МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Федоров Глеб Владимирович

Теория функциональных непрерывных дробей в гиперэллиптических полях и ее приложения

Специальность
1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика»

Автореферат
диссертации на соискание учёной степени
доктора физико-математических наук

Москва — 2024

Работа выполнена на кафедре математических и компьютерных методов анализа механико-математического факультета МГУ имени М.В. Ломоносова.

Научный консультант:	**Платонов Владимир Петрович** — академик РАН, доктор физико-математических наук, профессор, ФГУ ФНЦ НИИСИ РАН, отдел теоретической и прикладной алгебры и теории чисел, главный научный сотрудник.
Официальные оппоненты:	**Добровольский Николай Михайлович** — доктор физико-математических наук, профессор ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого», кафедра алгебры, математического анализа и геометрии, заведующий кафедрой;
	Устинов Алексей Владимирович — профессор РАН, доктор физико-математических наук, доцент, ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики», факультет компьютерных наук, департамент больших данных и информационного поиска, профессор;
	Чирский Владимир Григорьевич — доктор физико-математических наук, доцент, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, кафедра математического анализа, профессор.

Защита диссертации состоится «27» декабря 2024 года в 16 ч. 45 мин. на заседании диссертационного совета МГУ.011.4 Московского государственного университета имени М. В. Ломоносова, по адресу: 119991, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», механико-математический факультет, аудитория 14–08.

E-mail: *dissovet.msu.011.4@math.msu.ru*

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки Московского государственного университета имени М.В. Ломоносова» (Москва, Ломоносовский проспект, д. 27) и на портале:

https://dissovet.msu.ru/dissertation/3186

Автореферат разослан «25» октября 2024 года.

Ученый секретарь диссертационного совета
кандидат физико-математических наук В. А. Кибкало

Диссертация посвящена существенному развитию и созданию нового научного направления на стыке таких областей математики как теория чисел, алгебра и арифметическая геометрия. Это стало возможным благодаря предложенным новым методам в теории функциональных непрерывных дробей и построению совершенно новой теории функциональных непрерывных дробей обобщенного типа.

Для мирового математического сообщества многие годы остается недоступным решение проблемы кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел и над полями алгебраических чисел (далее — проблема кручения). С проблемой кручения тесно связаны следующие глубокие проблемы: проблема периодичности разложения в функциональную непрерывную дробь элементов гиперэллиптических полей, проблема существования и построения фундаментальных единиц и S-единиц в гиперэллиптических полях, проблема поиска решений функциональных аналогов уравнений типа Пелля, проблема ограниченности порядков подгрупп кручения в группах классов дивизоров гиперэллиптических кривых. Эти проблемы относятся к числу важных и трудных проблем современной математики. В настоящий момент нет единого подхода, который мог бы приблизить к решению этих проблем, и каждое продвижение дается с большим трудом. Полное решение указанных проблем невозможно без построения эффективных алгоритмов и высокопроизводительных компьютерных вычислений.

В рамках указанных проблем в диссертации разработан новый подход к изучению арифметических свойств гиперэллиптических кривых и гиперэллиптических полей на основании глубокого анализа группы классов дивизоров и построенной теории функциональных непрерывных дробей обобщенного типа. Этот подход позволил обнаружить множество ярких теоретико-числовых, алгебраических и геометрических свойств и связей таких математических объектов, как функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. С помощью разработанных новых методов в диссертации решена проблема классификации эллиптических полей по признаку периодичности функциональных непрерывных дробей над полем рациональных чисел и над квадратичными полями алгебраических чисел для эллиптических полей, входящих в рациональную параметризацию модулярными кривыми.

Масштаб и актуальность рассматриваемых проблем

Для мирового математического сообщества многие годы остается недоступным решение проблемы кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел и над полями алгебраических чисел. Эту проблему можно отнести к важнейшим фундаментальным проблемам теории чисел и алгебраической геометрии.

Проблема существования и поиска фундаментальных единиц в гиперэллиптических полях, проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел, проблема периодичности разложения в функциональную непрерывную дробь элементов гиперэллиптических полей относятся к числу важных и трудных проблем современной математики. Они находятся на стыке таких актуальных и глубоких областей математики, как алгебраическая теория чисел, арифметическая геометрия, диофантова геометрия. В настоящий момент нет единого подхода, который мог бы приблизить к решению этих проблем, и каждое продвижение дается с большим трудом. Полное решение указанных проблем невозможно без построения эффективных алгоритмов и высокопроизводительных компьютерных вычислений.

В последнее время рассматриваемые проблемы получили особую практическую актуальность в связи с активным развитием компьютерной техники, цифровых технологий, высокопроизводительных вычислительных систем, новых криптографических протоколов, интеллектуальных систем защиты информации. Основанием рассматриваемой тематики можно считать классические работы Н. Абеля и П.Л. Чебышева. В этих работах была обнаружена связь функциональных непрерывных дробей с так называемыми эллиптическими интегралами. Благодаря указанным работам и работам К. Якоби[1] был открыт якобиан кривой, построено отображение Абеля-Якоби кривой в ее якобиан, а также была осознана важность подгруппы кручения в якобиане. В дальнейшем фундаментальные результаты были получены в работах Дж. Тейта[2], П. Делиня[3], Ж.-П. Серра[4], Г. Фалтингса[5], Д. Мамфорда[6], Д. Кантора[7], Дж. Игузы[8] и др. Среди

[1] *Jacobi C. G. J.* Considerationes generales de transcendentibus Abelianis. 1832; *Jacobi C. G. J.* De functionibus duarum variabilium quadrupliciter periodicis, quibus theoria transcendentium Abelianarum innititur. 1835.

[2] *Mazur B.*, *Tate J.* Points of order 13 on elliptic curves // Inventiones Mathematicae. 1973. Т. 22, № 1. С. 41—49. ISSN 1432-1297.

[3] *Deligne P.* The Weil conjecture. I // Uspekhi Matematicheskikh Nauk. 1975. Т. 30, № 5. С. 159—190.

[4] *Serre J.-P.* Algebraic groups and class fields. Т. 117. Springer Science & Business Media, 2012.

[5] *Faltings G.* Erratum: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern // Inventiones Mathematicae. 1984. Т. 75, № 2. С. 381—381. ISSN 1432-1297.

[6] *Мамфорд Д.* Лекции о тэта-функциях: (Монография). Мир, 1988. ISBN 9785030007458.

[7] *Cantor D. G.* Computing in the Jacobian of a hyperelliptic curve // Mathematics of computation. 1987. Т. 48, № 177. С. 95—101.

[8] *Igusa J.-i.* Arithmetic variety of moduli for genus two // Annals of Mathematics. 1960. С. 612—649.

