptography. Master's thesis, Department of Computer Science, Technical University of Darmstadt, 2002.

[21] Enge A., Schertz R. Constructing elliptic curves over finite fields using double eta-quotients // Journal de Théorie des Nombres de Bordeaux. 2004. Vol. 16, no. 3. Pp. 555–568.

[22] Konstantinou E., Kontogeorgis A., Stamatiou Y. C., Zaroliagis C. D. On the Efficient Generation of Prime-Order Elliptic Curves // J. Cryptology. 2010. Vol. 23, no. 3. Pp. 477–503.

алгебраической геометрии, утверждает, что $|N| \leqslant (n-1)\sqrt{p}$. В 1969 году С. А. Степанов[23] доказал элементарными методами оценку $|N| \leqslant \sqrt{3n}n\sqrt{p}$ при $p > 9n^2$. Доказательство основывается на построении ненулевого многочлена не слишком большой степени такого, что все числа $x : \left(\frac{f(x)}{p}\right) = 1$ являются его корнями достаточно высокой кратности, откуда следует оценка на их количество. Степанов строил такой многочлен как линейную комбинацию с неопределёнными коэффициентами. Позднее, в 1971 году Н. М. Коробов[24] построил аналогичный многочлен явным образом, что позволило получить элементарным методом оценку $|N| \leqslant (n-1)\sqrt{p - \frac{(n-3)(n-4)}{4}}$. В 2005 году Д. А. Митькин[25] выдвинул утверждение $|N| \leqslant (n-1)\sqrt{p - \frac{(n-3)(n+1)}{4}}$, но его доказательство неполное, так как использует лемму из статьи Коробова для значений параметров, не подходящих под ограничения из статьи Коробова.

Цель работы

Цель диссертации — получение новых оценок на количество решений уравнений

$$g^x \equiv x \pmod{p}, \quad x \in \{0, \ldots, p-1\}, \tag{3}$$

$$y^2 \equiv f(x) \pmod{p}, \quad x, y \in \mathbb{F}_p, f \in \mathbb{F}_p[x], 2 \nmid \deg f, \tag{4}$$

где p — простое нечётное, а также оптимизация построения эллиптических кривых, для которых соответствующее уравнение вида (4) имеет число решений с предписанными свойствами.

Научная новизна

Результаты диссертации являются новыми и состоят в следующем:

- Получены двусторонние оценки на число решений уравнения (3) в парах (g, x), где g — первообразный корень по модулю p. В частности, доказано, что в случае, когда имеется растущая последовательность простых p, для которых $p-1$ не имеет простых делителей в отрезке $[\frac{\ln p - \ln 2}{\ln \ln p}, p^{1/s}]$ для фиксированного натурального s, то среднее число решений по всем первообразным g есть $1 + o(1)$.

- Доказано, что число решений уравнения (4) в парах (x, y) при $\deg f = 2g+1$ отличается от p по модулю менее чем на $2g\sqrt{p+1-g^2}$.

[23] Степанов С. А. О числе точек гиперэллиптической кривой над простым конечным полем // Известия АН СССР. Серия математическая. 1969. Т. 33, № 5. С. 1171–1181.

[24] Коробов Н. М. Оценка сумм символов Лежандра // Доклады АН СССР. 1971. Т. 196, № 4. С. 764–767.

[25] Митькин Д. А. Уточнение оценки для суммы символов Лежандра от многочленов нечётной степени // Чебышевский сборник. 2005. Т. 6, № 3. С. 123–126.

- Получена оценка снизу на максимальное число решений уравнения (4) при $\deg f = 5$. В частности, показано, что для любого p эта оценка отличается от полученной верхней оценки не более чем на 3. Доказательство содержит конструктивное построение гиперэллиптических кривых рода 2 большого порядка (соответствующих уравнению вида (4) с $\deg f = 5$) из эллиптических кривых.

- Предложена новая модификация метода построения эллиптических кривых, использующего комплексное умножение. Показано, что можно эффективно использовать делитель многочлена Гильберта с коэффициентами, являющимися целыми в поле родов мнимоквадратичного поля.

- Вычислен базис кольца целых поля родов мнимоквадратичного поля. Предложен алгоритм построения совместных рациональных приближений к элементам построенного базиса. Доказаны оценки на скорость сходимости типа Дирихле.

- Предложен алгоритм восстановления точных значений коэффициентов разложения целого алгебраического числа из поля родов мнимоквадратичного поля по приближённому значению числа и оценке модуля всех сопряжённых к нему.

- Написана программа, которая строит эллиптические кривые с числом точек, равным простому числу вида Софи Жермен.

Основные методы исследования

В диссертации используются методы из алгебраической и алгоритмической теории чисел.