современных исследований можно отметить значительные достижения научной школы академика В.П. Платонова, а также работы таких авторов как У. Занье[9], Н. Элкиса[10], Э. Флина[11], Ф. Лепрево[12], Х. Огава[13], Б. Пунен[14], В. Адамс и М. Разар[15], Т. Берри[16], А. Штейн[17], М. Садек[18], А. Пуртен[19] и др. Каждый год представляются к защите PhD диссертации на близкие темы (для примера, З. Шерр[20], Мичиганский университет, 2013 г.; М. Кронберг[21], Университет Ольденбурга, 2015 г.; К. Доусуд[22], Университет штата Орегон, 2015 г.; О. Мер-

[9] *Avanzi R. M.*, *Zannier U. M.* Genus one curves defined by separated variable polynomials and a polynomial Pell equation // Acta Arithmetica. 2001. Т. 99. С. 227—256; *Zannier U.* Hyperelliptic continued fractions and generalized Jacobians // American Journal of Mathematics. 2019. Т. 141, № 1. С. 1—40.

[10] *Elkies N. D.* Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order // preprint, Harvard University. 2010.

[11] *Flynn E. V.* Large rational torsion on abelian varieties // Journal of Number Theory. 1990. Т. 36, № 3. С. 257—265.

[12] *Leprevost F.* Jacobiennes décomposables de certaines courbes de genre 2: torsion et simplicité // J. Théorie des Nombres de Bordeaux. 1991. Т. 7, № 1. С. 283—306; *Leprevost F.* Famille de courbes de genre 2 munies d une classe de diviseurs rationnels d ordre 13 // C. R. Acad. Sci. Paris Ser. I Math. 1991. Т. 313. С. 451—454; *Leprevost F.* Familles de courbes de genre 2 munies d une classe de diviseurs rationnels d ordre 15, 17, 19 ou 21 // C. R. Acad. Sci. Paris Ser. I Math. 1991. Т. 313. С. 771—774; *Leprévost F.* Points rationnels de torsion de jacobiennes de certains courbes de genre 2 // Comptes rendus de l'Académie des sciences. Série 1, Mathématique. 1993. Т. 316, № 8. С. 819—821.

[13] *Ogawa H.* Curves of genus 2 with a rational torsion divisor of order 23 // Proc. Japan Acad. Ser. A Math. Sci. 1994. Т. 70. С. 295—298.

[14] *Poonen B.* Computational aspects of curves of genus at least 2 // Algorithmic Number Theory. Springer Berlin Heidelberg, 1996. С. 283—306. ISBN 9783540706328.

[15] *Adams W. W.*, *Razar M. J.* Multiples of points on elliptic curves and continued fractions // Proceedings of the London Mathematical Society. 1980. Т. 3, № 3.

[16] *Berry T. G.* On periodicity of continued fractions in hyperelliptic function fields // Archiv der Mathematik. 1990. Т. 55, № 3. С. 259—266. ISSN 1420-8938; *Berry T. G.* Continued Fractions in Hyperelliptic Function Fields // Coding Theory, Cryptography and Related Areas. Springer Berlin Heidelberg, 2000. С. 29—41. ISBN 9783642571893; *Berry T. G.* A Type of Hyperelliptic Continued Fraction // Monatshefte für Mathematik. 2005. Т. 145, № 4. С. 269—283. ISSN 1436-5081.

[17] *Stein A.* Introduction to continued fraction expansions in real quadratic function fields // Faculty of Mathematics. University of Waterloo, 2002. С. 1—23; *Jacobson M. J.*, *Scheidler R.*, *Stein A.* Fast arithmetic on hyperelliptic curves via continued fraction expansions // Advances in Coding Theory and Cryptography. World Scientific, 2007. С. 200—243.

[18] *Sadek M.* Periodic continued fractions and elliptic curves over quadratic fields // Journal of Symbolic Computation. 2016. Т. 76. С. 200—218.

[19] *Poorten A. J. van der*, *Tran X. C.* Quasi-Elliptic Integrals and Periodic Continued Fractions // Monatshefte fur Mathematik. 2000. Т. 131, № 2. С. 155—169. ISSN 1436-5081; *Poorten A. J. van der*, *Tran X. C.* Periodic Continued Fractions in Elliptic Function Fields // Algorithmic Number Theory. Springer Berlin Heidelberg, 2002. С. 390—404. ISBN 9783540454557; *Poorten A. van der.* Periodic continued fractions and elliptic curves. 2004; *Pappalardi F.*, *Van Der Poorten A. J.* Pseudo-elliptic integrals, units, and torsion // Journal of the Australian Mathematical Society. 2005. Т. 79, № 3. С. 335—347. ISSN 1446-8107.

[20] *Scherr Z. L.* Rational Polynomial Pell Equations : PhD thesis / Scherr Zachary L. The University of Michigan, 2013.

[21] *Kronberg M.* Explicit construction of rational torsion divisors on Jacobians of curves : PhD thesis / Kronberg Max. Universit at Oldenburg, 2016.

[22] *Daowsud K.* Continued fractions and the divisor at infinity on a hyperelliptic curve: Examples and order bounds : PhD thesis / Daowsud Katthaleeya. Oregon State University, 2013.

серт[23], Высшая нормальная школа (Пиза), 2016 г.; Ф. Малаголи[24], Пизанский университет, 2017 г.; М.М. Петрунин[25], НИИСИ РАН, 2019 г.; В. Арул[26], Массачусетский технологический институт, 2020 г.; Д. Ричман[27], Мичиганский университет, 2020; Н.А. Каладжиева[28], Университетский колледж Лондона, 2020 г.; С.А. Линднер[29], Университет Калгари, 2020 г.; Т. Гузвич[30], Загребский университет, 2021 г.; С. Добсон[31], Оклендский университет, 2022 г.; С. Ноуэлл[32], Университетский колледж Лондона, 2022 г.; Х. Грин[33], Университетский колледж Лондона, 2023 г.).

Проблема ограниченности подгрупп кручения в якобианах гиперэллиптических кривых над полем $\mathbb{Q}$ остается открытой уже более 40 лет даже для кривых рода 2. За это время не было найдено существенных идей для решения этой проблемы в общем виде. Усилиями целого ряда математиков было доказано существование гиперэллиптических кривых рода 2, в якобианах которых есть $\mathbb{Q}$-точки порядка m, $1 \leq m \leq 30$, $m \in \{32, 33, 34, 35, 36, 39, 40, 45, 48, 60, 63, 70\}$. Эти точки были получены с использованием различных методов, индивидуальных для отдельных порядков.

В 2012 году новый метод В.П. Платонова[34] позволил завершить доказательство гипотезы о существовании $\mathbb{Q}$-точек порядков m, $m \leq 30$, в якобианах различных гиперэллиптических кривых рода 2. Ранее для кривых C рода $g = 2$ М. Столлом[35] был предложен p-адический алгоритм вычисления подгруппы кру-

[23] *Merkert O.* Reduction and specialization of hyperelliptic continued fractions : PhD thesis / Merkert Olaf. Scuola Normale Superiore, 2017.

[24] *Malagoli F.* Continued fractions in function fields: polynomial analogues of McMullen's and Zaremba's conjectures : PhD thesis / Malagoli Francesca. Università di Pisa, 2017.

[25] *Петрунин М. М.* S-единицы и функциональные непрерывные дроби в гиперэллиптических полях : PhD thesis / Петрунин Максим Максимович. НИИСИ РАН, 2019.

[26] *Arul V.* Explicit division and torsion points on superelliptic Curves and jacobians : PhD thesis / Arul Vishal. Massachusetts Institute of Technology, 2020.

[27] *Richman D.* Weierstrass points and torsion points on tropical curves : PhD thesis / Richman David. The University of Michigan, 2020.

[28] *Kalaydzhieva N. D.* On problems related to multiple solutions of Pell's equation and continued fractions over function fields : PhD thesis / Kalaydzhieva Nikoleta Dianova. University College London, 2020.

[29] *Lindner S. A.* Improvements to Divisor Class Arithmetic on Hyperelliptic Curves : PhD thesis / Lindner Sebastian A. University of Calgary, 2020.

[30] *Gužvić T.* Torsion of elliptic curves with rational j-invariant over number fields : PhD thesis / Gužvić Tomislav. University of Zagreb, 2021.

[31] *Dobson S.* Key Exchange and Zero-Knowledge Proofs from Isogenies and Hyperelliptic Curves : PhD thesis / Dobson Samuel. The University of Auckland, 2022.

[32] *Nowell S. C.* Models of hyperelliptic curves over p-adic fields : PhD thesis / Nowell Sarah Catherine. University College London, 2022.

[33] *Green H.* The Parity Conjecture for Hyperelliptic Curves : PhD thesis / Green Holly. University College London, 2023.

[34] *Платонов В. П.*, *Петрунин М. М.* О проблеме кручения в якобианах кривых рода 2 над полем рациональных чисел // Докл. РАН. 2012. Т. 446, № 3. С. 263—264.

[35] *Stoll M.* On the height constant for curves of genus two // Acta Arithmetica. 1999. Т. 90, № 2. С. 183—201.

чения $J(\mathbb{Q})_{tors}$, который в дальнейшем был расширен для кривых рода 3[36].

Долгое время не удавалось найти кривые рода 2 над полем $\mathbb{Q}$, якобиан которых содержит $\mathbb{Q}$-точку порядка 28[37]. Первая такая кривая была найдена в 2012 году В.П. Платоновым и М.М. Петруниным[38], тем самым было завершено доказательство вышеупомянутой гипотезы[39] о том, что для всякого $m \leq 30$ существует кривая рода 2 над полем $\mathbb{Q}$ рациональных чисел, якобиан которой содержит $\mathbb{Q}$-точку порядка m. В дальнейшем научная группа под руководством академика В.П. Платонова нашла другие примеры кривых рода 2 над полем $\mathbb{Q}$, якобиан которых содержит $\mathbb{Q}$-точки порядка 28 и других высоких порядков[40]. В 2018 году В.П. Платонов и Г.В. Федоров нашли бесконечное семейство неизоморфных гиперэллиптических кривых рода 2 над полем $\mathbb{Q}$, якобиевы многообразия которых содержат $\mathbb{Q}$-точки порядка 28.

На данный момент известны различные гиперэллиптические кривые рода 2, якобианы которых обладают $\mathbb{Q}$-точками кручения всех простых порядков вплоть до 29, причем для порядка $m = 29$ с точностью до изоморфизма до сих пор известна только одна такая кривая.

В работе К. Николса[41] приведено актуальное состояние множества известных реализуемых порядков кручения в якобианах гиперэллиптических кривых рода 2, 3, 4 над полем рациональных чисел. Среди указанных примеров якобиевых многообразий выделяются абсолютно простые, поскольку они не могут быть получены путем спаривания эллиптических кривых[42].

Основой алгебраического подхода к фундаментальной проблеме кручения в якобианах гиперэллиптических кривых является глубокая связь между нетривиальными S-единицами гиперэллиптического поля и точками конечного порядка в якобиане гиперэллиптической кривой[43]. В свою очередь, проблема поиска и

[36] *Stoll M.* An explicit theory of heights for hyperelliptic Jacobians of genus three // Algorithmic and experimental methods in algebra, geometry, and number theory. 2017. С. 665—715; *Müller J. S.*, *Reitsma B.* Computing torsion subgroups of Jacobians of hyperelliptic curves of genus 3 // Research in Number Theory. 2023. Т. 9, № 2. С. 23.

[37] *Elkies N. D.* Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order. URL: https://people.math.harvard.edu/~elkies/g2_tors.html#bkgd (дата обр. 17.03.2024).

[38] *Платонов В. П.*, *Петрунин М. М.* Новые порядки точек кручения в якобианах кривых рода 2 над полем рациональных чисел // Докл. РАН. 2012. Т. 443, № 6. С. 664—664.

[39] *Платонов В. П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // Успехи математических наук. 2014. Т. 69, 1 (415. С. 3—38.

[40] *Платонов В. П.*, *Петрунин М. М.* Новые кривые рода 2 над полем рациональных чисел, якобианы которых содержат точки кручения больших порядков // Докл. РАН. Матем., информ., проц. упр. 2015. Т. 461, № 6. С. 638—638.

[41] *Nicholls C.* Descent methods and torsion on Jacobians of higher genus curves : PhD thesis / Nicholls Christopher. University of Oxford, 2018.

[42] *Платонов В. П.*, *Петрунин М. М.*, *Жгун В. С.* К вопросу о простоте якобианов кривых рода 2 над полем рациональных чисел с точками кручения больших порядков // Докл. РАН. Матем., информ., проц. упр. 2013. Т. 450, № 4. С. 385—388.

[43] *Платонов В. П.* Арифметика квадратичных полей и кручение в якобианах // Докл. РАН. 2010. Т. 430,

построения нетривиальных S-единиц гиперэллиптического поля тесно связана с проблемой периодичности функциональных непрерывных дробей, в которые могут разлагаться элементы гиперэллиптического поля. В.П. Платонов высказал две гипотезы. Первая утверждает, что степень фундаментальной единицы в гиперэллиптических полях данного рода над полем рациональных чисел ограничена. Вторая гипотеза является обобщением первой и утверждает, что степень фундаментальных S-единиц в гиперэллиптических полях данного рода над полем рациональных чисел ограничена. Обе эти гипотезы являются трудными и глубокими.

Сформулированные проблемы важны и актуальны в мировом научном пространстве. В последние годы рассматриваемые задачи вызывают живой интерес у ведущих специалистов в современных областях математики в связи с развитием новых теоретико-числовых, алгебро-геометрических и вычислительных подходов к их решению. Результаты теоретических и практических исследований могут быть использованы в криптографии[44]: при создании новых криптографических протоколов[45], в вопросах исследования стойкости существующих криптосистем (например, атака Винера[46], ро-алгоритм Полларда[47], алгоритм Гельфонда — Шенкса[48], алгоритм индексного исчислениея для абелевых многообразий[49]), в теории кодирования[50] для анализа псевдослучайных последовательностей[51] и в других разделах интеллектуальной защиты информации.

№ 3. С. 318—320.

[44] *Koblitz N.* Algebraic aspects of cryptography. Т. 3. Springer Science & Business Media, 2012; Handbook of elliptic and hyperelliptic curve cryptography / H. Cohen [и др.]. CRC press, 2005; *Galbraith S. D.* Mathematics of public key cryptography. Cambridge University Press, 2012; *Wollinger T.* Software and hardware implementation of hyperelliptic curve cryptosystems. Ruhr University Bochum, 2004.