Теоретическая и практическая ценность

В диссертации доказываются теоремы и выводятся формулы, которые могут найти применение в алгебраической теории чисел. Построенные алгоритмы с оценками сложности могут использоваться в вычислительной теории чисел. Программа для построения эллиптических кривых на основе результатов главы 5 диссертации внедрена в НИИ «Автоматики».

Апробация работы

Результаты диссертации докладывались автором на следующих научных семинарах и конференциях:

- на научно-исследовательском семинаре кафедры теории чисел (МГУ, Москва, 2011 г.);

- на семинаре «Теоретико-числовые вопросы криптографии» (МГУ, Москва, неоднократно 2008–2010 гг.);
- на конференции «Ломоносовские чтения» (МГУ, Москва, 2009 г.);
- на X международной конференции «Интеллектуальные системы и компьютерные науки» (МГУ, Москва, 2011 г.).

Публикации

Результаты автора по теме диссертации опубликованы в 5 работах [1], [2], [3], [4], [5].

Структура и объём диссертации

Диссертация состоит из введения, четырёх глав и библиографии (54 наименований). Общий объём диссертации составляет 113 страниц.

Содержание работы

Во введении, являющемся первой главой, описывается структура диссертации; обосновывается актуальность темы и научная новизна полученных результатов; излагаются основные результаты диссертации.

Далее записи $f = O_a(g)$ и $f \ll_a g$, где f, g — некоторые выражения, a — параметр (один или несколько), будут означать существование некоторой константы $C = C(a)$, зависящей от параметра a, такой, что $|f| \leqslant Cg$.

Во второй главе доказываются двусторонние оценки для числа решений $N(p)$ уравнения (1) без ограничений по x в среднем по примитивным g:

$$N(p) = \frac{1}{\varphi(p-1)} \sum_g \big|\{0 \leqslant x \leqslant p-1 : g^x \equiv x \pmod p\}\big|.$$

При $a \geqslant 1$ через $F(a)$ обозначим единственный корень уравнения $x^x = a$, не меньший 1. При $\ln a > 1$ выполнено неравенство $F(a) \geqslant \frac{\ln a}{\ln\ln a}$, асимптотически при $a \to \infty$ справедлива эквивалентность $F(a) \sim \frac{\ln a}{\ln\ln a}$.

Теорема 2.1. *Среднее число решений $N(p)$ представляется в виде $N(p) = 1 + S(p)$, где для функции $S(p)$ при произвольном $\varepsilon > 0$ справедливы оценки:*

- $S(p) \geqslant -C(\varepsilon)p^{-\frac{1}{4}+\varepsilon}$, *где константа $C(\varepsilon) > 0$ зависит только от ε;*
- $S(p) \leqslant \exp\left\{C' \operatorname{Li}\left((\ln p)^{c\frac{\ln\ln\ln p}{\ln\ln\ln p}}\right)\right\}$ *при достаточно больших p.*

Пусть $s \in \mathbb{N}, s \geqslant 7$. *Если число* $p-1$ *не имеет делителей из отрезка* $[F(p/2), p^{\frac{1}{s}}]$, *то*

$$S(p) = O_{s,\varepsilon}\left(p^{-\frac{1}{s}+\frac{1}{s(s-1)}+\varepsilon}\right).$$

Для доказательства теоремы величина $S(p)$ представляется в виде некоторой суммы по делителям $p-1$. А именно, вводятся функции

$$N_1(p,d) = \left|\{1 \leqslant y \leqslant p-1 : (\operatorname{ind}_{g_0} y, p-1) = \frac{p-1}{d}, (y, p-1) = \frac{p-1}{d}\}\right|,$$

$$S_1(p,d) = N_1(p,d) - \frac{\varphi^2(d)}{p}.$$

Связь между $S(p)$ и введёнными функциями описывает следующее утверждение.

Утверждение 2.1. *Функцию* $S(p)$ *можно представить в виде*

$$S(p) = \sum_{d|p-1} \frac{S_1(p,d)}{\varphi(d)} - \frac{1}{p}.$$

На различных диапазонах для d для оценки $S_1(p,d)$ приходится использовать существенно различные методы. Есть тривиальная нижняя оценка $N_1(p,d) \geqslant 0$. Известна[1] оценка

$$|S_1(p,d)| \ll_\varepsilon p^{\frac{1}{2}+\varepsilon},$$

нетривиальная при очень больших d. Оценки для меньших d дают следующие утверждения.

Утверждение 2.2. *При* $d < p^{2/3}$ *и произвольном* $\varepsilon > 0$ *справедлива оценка*

$$N_1(p,d) \ll_\varepsilon d^{3/4} p^\varepsilon.$$

Утверждение 2.3. *Существуют такие абсолютные константы* $c_i > 0$, *что при* $d > c_1$, $p > c_2$ *справедливы следующие оценки.*

При $d \geqslant p^{\frac{\ln\ln\ln p}{\ln\ln p}}$

$$N_1(p,d) \leqslant d^{c_3 \frac{\ln d}{\ln p}},$$

а при $d \leqslant p^{\frac{\ln\ln\ln p}{\ln\ln p}}$

$$N_1(p,d) \leqslant d^{c_4 \frac{\ln\ln\ln d}{\ln\ln d}}.$$

Кроме того, для любого $\varepsilon > 0$ *и натурального* s *при* $d \leqslant p^{\frac{1}{s}}$ *выполнена оценка*

$$N_1(p,d) \ll_{\varepsilon,s} d^{\frac{1}{s}+\varepsilon}.$$

Если $2d^d < p$, *то*

$$N_1(p,d) = 0.$$

[1] Campbell M. E. On fixed points for discrete logarithms. C. 1

Для доказательства последнего утверждения используется следующая лемма, представляющая самостоятельный интерес. Она обобщает хорошо известную[2] верхнюю оценку для количества делителей натурального числа: $\tau(n) < \exp\left\{(1+\varepsilon)\frac{\ln n}{\ln\ln n}\ln 2\right\}$ при любом $\varepsilon > 0$ и всех достаточно больших n.

Лемма 2.2. *Обозначим через $\tau_k(n)$ количество представлений натурального числа n в виде произведения k натуральных сомножителей. Для любого $\varepsilon > 0$ при всех $x \geqslant x_0(\varepsilon)$ и $2 \leqslant k \leqslant \ln\ln x$ справедлива оценка*

$$\max_{n\leqslant x} \tau_k(n) \leqslant \exp\left\{(1+\varepsilon)\frac{\ln x}{\ln\ln x}\ln k\right\}.$$

Результаты второй главы опубликованы в работе [1].

В третьей главе приведено полное доказательство результата, анонсированного Д. А. Митькиным[1]. А именно, пусть

$$S(f) = \sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right).$$

Тогда число решений уравнения (2) есть $p + S(f)$ и справедлива следующая теорема.

Теорема 3.1. *При нечётном $n \geqslant 3$, простом $p \geqslant \frac{n^2-1}{2}$ и многочлене $f \in \mathbb{F}_p[x]$ степени n выполнено неравенство*

$$|S(f)| < (n-1)\sqrt{p - \frac{(n-3)(n+1)}{4}} = (n-1)\sqrt{p+1-\left(\frac{n-1}{2}\right)^2}.$$

Применительно к $n = 5$ и $p > 19$ теорема означает следующее.

Следствие. При простом $p > 19$ и многочлене $f \in \mathbb{F}_p[x]$ степени 5 выполнено неравенство

$$|S(f)| \leqslant 4[\sqrt{p}] + \delta_{up}(p), \text{ где } \delta_{up}(p) = \begin{cases} -1, & p \in \{k^2+1, k^2+2, k^2+3\}, k \in \mathbb{N} \\ 0, & p = k^2 + l, 3 < l \leqslant \frac{k}{2}, k \in \mathbb{N} \\ 1, & p = k^2 + l, \frac{k}{2} < l \leqslant k, k \in \mathbb{N} \\ 2, & p = k^2 + l, k < l \leqslant \frac{3k}{2}, k \in \mathbb{N} \\ 3, & p = k^2 + l, \frac{3k}{2} < l \leqslant 2k, k \in \mathbb{N} \end{cases}$$

Результаты третьей главы опубликованы в работе [3].

В четвёртой главе исследуется вопрос о точности оценки из третьей главы в случае $\deg f = 5$. Для этого явным образом строятся многочлены f степени 5 с большим числом решений уравнения (2), близким к верхней границе, доказанной в третьей главе. А именно, доказывается следующая теорема.

---

[2] Hardy G. H., Wright E. M. An introduction to the theory of numbers. Oxford University Press, 1979.

[1] Митькин Д. А. Уточнение оценки для суммы... С. 4

Теорема 4.1. *Имеет место оценка*

$$\max_{f:\deg f=5} |S(f)| \geqslant 4[\sqrt{p}] + \delta_{down}(p),$$

где

$$\delta_{down}(p) = \begin{cases} -4, & p = k^2+1, k \in \mathbb{N}; \\ -2, & p \in \{k^2+2, k^2+3\}, k \in \mathbb{N}; \\ 0, & \textit{иначе.} \end{cases}$$

Конструкция f основывается на следующей лемме.

Лемма 4.1. *Пусть a_1, a_2, b — целые числа, $a_1 \not\equiv a_2 \pmod p$,*

$$\sum_{x=0}^{p-1} \left(\frac{x-a_1}{p}\right)\left(\frac{x^2-b}{p}\right) = S_1, \qquad \sum_{x=0}^{p-1} \left(\frac{x-a_2}{p}\right)\left(\frac{x^2-b}{p}\right) = S_2.$$

Тогда

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{\left(x^2+2(a_1+a_2)x+(a_1-a_2)^2\right)^2-16bx^2}{p}\right) = S_1+S_2.$$

Результаты четвёртой главы опубликованы в работе [4].