[45] *Koblitz N.* Hyperelliptic cryptosystems // Journal of cryptology. 1989. Т. 1. С. 139—150; Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors / M. Katagi [и др.] // Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers 5. Springer. 2005. С. 345—359; *Lange T.* Formulae for arithmetic on genus 2 hyperelliptic curves // Applicable Algebra in Engineering, Communication and Computing. 2005. Т. 15. С. 295—328.

[46] *Wiener M. J.* Cryptanalysis of short RSA secret exponents // IEEE Transactions on Information theory. 1990. Т. 36, № 3. С. 553—558.

[47] *Pollard J. M.* A Monte Carlo method for factorization // BIT Numerical Mathematics. 1975. Т. 15, № 3. С. 331—334.

[48] *Shanks D.* The infrastructure of a real quadratic field and its applications // Proceedings of the Number Theory Conference. University of Colorado, Boulder, 1972. С. 217—224; *Нечаев В.* Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и педвузов. М.: Высшая школа, 1999.

[49] *Shoup V.* Lower bounds for discrete logarithms and related problems // Advances in Cryptology—EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings 16. Springer. 1997. С. 256—266; *Gaudry P.* Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem // Journal of Symbolic computation. 2009. Т. 44, № 12. С. 1690—1702.

[50] *Faure C.*, *Minder L.* Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes // Proceedings of the 11th international workshop on Algebraic and Combinatorial Coding Theory, ACCT. Т. 2008. 2008. С. 99—107; *Joyner D.*, *Kim J.-L.* Selected unsolved problems in coding theory. Springer Science & Business Media, 2011.

[51] *Niederreiter H.* Sequences with almost perfect linear complexity profile // Advances in Cryptology—

Научные проблемы диссертации и степень их разработанности

Тематика диссертации лежит на стыке таких областей математики как теория чисел, алгебра и алгебраическая геометрия. Исследования выполнены в рамках научной школы академика РАН В.П. Платонова.

Одним из наиболее интересных и изученных направлений арифметической (диофантовой) геометрии[52] является теория алгебраических кривых $C = \{(x, y) \in K \times K \mid F(x, y) = 0\}$, где $F(x, y) \in K[x, y]$ — неприводимый многочлен от двух переменных над полем K. Наши усилия сконцентрированы в первую очередь на алгебраическом и теоретико-числовом подходах изучения свойств алгебраических кривых и их полей функций над алгебраически незамкнутыми полями K. Алгебраический подход берет свое начало с работ Р. Дедекинда и Л. Кронекера 19 века (над полем комплексных чисел $\mathbb{C}$), а далее продолжен в начале 20-го века в работах Х. Хассе, Ф.К. Шмидта и А. Вейля (подробнее см. в книках К. Шевалле[53] и М. Дойринг[54]). Теоретико-числовой подход и связь с алгебраической теорией чисел представлен, например, в работах Э. Артина[55] и М. Эйхлера[56]. Современное изложение этих подходов представлено, например, в книгах И.Р. Шафаревича[57] и Х. Стихтенота[58].

Важным аспектом наших исследований является применение для объектов в полях алгебраических функций теоретико-числовых конструкций или построение их аналогов в функциональном случае. Среди таких конструкций можно отметить теорию непрерывных дробей, решение норменных уравнений и уравнений типа Пелля, поиск единиц и S-единиц колец целых элементов, применение арифметики дивизоров.

Вдохновение к применению теоретико-числовых методов к алгебраическим и геометрическим задачам исходит от классических работ Н. Абеля и П.Л. Чебышева, в которых впервые была отмечена удивительная связь между такими фундаментальными проблемами, как проблема периодичности функциональных непрерывных дробей, проблема кручения в якобианах гиперэллиптических кривых, проблема решения норменных уравнений и уравнений типа Пелля в функциональном случае.

EUROCRYPT'87: Workshop on the Theory and Application of Cryptographic Techniques Amsterdam, The Netherlands, April 13–15, 1987 Proceedings 6. Springer. 1988. С. 37—51.

[52] *Lang S.* Fundamentals of Diophantine geometry. Springer Science & Business Media, 2013; *Hindry M., Silverman J. H.* Diophantine geometry: an introduction. Т. 201. Springer Science & Business Media, 2013.

[53] *Chevalley C.* Introduction to the theory of algebraic functions of one variable. American Mathematical Soc., 1951.

[54] *Deuring M.* Lectures on the theory of algebraic functions of one variable. Т. 314. Springer, 2006.

[55] *Artin E.* Algebraic numbers and algebraic functions. Т. 358. American Mathematical Soc., 2005.

[56] *Eichler M.* Introduction to the Theory of Algebraic Numbers and Fuctions. Academic Press, 1966.

[57] *Шафаревич И. Р.* Основы алгебраической геометрии. МЦНМО, 2007.

[58] *Stichtenoth H.* Algebraic function fields and codes. Т. 254. Springer Science & Business Media, 2009.

В.П. Платонов в ключе рассмотрения этих трех проблем предложил ряд новых основополагающих идей, позволяющих не только установить тесную связь между этими проблемами, но и выделить новую самостоятельную область исследований, лежащую на границе теории чисел, алгебры, и геометрии. Важную роль в новом подходе, предложенном В.П. Платоновым, играют алгебраические и теоретико-числовые методы исследования фундаментальных единиц и S-единиц колец целых и S-целых элементов в гиперэллиптических полях (полях функций гиперэллиптических кривых). Тем самым, к указанным трем проблемам добавляется еще одна — проблема поиска и построения фундаментальных единиц и S-единиц в гиперэллиптических полях.

Эллиптическим кривым посвящено огромное количество книг и статей, в которых получены впечатляющие результаты, в том числе имеющие важнейшее прикладное значение в современном “цифровом мире”. Однако остаются и множество нерешенных задач. Ряд результатов, представленных в этой диссертации, также относится к разделу исследований эллиптических кривых и связанных с ними объектов (см., например, главу 4).

Для кривых рода 2 и выше значительно меньше качественных результатов по сравнению с эллиптическими кривыми. Среди таких результатов можно, например, отметить знаменитую гипотезу Л. Морделла[59], доказанную в 1983 году Г. Фалтингсом[60]. Теорема Фалтингса утверждает, что на кривых C рода 2 и выше, определенных над полями алгебраических чисел K, может содержаться только конечное число K-точек. Но эта теорема неэффективна в том смысле, что не дает алгоритм, позволяющий найти все K-точки на кривой C. В рассматриваемых нами проблемах мы также сталкиваемся с подобным разделением качественных и количественных результатов (см., например, §§3.3.3-3.3.6 диссертации).

В последние 30 лет с ростом возможностей вычислительной техники количественные результаты вышли на новый уровень, что не только взвинтило интерес к рассматриваемым проблемам, но и привело к существенному развитию теоретико-числовых методов компьютерной алгебры. В связи с этим академик В.П. Платонов отмечает, что “естественное соединение глубокой теории, математических алгоритмов, софтверной реализации и супервычислений будет играть все большую роль в математике 21 века”. Отметим, что часть результатов диссертации, несмотря на свой фундаментальный теоретический характер, были бы невозможны без применения высокопроизводительных компьютерных вычислений (см., например, главу 4 диссертации).