В пятой главе рассматривается построение эллиптических кривых над конечным полем с предписанным порядком. В отличие от предыдущих глав, здесь рассматривается произвольное конечное поле $\mathbb{F}_q$, не обязательно простое поле $\mathbb{F}_p$; это связано с тем, что на практике иногда используются эллиптические кривые над полем $\mathbb{F}_{2^n}$, поскольку при программной реализации некоторые операции в таком поле более эффективны.

Параграф 5.1, с которого начинается глава, содержит постановку задачи и общий обзор структуры пятой главы.

Параграфы 5.2 и 5.3 содержат краткий обзор используемой теории, а также подробное описание метода комплексного умножения. Для формулировки дальнейших утверждений отметим только, что в методе комплексного умножения вычисляется многочлен

$$H_D[\theta](x) = \prod_{(A,B,C)} (x - \theta(A,B,C)) \in \mathbb{Z}[x], \tag{5.1}$$

где произведение берётся по некоторому конечному эффективно вычислимому множеству троек, зависящему от параметра $D < 0$, $D \equiv 0,1 \pmod 4$ и от вида функции θ, причём сначала $H_D[\theta]$ вычисляется приближённо с достаточно высокой точностью, потом точное значение восстанавливается округлением в силу того, что все коэффициенты целые. В базовом варианте метода

$$\theta(A,B,C) = j\left(\frac{-B+\sqrt{D}}{2A}\right),$$

в различных модификациях функция θ может быть другой (возможные варианты описаны в параграфе 5.3), но всегда значение j можно восстановить по известному значению θ и многочлен $H_D[\theta]$ имеет целые коэффициенты.

Буквой D в этой главе всегда обозначается целое число, сравнимое с 0 или 1 по модулю 4. Для любого такого D существует единственное представление в виде $D = df^2$, где f — натуральное, а d удовлетворяет одному из двух условий:

- либо
$$d \equiv 1 \pmod 4 \text{ и } d \text{ свободно от квадратов,} \tag{5.2}$$
- либо
$$d \equiv 0 \pmod 4, \qquad \frac{d}{4} \text{ свободно от квадратов,} \qquad \frac{d}{4} \not\equiv 1 \pmod 4. \tag{5.3}$$

Лемма 5.2. *Пусть $d < 0$ удовлетворяет одному из условий (5.2) и (5.3). Тогда d может быть единственным с точностью до порядка множителей способом представлен в виде произведения*

$$d = q_1^* \dots q_t^*,$$

где все q_i^* попарно взаимно просты, для каждого i либо

$$q_i^* = (-1)^{\frac{q_i - 1}{2}} q_i,$$

для некоторого нечётного простого $q_i > 0$, либо $q_i^* \in \{-4, \pm 8\}$.

В параграфе 5.4 рассматривается структура кольца целых $\mathcal{O}_{K_G}$ поля родов $K_G = K(\sqrt{q_1^*}, \dots, \sqrt{q_t^*})$ для поля $K = \mathbb{Q}(\sqrt{d})$. Сначала найден фундаментальный базис K_G. Затем найдены базисы вещественной и мнимой частей K_G, то есть $K_G \cap \mathbb{R}$ и $K_G \cap i\mathbb{R}$, которые и будут использованы в дальнейшем. В зависимости от значений q_i^* эти базисы задаются следующими теоремами, в которых используются следующие обозначения.

Если q_i^* — нечётное число, то положим $\alpha_i = \frac{1+\sqrt{q_i^*}}{2}$ и $\tilde{\alpha}_i = \frac{1-\sqrt{q_i^*}}{2}$.

Группа Галуа $\mathrm{Gal}(K_G/\mathbb{Q})$ содержит t элементов τ_j, действующих следующим образом:

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

Вся группа Галуа исчерпывается автоморфизмами вида

$$\tau'_\mu = \tau_1^{\mu_1} \dots \tau_t^{\mu_t} \in \mathrm{Gal}(K_G/\mathbb{Q})$$

при $\mu \in \{0,1\}^t$.