Путь A — абелево многообразие размерности g над полем алгебраических

[59] *Mordell L. J.* On the rational resolutions of the indeterminate equations of the third and fourth degree // Proc. Cambridge Phil. Soc. T. 21. 1922. C. 179—192.

[60] *Faltings G.* Endlichkeitssätze für abelsche Varietäten über Zahlkörpern // Inventiones Mathematicae. 1983. T. 73, № 3. C. 349—366. ISSN 1432-1297.

чисел K. Теорема Мордела-Вейля[61] утверждает, что множество K-точек $A(K)$ многообразия A является конечно порожденной абелевой группой. По теореме о классификации конечнопорожденных абелевых групп группа $A(K)$ изоморфна прямому произведению свободной абелевой группы ранга r и $A(K)_{tors}$ — группы кручения K-точек многообразия A: $A(K) \simeq \mathbb{Z}^r \times A(K)_{tors}$. Естественным образом возникают две глобальные проблемы: проблема полного перечисления конечных групп, реализуемых как группа кручения $A(K)_{tors}$ многообразия A над полями алгебраических чисел K, и проблема полного описания многообразий A над полями алгебраических чисел K, реализующих данную группу кручения $A(K)_{tors}$.

В качестве абелевых многообразий в диссертации в первую очередь рассматриваются якобиевы многообразия (якобианы) $J(C)$ неособых алгебраических кривых C рода g. Проблема ограниченности подгрупп кручения (проблема кручения) в якобианах гиперэллиптических кривых рода g над полем рациональных чисел $\mathbb{Q}$ является одной из фундаментальных проблем теории чисел и алгебраической геометрии. Ее важность для современной математики подчеркивается колоссальным множеством работ, появившихся в этой области с начала XX века. В последнее время с появлением новых теоретико-числовых методов исследования, в том числе с использованием компьютерных вычислений, эта проблема получила особую актуальность. Проблему кручения в якобианах гиперэллиптических кривых над полем рациональных чисел можно разделить на две проблемы: проблема об оценке и описания подгрупп кручения якобианов кривых данного рода g и проблема нахождения порядков точек кручения.

Для эллиптических кривых E якобиан изоморфен самой кривой. В этом случае проблема кручения над полем рациональных чисел была полностью решена Б. Мазуром[62] в 1978 году, а именно было доказано, что порядок m $\mathbb{Q}$-точки кручения может принимать одно из значений $1 \leq m \leq 10$, $m = 12$. Более того, были выписаны все 15 групп, которые могут быть реализованы как подгруппы кручения $E(\mathbb{Q})_{tors}$ эллиптических кривых над полем $\mathbb{Q}$. В дальнейшем исследования подгрупп кручения эллиптических кривых были активно продолжены над полями алгебраических чисел K небольшой степени[63]. Эти результаты нашли

[61] *Weil A.* L'arithmétique sur les courbes algébriques // Oeuvres Scientifiques Collected Papers. Springer New York, 1979. C. 11—45. ISBN 9781475717051; *Weil A.* L'arithmétique sur les courbes algébriques // Acta mathematica. 1929. T. 52, № 1. C. 281—315.

[62] *Mazur B.* Rational points on modular curves // Modular Functions of one Variable V: Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik July 2–14, 1976. Springer. 2006. C. 107—148; *Mazur B.*, *Goldfeld D.* Rational isogenies of prime degree // Inventiones mathematicae. 1978. T. 44. C. 129—162.

[63] *Kubert D. S.* Universal bounds on the torsion of elliptic curves // Proceedings of the London Mathematical Society. 1976. T. s3—33, № 2. C. 193—237. ISSN 0024-6115; *Kenku M. A.*, *Momose F.* Torsion points on elliptic curves defined over quadratic fields // Nagoya Mathematical Journal. 1988. T. 109. C. 125—149. ISSN 2152-6842; *Sutherland A. V.* Constructing elliptic curves over finite fields with prescribed torsion // Mathematics of

применение для исследования функциональных непрерывных дробей элементов эллиптических полей и связанных с ними проблем (подробнее см. в главе 4 диссертации).

В связи с отсутствием глобальных подходов основные усилия специалистов в этой области были направлены на решение проблемы кручения для кривых с фиксированным родом $g = 2, 3, 4$. Надо отметить, что результаты, полученные в этом направлении за последнее время, заключались в поиске кривых, якобианы которых обладают точками кручения определенного порядка. Более того, они имели частный характер и опирались на специфические свойства конкретных кривых[64].

В.П. Платонов предложил в этом направлении три новых метода, которые, в частности, позволили существенно продвинуться в поиске кривых, якобианы которых обладают точками кручения высоких порядков. Первый метод базируется на применении и исследовании теории ганкелевых матриц. Второй метод базируется на свойствах функциональных непрерывных дробей. Наконец, в основе третьего метода лежат свойства фундаментальных S-единиц и связанных с ними функциональных уравнений типа Пелля.

В рамках диссертации мы продолжаем эти исследования и предлагаем новые подходы к указанным проблемам, основанные на теории функциональных непрерывных дробей (см. главы 3, 4 диссертации), развитом анализе дивизоров, а также на арифметике дивизоров с использованием представления Мамфорда и функциональных непрерывных дробей обобщенного типа (см. главу 5 диссертации).

Объект и предмет исследования

В диссертации исследуется строение и свойства гиперэллиптических кривых и гиперэллиптических полей, а также связанных с ними теоретико-числовых, алгебраических и геометрических объектов таких, как функциональные непрерывные дроби, функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. Отдельное внимание уделяется исследованию связей и зависимостей между этими объектами и их ключевыми свойствами. Приведенные объекты рассматриваются как над произвольными полями K характеристики,

Computation. 2011. Т. 81, № 278. С. 1131—1147. ISSN 1088-6842; *Rabarison F. P.* Structure de torsion des courbes elliptiques sur les corps quadratiques // Acta Arithmetica. 2010. Т. 144, № 1. С. 17—52. ISSN 1730-6264; *Kamienny S.*, *Najman F.* Torsion groups of elliptic curves over quadratic fields // Acta Arithmetica. 2012. Т. 152, № 3. С. 291—305. ISSN 1730-6264; *Sutherland A. V.* Torsion subgroups of elliptic curves over number fields // Avalaible on https://math.mit.edu/drew/MazursTheoremSubsequentResults.pdf. 2012. Т. 1. С. 14.

[64] *Howe E. W.* Genus-2 Jacobians with torsion points of large order // Bulletin of the London Mathematical Society. 2015. Т. 47, № 1. С. 127—135.

отличной от 2, так и в отдельных случаях над полем рациональных чисел $\mathbb{Q}$ или над полями алгебраических чисел, являющимися конечными расширениями поля $\mathbb{Q}$.

Методы исследования

В работе используются как традиционные методы алгебраической теории чисел, классических направлений алгебры и арифметической геометрии, так и возникшие недавно (в том числе в работах автора) новые арифметические методы из теории функциональных непрерывных дробей, теории единиц колец целых или S-целых элементов гиперэллиптических полей, теории дивизоров гиперэллиптических кривых. Ряд результатов получен с использованием систем компьютерной алгебры и символьных компьютерных вычислений.