Среди q_i^* есть отрицательные числа. Обозначив через u число положительных среди q_i^*, $0 \leqslant u < t$, можно без ограничения общности считать, что $q_1^* > 0, \ldots, q_u^* > 0, q_{u+1}^* < 0, \ldots, q_t^* < 0$. Группа Галуа $\mathrm{Gal}((K_G \cap \mathbb{R})/\mathbb{Q})$ состоит из автоморфизмов

$$\tau_\lambda = \tau_{\lambda_1,\ldots,\lambda_{t-1}} = \tau'_{\lambda_1,\ldots,\lambda_{t-1},0} = \tau_1^{\lambda_1} \ldots \tau_{t-1}^{\lambda_{t-1}} \tag{5.4}$$

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

Теорема 5.9. *Пусть $q_1^*, \ldots, q_t^*$ такие же, как в лемме 5.2, 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, $K_G = \mathbb{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$, τ_λ заданы формулой (5.4). Тогда:*

1. *Числа*

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

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

2. *Числа*

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

   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*

$$\sum_{\mu \in \{0,1\}^{t-1}} (-1)^{\mu_1+\ldots+\mu_{t-1}} \tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}} \beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) = \\ = \begin{cases} (-1)^{\nu_1+\ldots+\nu_{t-1}} \sqrt{q_1^*} \ldots \sqrt{q_t^*}, & \text{если } \eta = \nu, \\ 0, & \text{иначе.} \end{cases}$$

Теорема 5.10. *Пусть $t \geqslant 2$, $q_2^*, \ldots, q_t^*$ такие же, как в теореме 5.9, 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 (5.4). 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*

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

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* $\eta, \nu \in \{0,1\}^{t-1}$ *справедливо равенство*

$$\sum_{\mu\in\{0,1\}^{t-1}} (-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right) =$$
$$= \begin{cases} (-1)^{\nu_1+\ldots+\nu_{t-1}}\sqrt{q_1^*}\ldots\sqrt{q_t^*}, & \text{если } \eta = \nu, \\ 0, & \text{иначе.} \end{cases}$$

Теорема 5.11. *Пусть* $t \geqslant 2$, $q_1^*,\ldots,q_{t-1}^*$ *такие же, как в теореме 5.9, 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 (5.4). 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*

$$\sum_{\mu\in\{0,1\}^{t-1}}(-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right)=$$
$$=\begin{cases}(-1)^{\nu_1+\ldots+\nu_{t-1}}\sqrt{q_1^*}\ldots\sqrt{q_t^*}, & \text{если } \eta=\nu,\\ 0, & \text{иначе.}\end{cases}$$

Теорема 5.12. *Пусть* $q_1^*,\ldots,q_{t-1}^*$ *нечётные положительные,* $q_t^*=-4$ *или* $q_t^*=-8$*. Тогда:*

1. *Числа*

$$\beta_{s_1,\ldots,s_{t-1}} = \beta_{s_1,\ldots,s_{t-1}}(q_1^*,\ldots,q_t^*) = \prod_{i=1}^{t-1}\tilde{\alpha}_i^{s_i}\alpha_i^{1-s_i},$$

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

2. *Числа*

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

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*

$$\sum_{\mu\in\{0,1\}^{t-1}}(-1)^{\mu_1+\ldots+\mu_{t-1}}\tau_\mu\left(\beta_{\eta_1,\ldots,\eta_{t-1}}\beta^*_{\nu_1,\ldots,\nu_{t-1}}\right)=$$
$$=\begin{cases}(-1)^{\nu_1+\ldots+\nu_{t-1}}\sqrt{q_1^*}\ldots\sqrt{q_t^*}, & \text{если } \eta=\nu,\\ 0, & \text{иначе.}\end{cases}$$

В параграфе 5.5 предлагается новая модификация метода комплексного умножения, заключающаяся в использовании вместо многочлена $H_D[\theta]$ его делителя $\hat{H}_D[\theta]$. Напомним, что при определении (5.1) многочлена $H_D[\theta]$ по D определённым образом строится набор троек (A, B, C); их всегда можно выбирать так, чтобы $\gcd(A, D) = 1$. Определим на них отображение φ в $\{\pm 1\}^t$ формулой

$$\varphi(A, B, C) = \left(\left(\frac{q_1^*}{A}\right), \ldots, \left(\frac{q_t^*}{A}\right) \right),$$

где q_i^*, как и ранее, взяты из леммы 5.2, а $\left(\frac{a}{b}\right)$ — символ Кронекера, мультипликативный по b, равный символу Лежандра при нечётных простых b, для $b = 2$ определённый только в случае $a \equiv 0, 1 \pmod 4$ формулой

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

Теорема 5.13. *Образ отображения φ совпадает с группой $\{(\varepsilon_1, \ldots, \varepsilon_t) : \prod_{i=1}^t \varepsilon_i = 1\}$ с покомпонентным умножением. На наборе троек (A, B, C) из определения* (5.1) *можно ввести групповую структуру, относительно которой φ является гомоморфизмом групп.*

Определим многочлен $\hat{H}_D[\theta]$ следующим образом:

$$\hat{H}_D[\theta](x) = \prod_{(A,B,C):\varphi(A,B,C)=(1,\ldots,1)} (x - \theta(A, B, C)).$$

Аналогично многочлену $H_D[\theta]$, многочлен $\hat{H}_D[\theta]$ легко вычислить по определению с любой наперёд заданной точностью. В отличие от многочлена $H_D[\theta]$, многочлен $\hat{H}_D[\theta]$ имеет коэффициенты из $\mathcal{O}_{K_G}$, поэтому для его использования в методе комплексного умножения нужно уметь восстанавливать числа из $\mathcal{O}_{K_G}$ по достаточно точным приближениям.