Теоретическая и практическая ценность

Диссертация носит теоретический характер. Ее результаты могут быть использованы в таких теоретических разделах математики, как алгебраическая теория чисел, диофантова геометрия и арифметическая геометрия. Также результаты диссертации могут быть использованы в области защиты информации и в системах компьютерной алгебры.

Степень достоверности и апробации результатов

Достоверность всех результатов исследований обоснована строгими математическими доказательствами.

Результаты диссертации многократно докладывались на научных семинарах, в частности, на семинарах отдела теоретической и прикладной алгебры и теории чисел НИИСИ РАН под руководством академика РАН В.П. Платонова; на научно-исследовательском семинаре кафедры математических и компьютерных методов анализа (под руководством профессора В.Н. Чубарикова), на научно-исследовательском семинаре кафедры высшей алгебры (под руководством профессора В.А. Аратамонова, профессора В.Н. Латышева) на научно-исследовательском семинаре “Узлы и теория представлений” (под руководством профессора О.В. Мантурова, доцента И.М. Никонова) механико-математического факультета МГУ имени М.В. Ломоносова; на отчетных семинарах научного центра информационных технологий и искусственного интеллекта Университета Сириус.

Результаты диссертации были доложены на международных и всероссийских научных конференциях, среди которых: VII-XXII Международная конференция «Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории» в 2010-2023 гг. в г. Тула, г. Саратов, г. Волгоград; I-IV Конференция памяти А. А. Карацубы по теории чисел и приложениям в 2014-2017 гг. в г. Москва; Международная научная конференция «Современные проблемы математики и механики», посвященная 80-летию академика В. А. Садовничего в 2019 году в г. Москва; Международная конференция «Аналитическая теория чисел», посвященная 75-летию Г.И. Архипова и С.М. Воронина в 2020 году в г. Москва; III-IV Конференция математических центров России в 2023-2024 году в г. Майкоп и в г. Санкт-Петербург; Конференция "Современные проблемы теории чисел" в 2024 году в пгт. Сириус и др.

Работа выполнена при частичной поддержке РНФ, проект №22-71-00101, проект №19-71-00029 (разделы 3.3, 4.3, 5.3, 5.4).

Цели и задачи диссертации

Главными целями диссертации являются следующие:

1. нахождение точных оценок длин периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по нормированию первой степени, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц;

5. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по двум несопряженным линейным нормированиям, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц;

6. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по нормированию второй степени, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц.

Научная новизна

Все основные результаты диссертации являются новыми и получены автором самостоятельно.

Некоторые результаты диссертации опубликованы в статьях, написанных в соавторстве с научным консультантом В.П. Платоновым в ходе тесной нераздельной совместной работы (разделы 3.2, 4.1, 4.2, 5.2). Эти совместные результаты важны и имеют принципиальный характер для диссертации.

Основные результаты состоят в следующем:

1. найдены точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. разработана теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

Положения, выносимые на защиту

По результатам исследований на защиту выносятся следующие положения и утверждения:

1. точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

Публикации

Основные результаты диссертации опубликованы в 20 работах автора: [1—20]. Все указанные работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика» и входящих в базы цитирования RSCI, Scopus, Web of Science.

Структура и объем работы

Диссертация состоит из введения и пяти глав. Главы разбиты на разделы, а разделы на подразделы — параграфы. Текст диссертации изложен на 298 страницах. Список литературы содержит 187 наименований. Порядок библиографии соответствует упоминанию публикаций в тексте. Нумерация утверждений, формул и замечаний подчинена нумерации глав, разбиению глав на разделы и разделов на параграфы. Номера следствий подчинены теоремам. Номера теорем во введении соответствуют нумерации в тексте диссертации.

Содержание работы

Диссертация посвящена исследованию четырех фундаментальных проблем алгебраической теории чисел и арифметической геометрии, а также связи между ними: проблема кручения в якобианах гиперэллиптических кривых, проблема периодичности функциональных непрерывных дробей, проблема решения норменных уравнений и уравнений типа Пелля в функциональном случае, проблема поиска и построения фундаментальных единиц и S-единиц в гиперэллиптических полях. Эти проблемы рассматриваются как над произвольными полями констант K, характеристики отличной от двух, так и в отдельных случаях над полями алгебраических чисел или над $\mathbb{Q}$.

Далее представим краткий обзор структуры и основных результатов диссертации. В каждой главе и в каждом разделе приведено более детальное описание полученных результатов, обзор основной литературы, посвященной рассматриваемой теме, и ссылки на статьи, где эти результаты были опубликованы.

Глава 1 является вводной, в ней содержится общая характеристика работы, представлено описание научных проблем диссертации, указан их масштаб и актуальность, приведены вводные и исторические сведения рассматриваемой тематики, а также описана структура и приведены основные результаты диссертации.

В главе 2 дается краткое изложение необходимых базовых понятий и утверждений, которые используются в диссертации. Отметим, что по возможности изложение ведется на языке алгебры и алгебраической теории чисел, поскольку именно такой подход к указанным проблемам используется в диссертации. Наиболее важными являются §2.3.2 и §2.4.5, в которых дается введение в теорию нормирований и теорию дивизоров гиперэллиптических полей. В дальнейшем эти понятия используется на протяжении всей диссертации[65].

Глава 3 посвящена исследованию функциональных непрерывных дробей и их свойств таких, как периодичность и квазипериодичность (§3.1.6, §3.1.7, §3.2.1, §3.2.3), свойство наилучшего приближения (§3.1.8), связь с уравнениями типа Пелля (§3.1.8, §3.2.1, §3.2.2) и с нетривиальными единицами и S-единицами гиперэллиптического поля (§3.2.1, §3.3.3). Также в этой главе рассматриваются вопросы о строении функциональной непрерывной дроби: симметрии периодов и квазипериодов (§3.1.6, §3.1.7, §3.2.5), оценки на длины предпериодов, квазипериодов и периодов (§3.1.2, §§3.3.2-3.3.4). Основные результаты и утверждения снабжены показательными примерами и контрпримерами (§3.2.4, §3.2.5, §3.3.4). Исследования ведутся как элементарным методом, так и с помощью анализа дивизоров объектов, связанных с функциональными непрерывными дробями. Отдельное внимание заслуживают вычислительные приложения функциональных непрерывных дробей. Для поиска точек конечного порядка в якобиане гиперэллиптической кривой стандартной техникой является использование алгоритма Кантора (§2.4.6) и его обобщений[66]. В §3.2.4 для этой задачи предложены эффективные алгоритмы, основанные на применении функциональных непрерывных дробей (см. также §3.1.4).

Отдельно отметим раздел 3.3, в котором получены оценки сверху на длины периодов и квазипериодов функциональных непрерывных дробей произвольных элементов гиперэллиптического поля (см. теоремы 3.3.2.3, 3.3.2.4 и следствие 3.3.2.4). В теореме 3.3.3.3 и следствии 3.3.3.5 найдены точные оценки на длину периода и длину квазипериода непрерывной дроби для “ключевых” элементов вида $\sqrt{f}/x^s$ гиперэллиптического поля $L = K(x)(\sqrt{f})$, определенного над полем K алгебраических чисел.

Теорема (3.3.3.3)**.** *Пусть K — расширение поля рациональных чисел $\mathbb{Q}$ степени k. Пусть $f \in K[x]$ — свободный от квадратов многочлен, и в кольце целых элементов поля $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $u = \Psi_1+\Psi_2\sqrt{f}$ степени m, где $\Psi_1, \Psi_2 \in K[x]$. Пусть для $j \in \mathbb{N}$ многочлены $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[x]$*

[65] *Fulton W.* Algebraic Curves: An Introduction To Algebraic Geometry. Third edition. Benjamin, New York, 2008; *Galbraith S. D.* Mathematics of public key cryptography. Cambridge University Press, 2012; *Silverman J. H.* The arithmetic of elliptic curves. Т. 106. Springer, 2009; *Mumford D.*, *Ramanujam C. P.*, *Manin J. I.* Abelian varieties. Т. 5. Oxford university press Oxford, 1974; *Харрис Д.* Алгебраическая геометрия. Начальный курс. 2005; *Griffiths P.*, *Harris J.* Principles of algebraic geometry. John Wiley & Sons, 2014; *Hartshorne R.* Algebraic geometry. Т. 52. Springer Science & Business Media, 2013.

[66] *Paulus S.*, *Stein A.* Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves // Algorithmic Number Theory. Springer Berlin Heidelberg, 1998. С. 576—591. ISBN 9783540691136.

определены соотношениями

$$\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{f} = \left(\Psi_1 + \Psi_2\sqrt{f}\right)^j.$$

1. *Если хотя бы одно из значений* $v_x(f), v_x(\Psi_1), v_x(\Psi_2)$ *отлично от нуля, то непрерывная дробь элемента* $\sqrt{f}/x^s$*, построенная в* $K((1/x))$*, периодическая тогда и только тогда, когда*

$$-v_x(\Psi_1) - v_x(\Psi_2) \le s \le v_x(\Psi_1) + v_x(\Psi_2) + v_x(f).$$

   В случае периодичности непрерывной дроби $\sqrt{f}/x^s$*, длина квазипериода* N *не превосходит* $m-\delta$*, где значение* δ *определено при некотором* $f_1 \mid f$*,* $\deg f_1 < \deg f$*,*

$$\delta = \max\bigl(0, |g+1-s|-1\bigr) + \max\bigl(0, |s+g+1-\deg f_1|-1\bigr).$$

2. *Если* $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$*, то непрерывная дробь элемента* $\sqrt{f}/x^s$*, построенная в* $K((1/x))$*, периодическая тогда и только тогда, когда найдется такой номер* n*, что* $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(n-1)}\right) = 0$*,* $|s| \le v_x\left(\Omega_2^{(n)}\right)$ *и* $\phi(n) \mid 2k$*. В случае периодичности непрерывной дроби* $\sqrt{f}/x^s$*, длина квазипериода* N *не превосходит* $nm-\delta$*.*

Найденные оценки являются точными как в случае, когда гиперэллиптическое поле задается многочленом четной степени, так и в случае, когда гиперэллиптическое поле задается многочленом нечетной степени. Особенность четного случая заключается в том, что длина квазипериода может быть в несколько раз больше степени фундаментальной S-единицы (см. соответствующие примеры в §3.3.4). В связи с этим неожиданным свойством, в §3.3.6 доказано, что в каждом гиперэллиптическом поле, обладающим периодическими элементами, найдется такой элемент, длина периода которого больше любого наперед заданного числа. В §3.3.5 для гиперэллиптического поля L, определенного над полем K алгебраических чисел, доказана теорема 3.3.5.1 о конечности множества таких дискриминантов D, что найдется элемент $\alpha \in L$ с дискриминантом D, обладающий квазипериодическим разложением в непрерывную дробь. В §3.3.7 найденные результаты проиллюстрированы на случае, когда базовое поле K является квадратичным расширением поля $\mathbb{Q}$.

Глава 4 посвящена проблеме классификации эллиптических полей, имеющих вид $L = K(x)(\sqrt{f})$, по признаку периодичности непрерывных дробей для ключевых элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$. Проблема классификации впервые была поставлена академиком В.П. Платоновым в 2017 году. Наиболее важной и трудной в проблеме классификации является задача о поиске полей $L = K(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$. Если рассматривать непрерывные дроби в поле формальных степенных рядов $K((1/x))$ и многочлены f четной степени, то этой задаче посвящено много работ .

Для случая поля формальных степенных рядов $K((x))$ сначала различными методами удавалось найти только примеры полей $L = K(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь (см. §4.1.1 и[67]). В разделе 4.1 найдено полное решение проблемы классификации для кубических эллиптических полей над полем рациональных чисел. В теореме 4.1.3.1 доказано, что за исключением тривиальных случаев с точностью до изоморфизма существует только 3 эллиптических поля $L = \mathbb{Q}(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $\mathbb{Q}((x))$. Позднее коллективом под руководством В.П. Платонова удалось существенно продвинуться в этой задаче для кубических эллиптических полей, определенных над конечными расширениями K поля рациональных чисел, $[K : \mathbb{Q}] \leq 6$ (см.[68]), а также вне зависимости от поля K с органичениями на степень фундаментальной S-единицы (см.[69]).

В разделе 4.2 найдено полное решение проблемы классификации для эллиптических полей, заданных многочленом четвертой степени над полем рациональных чисел. В теореме 4.2.1.1 доказано, что с точностью до изоморфизма существует 4 бесконечные серии и еще ровно 7 эллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $\mathbb{Q}((x))$.

Теорема (4.2.1.1)**.** *С точностью до отношения эквивалентности, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx)$ для $a, b \in \mathbb{Q}^*$, множество свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 4$, для которых разложение $\sqrt{f}$ в непрерывную дробь в поле $\mathbb{Q}((x))$ периодично, описывается*

[67] *Платонов В. П.*, *Петрунин М. М.* S-единицы и периодичность в квадратичных функциональных полях // Успехи математических наук. 2016. Т. 71, 5 (431). С. 181—182; *Петрунин М. М.* S-единицы и периодичность квадратного корня в гиперэллиптических полях // Докл. РАН. Матем., информ., проц. упр. 2017. Т. 474, № 2. С. 155—158; *Платонов В. П.*, *Петрунин М. М.* Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Труды Математического института имени В.А. Стеклова. 2018. Т. 302. С. 354—376.

[68] *Платонов В. П.*, *Жгун В. С.*, *Петрунин М. М.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов f над полями алгебраических чисел // Матем. сб. 2022. Т. 213, № 3. С. 139—170.

[69] *Платонов В. П.*, *Петрунин М. М.* О конечности числа периодических разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над полями алгебраических чисел // Докл. РАН. Матем., информ., проц. упр. 2020. Т. 495. С. 48—54; *Платонов В. П.*, *Жгун В. С.*, *Петрунин М. М.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над числовыми полями // Докл. РАН. Матем., информ., проц. упр. 2020. Т. 493. С. 32—37.