В параграфе 5.6 вычислена оценка T_0 на все сопряжённые к коэффициентам многочлена $\hat{H}_D[\theta]$. Автоморфизмы из группы Галуа $\mathrm{Gal}(K_G/\mathbb{Q})$ переводят многочлен $\hat{H}_D[\theta]$ в многочлены вида

$$\hat{H}_{D,\varphi_0}[\theta](x) = \prod_{(A,B,C):\varphi(A,B,C)=\varphi_0} (x - \theta(A, B, C)).$$

Теорема 5.14. *Каждый коэффициент многочлена* $\hat{H}_{D,\varphi_0}[j]$ *по модулю не превосходит*

$$\exp\left\{c_5 h + c_1 N\left(\ln^2 N + 4\gamma \ln N + c_6 + \frac{\ln N + \gamma + 1}{N}\right)\right\}$$

$$\leqslant \exp\left\{c_1 N \ln^2 N + c_2 N \ln N + c_3 N + c_1 \ln N + c_4\right\},$$

где $N = \sqrt{\frac{|D|}{3}}$, $\gamma = 0.577...$ — *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*

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

также выполняется для других функций θ, *подходящих для использования в методе комплексного умножения.*

В качестве T_0 можно взять оценку из теоремы 5.14, но на практике предлагается использовать эвристическую, но более точную оценку

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

при использовании инварианта j. При использовании других функций θ следует умножить оценку на $\frac{\deg_j \Phi}{\deg_\theta \Phi}$, где Φ — многочлен от двух переменных, связывающий j и θ, $\Phi(j(z), \theta(z)) = 0$ (такой многочлен существует для всех θ, подходящих для использования в методе комплексного умножения).

Ещё одним необходимым этапом является построение совместных приближений к элементам базиса K_G. Для построения совместных приближений существуют различные универсальные алгоритмы, изучению которых посвящена книга A. Brentjes[1]. На практике характеристики получаемых приближений существенно различаются для разных алгоритмов, для практических целей, по-видимому, наилучшим является алгоритм скалярных произведений из главы 6A указанной книги. К сожалению, для универсальных алгоритмов довольно трудно получить теоретические оценки качества. Поэтому в параграфе 5.7 мы предлагаем алгоритм, подходящий только для наборов чисел нужного нам вида, работающий на практике примерно столь же хорошо, сколь и алгоритм скалярных произведений. В том же параграфе мы доказываем для нашего алгоритма оценку качества получаемых приближений, по порядку совпадающего с оценкой теоремы Дирихле.

[1] Brentjes A. J. Multi-dimensional continued fraction algorithms. Amsterdam: Mathematisch Centrum, 1981.

Доказательство оценки качества основано на следующей теореме. Основную её часть по существу описал L. Peck[2], хотя в нашем случае утверждения из этой работы неприменимы. Основные отличия нашей теоремы от работы L. Peck заключаются в явной формулировке (в том числе явных константах), введении функции $\mathfrak{M}$ (L. Peck оперирует двойственными базисами, что эквивалентно $\mathfrak{M} = 1$) и специализацией для интересующего нас случая (L. Peck не требует нормальности расширения $M/\mathbb{Q}$ и описывает также обратную теорему).

Теорема 5.15. *Пусть $M \subset \mathbb{R}$ — поле такое, что $M/\mathbb{Q}$ — расширение Галуа степени m. Пусть $W_1, \ldots, W_m$ и $W_1^*, \ldots, W_m^*$ — 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 $i = 2, \ldots, m$

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

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

$$\sum_{i=1}^{m} \Lambda_i W_i^* = Z \geqslant 1,$$

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

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 $i = 2, \ldots, m$ справедлива оценка*

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

[2] Peck L. G. Simultaneous rational approximations to algebraic numbers // Bull. Amer. Math. Soc. 1961. Vol. 67. Pp. 197–201.

Теорема применяется в случае $M = K_G \cap \mathbb{R}$, $m = [M : \mathbb{Q}] = 2^{t-1}$, к двум наборам элементов ω_μ и ω^*_μ, нумеруемым векторами из $\{0,1\}^{t-1}$, образующим базис M над $\mathbb{Q}$ и удовлетворяющим следующим условиям:

1. $\omega^*_{0,\dots,0} = 1$.
2. Любой элемент кольца целых $\mathcal{O}_M$ поля M разлагается по базису $\{\omega^*_\mu\}$ с целыми коэффициентами.
3. Если $\lambda, \lambda' \in \{0,1\}^{t-1}$, то

$$\sum_{\mu\in\{0,1\}^{t-1}} \mathfrak{M}(\tau_\mu)\tau_\mu\left(\omega_\lambda\omega^*_{\lambda'}\right) = \begin{cases} 1, & \text{если } \lambda = \lambda', \\ 0, & \text{если } \lambda \neq \lambda'. \end{cases} \tag{5.5}$$

Из теорем параграфа 5.4 следует, что базисы β_μ и β^*_μ после деления на первый элемент базиса удовлетворяют этим условиям. Более точно, выполнены следующие утверждения.

Утверждение. *Если*

$$\begin{aligned} \omega_{\mu_1,\dots,\mu_{t-1}} &= \tfrac{\beta_{\mu_1,\dots,\mu_{t-1}}}{\beta_{0,\dots,0}}, \\ \omega^*_{\mu_1,\dots,\mu_{t-1}} &= (-1)^{\mu_1+\dots+\mu_{t-1}}\tfrac{\beta^*_{\mu_1,\dots,\mu_{t-1}}}{\beta^*_{0,\dots,0}}, \\ \mathfrak{M}(\tau_{\mu_1,\dots,\mu_{t-1}}) &= (-1)^{\mu_1+\dots+\mu_{t-1}}\frac{\tau_{\mu_1,\dots,\mu_{t-1}}\left(\beta_{0,\dots,0}\beta^*_{0,\dots,0}\right)}{\sqrt{q^*_1}\cdots\sqrt{q^*_t}}, \end{aligned} \tag{5.6}$$

то условия 1–3 выполнены.

Утверждение. *Если*

$$\begin{aligned} \omega_{\mu_1,\dots,\mu_{t-1}} &= \tfrac{\beta^*_{\mu_1,\dots,\mu_{t-1}}}{\beta^*_{0,\dots,0}}, \\ \omega^*_{\mu_1,\dots,\mu_{t-1}} &= (-1)^{\mu_1+\dots+\mu_{t-1}}\tfrac{\beta_{\mu_1,\dots,\mu_{t-1}}}{\beta_{0,\dots,0}}, \\ \mathfrak{M}(\tau_{\mu_1,\dots,\mu_{t-1}}) &= (-1)^{\mu_1+\dots+\mu_{t-1}}\frac{\tau_{\mu_1,\dots,\mu_{t-1}}\left(\beta_{0,\dots,0}\beta^*_{0,\dots,0}\right)}{\sqrt{q^*_1}\cdots\sqrt{q^*_t}}, \end{aligned} \tag{5.7}$$

то условия 1–3 выполнены.

Для описания алгоритма нам понадобятся следующие величины. Пусть $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq (0,\dots,0)$. Через $\oplus$ будем обозначать сложение целых чисел по модулю 2. Положим

$$\delta_\lambda = (q^*_1)^{\lambda_1}\dots(q^*_{t-1})^{\lambda_{t-1}}(q^*_t)^{\lambda_{u+1}\oplus\dots\oplus\lambda_{t-1}}.$$

Если δ_λ чётно, положим

$$g_\lambda = \frac{\sqrt{\delta_\lambda}}{2},$$

в противном случае положим

$$g_\lambda = \frac{1+\sqrt{\delta_\lambda}}{2}.$$

Тогда $g_\lambda \in \mathcal{O}_M$.

Поскольку $\{\omega_\mu^*\}$ образуют $\mathbb{Q}$-базис поля M и числа g_μ лежат в этом поле, то в самом начале можно предвычислить такие $c_{\mu\xi\eta} \in \mathbb{Q}$, что

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

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 для каждого $\mu \in \{0,1\}^{t-1}$ $\frac{A_\mu}{A_{0,\ldots,0}}$ — приближение к $\frac{\omega_\mu}{\omega_{0,\ldots,0}}$.

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 некоторый смысл, объяснённый в тексте главы, в терминах цепных дробей к числам g_λ.

Действия алгоритма.

1. *Инициализация.* Присвоить начальные значения: положить для всех $\lambda \in \{0,1\}^{t-1}$, $\lambda \neq (0,\ldots,0)$

$$\begin{aligned} A_{0,\ldots,0} &:= 1 \\ A_\lambda &:= 0 \\ x_\lambda &:= 0 \\ (y_\lambda, \tilde{y}_\lambda) &:= (1, \lfloor \tfrac{\delta_\lambda}{4} \rfloor) \\ (z_\lambda, \tilde{z}_\lambda) &:= (1, g_\lambda) \end{aligned}$$

2. *Итерации.* Пока $|A_{0,\ldots,0}| < N_0$, повторять следующие шаги.

3. Выбрать некоторое λ такое, что $z_\lambda = \max_{\mu \neq (0,\ldots,0)} z_\mu$.

4. Вычислить $a = \left\lfloor \frac{g_\lambda + x_\lambda}{y_\lambda} \right\rfloor$.

5. Присвоить $(z_\lambda, \tilde{z}_\lambda) := (\tilde{z}_\lambda - a z_\lambda, z_\lambda)$.

6. Запомнить $x = x_\lambda$, присвоить $x_\lambda := a y_\lambda - x_\lambda - 4\left\{\frac{\delta_\lambda}{4}\right\}$, после чего присвоить $(y_\lambda, \tilde{y}_\lambda) := (\tilde{y}_\lambda - a(x_\lambda - x), y_\lambda)$. (При этом новое значение x_λ всегда целое неотрицательное, а новое значение y_λ натуральное.)

7. Вычислить для всех μ

$$A'_\mu = \frac{\sum_\xi A_\xi c_{\mu\xi\lambda} + A_\mu x_\lambda}{\tilde{y}_\lambda}.$$

(При этом $A'_\mu \in \mathbb{Z}$ для всех μ.) Присвоить $A_\mu := A'_\mu$.

Теорема 5.16. *Алгоритм завершается за $O(\ln N_0)$ шагов. В процессе работы алгоритма всегда выполнены неравенства*

$$0 \leqslant x_\lambda < \sqrt{\delta_\lambda} - g_\lambda,$$

$$0 < y_\lambda < \sqrt{\delta_\lambda};$$

$$Z = \sum_\mu A_\mu \omega_\mu^* \geqslant 1,$$

$$\left| \tau_\lambda \left(\sum_\mu A_\mu \omega_\mu^* \right) \right| \leqslant \frac{\sqrt{|d|}^m}{Z^{\frac{1}{m-1}}} \text{ при } \lambda \neq (0, \ldots, 0).$$

Из теорем 5.15 и 5.16 легко выводится следующее утверждение.

Следствие. Алгоритм даёт бесконечную последовательность приближений, для которых верна оценка

$$\max_\mu \left| \frac{A_\mu}{A_{(0,\ldots,0)}} - \frac{\omega_\mu}{\omega_{(0,\ldots,0)}} \right| \ll |A_{(0,\ldots,0)}|^{-1-\frac{1}{2^{t-1}-1}}.$$

Константа в знаке $\ll$ (которую можно выписать явно) зависит от d и от выбора базиса ω_μ^* и функции $\mathfrak{M}$.

Параграф 5.8 завершает описание предлагаемой новой модификации метода, показывая, как с помощью совместных приближений, вычисленных в параграфе 5.7, и знания оценки всех сопряжённых, вычисленной в параграфе 5.6, можно восстановить точные значения коэффициентов многочлена $\hat{H}_D[\theta]$, введённого в параграфе 5.5, в виде разложения по базису, найденному в параграфе 5.4. В конце параграфа приводится общая схема предлагаемой модификации метода комплексного умножения.

Параграф 5.9, завершающий главу, содержит некоторые численные данные по сравнению скорости работы реализации исходного метода и нашей модификации на отрезке $1000000 \leqslant |D| < 1001000$. Для случайных дискриминантов время уменьшилось примерно в два раза.

Результаты пятой главы опубликованы в работах [2] и [5].

Автор глубоко благодарен своим научным руководителям за постановку задач и помощь в работе. Устинов Алексей Владимирович, доктор физико-математических наук, привлёк моё внимание к изучению свойств операции $x \to g^x$, а также к работам Степанова и Коробова по оценкам числа точек на гиперэллиптических кривых. Михаил Алексеевич Черепнёв, кандидат физико-математических наук, доцент поставил задачу эффективного построения эллиптических кривых с предписанным порядком.

Автор испытывает огромную признательность всему коллективу кафедры теории чисел и отделения аспирантуры механико-математического факультета за поддержку в течение всего времени обучения в аспирантуре и написания диссертации. Автор также благодарен коллегам по работе за проявленное понимание.

Работы автора по теме диссертации

1. Гречников Е. А. Двусторонние оценки числа неподвижных точек дискретного логарифма // Вестник Московского университета. Серия 1. Математика. Механика. 2012. № 3. С. 3–8.

2. Гречников Е. А. Метод комплексного умножения для построения эллиптических кривых и его оптимизации // Прикладная дискретная математика. 2011. Т. 13, № 3. С. 17–54.

3. Гречников Е. А. Оценка суммы символов Лежандра // Матем. заметки. 2010. Т. 88, № 6. С. 859–866.

4. Гречников Е. А. Суммы символов Лежандра от многочленов степени 5 // Современные проблемы математики и механики, т.IV «Математика», выпуск 3. Изд-во Московского университета. 2009. С. 136–145.

5. Гречников Е. А. Оптимизация метода с комплексным умножением построения эллиптической кривой. 2011. Деп. в ВИНИТИ 21.06.11, № 305-В2011.