семью многочленами

$$\begin{gathered}(1-2x)(1+6x+32x^3),\\ (1-2x)(1+6x+96x^3),\\ (1-2x)(1+6x+32x^3/3),\\ 1-2x-2x^2-3x^3-3x^4/4,\\ (1+10x)(1-6x+32x^2-128x^3),\\ (27+144x+320x^2)(9-72x+400x^2)/243,\\ (1-10x)(1+14x+224x^2+5600x^3),\end{gathered}$$

и четырьмя семействами многочленов:

$$c_1x^4+1,\ -c_2^2x^4+2c_2x^2+1,\ (-c_3x^2+1)(3c_3x^2+1),\ -c_4^2x^4/3+2c_4x^2+1,$$

где параметр $c_1 \in \mathbb{Z}\setminus\{0\}$ *свободен от четвертых степеней, и параметры* $c_2, c_3, c_4 \in \mathbb{Z}\setminus\{0\}$ *свободны от квадратов.*

Отмеченные в разделе 3.3 особенности, возникающие для гиперэллиптических полей L, заданных многочленом f четной степени, существенно повлияли на доказательство теоремы 4.2.1.1 (по сравнению с теоремой 4.1.3.1), что отразилось не только в более сложных рассуждениях, но и существенно увеличило символьные компьютерные вычисления, необходимые для рассмотрения всех случаев.

В разделе 4.3 решена проблема классификации для эллиптических полей, заданных многочленом четвертой степени над квадратичными полями алгебраических чисел K и входящих в рациональную параметризацию модулярными кривыми. В теореме 4.3.1.1 для всех квадратичных числовых полей K приведено полное описание свободных от квадратов многочленов $f(x) \in K[x]$ степени 4 таких, что $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$, а эллиптическое поле $L = K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени m, $2 \le m \le 12$, $m \ne 11$, где множество S состоит из двух линейных сопряженных нормирований, определенных на поле L.

Теорема (4.3.1.1)**.** *Обозначим через* $\mathcal{U}_0^{(4)}$ *множество пар* $[f(x),\ K]$, *состоящих из числового поля* K *и свободного от квадратов многочлена* $f \in K[x]$ *с минимальным представлением степени* 4, *имеющего периодическое разложение* $\sqrt{f}$ *в непрерывную дробь в поле* $K((x))$, *с точностью до отношения эквивалентности, определенного допустимыми заменами многочлена* $f(x)$ *на* $a^2f(bx)$ *для* $a, b \in K^*$ *и заменой* $f(x)$ *на* $f^\sigma(x)$, *где* $\sigma \in Gal(K/\mathbb{Q})$. *Обозначим* *за* $\mathcal{U}^{(4)}$ *множество троек* $[m,\ f(x),\ K]$, *где* $[f(x),\ K] \in \mathcal{U}_0^{(4)}$ *и* m *— степень соответствующей фундаментальной* S*-единицы кольца* S*-целых элементов поля* $L = K(x)(\sqrt{f})$.

Множество троек $[m,\ f(x),\ K] \in \mathcal{U}^{(4)}$, *таких, что* $[K : \mathbb{Q}] \leq 2$, $m \leq 12$, $m \neq 11$, *описывается следующим образом*

$$
\begin{aligned}
&m = 3, \quad f_1 = -4x^4 - 4x^3 - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_2 = -12x^4 - 12x^3 - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_3 = -\frac{4x^4}{3} - \frac{4x^3}{3} - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_4 = -4x^4\left(3 - 2\sqrt{2}\right) - 4x^3\left(3 - 2\sqrt{2}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{2}),\\
&m = 3, \quad f_5 = -4x^4\left(7 - 4\sqrt{3}\right) - 4x^3\left(7 - 4\sqrt{3}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{3}),\\
&m = 3, \quad f_6 = -4x^4\left(5 - 2\sqrt{5}\right) - 4x^3\left(5 - 2\sqrt{5}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{5}),\\
&m = 3, \quad f_7 = -\frac{4x^4\left(5 - 2\sqrt{5}\right)}{5} - \frac{4x^3\left(5 - 2\sqrt{5}\right)}{5} - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{5}),\\
&m = 4, \quad f_8 = -\frac{3x^4}{4} - 3x^3 - 2x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 4, \quad f_9 = \frac{36 - 21\sqrt{3}}{2}x^4 + (15 - 9\sqrt{3})x^3 + (4 - 3\sqrt{3})x^2 - 2x + 1,\ K = \mathbb{Q}(\sqrt{3}),\\
&m = 5, \quad f_{10} = -5x^4 - 3x^3 - \frac{7x^2}{4} - x + 1, \quad K = \mathbb{Q},\\
&m = 6, \quad f_{11} = \frac{108x^4}{5} + \frac{324x^3}{25} + \frac{69x^2}{25} - \frac{6x}{5} + 1, \quad K = \mathbb{Q},\\
&m = 7, \quad f_{12} = -\frac{28x^4}{5} - \frac{84x^3}{25} + \frac{21x^2}{25} - \frac{2x}{5} + 1, \quad K = \mathbb{Q},\\
&m = 7, \quad f_{13} = \frac{(35 - 9\sqrt{-7})x^4}{2} + \frac{(33 - 3\sqrt{-7})x^3}{2} +\\
&\qquad\qquad + \frac{(41 + 5\sqrt{-7})x^2}{8} - \frac{(3 + \sqrt{-7})x}{2} + 1, \quad K = \mathbb{Q}(\sqrt{-7}),\\
&m = 7, \quad f_{14} = -\frac{x^4\left(32\sqrt{21} + 147\right)}{15} - \frac{x^3\left(621 + 136\sqrt{21}\right)}{75} -\\
&\qquad\qquad - \frac{x^2\left(304\sqrt{21} + 1469\right)}{300} - \frac{x\left(33 + 8\sqrt{21}\right)}{15} + 1, \quad K = \mathbb{Q}(\sqrt{21}).
\end{aligned}
$$

В главе 5 развита теория обобщенных функциональных непрерывных дробей, а также рассмотрено применение этой теории к проблеме поиска фундаментальных S-единиц в гиперэллиптических полях и к проблеме кручения в якобианах гиперэллиптических кривых. Теория функциональных непрерывных дробей, построенная в главе 3, оказывается менее эффективной для случаев, когда нормирование v_h, по которому строится непрерывная дробь, имеет степень выше 1. В частности, при $\deg h \geq 2$ не выполнено свойство наилучшего приближения у подходящих дробей.

В серии статей 2015-2024 гг. в соавторстве с В.П. Платоновым был развит теоретико-числовой подход к проблеме поиска и построения фундаментальных S-единиц гиперэллиптических полей, основанный на теории функциональных непрерывных дробей в поле формальных степенных рядов $K((x))$. В частности, было показано, что теория функциональных непрерывных дробей позволяет существенно продвинуться в поиске нетривиальных S-единиц и в изучении их строения в гиперэллиптических полях над произвольным числовым полем в качестве поля констант для множества S состоящего из двух нормирований. В главах 3 и 5 рассмотрены следующие случаи:

- множество S состоит из двух сопряженных (относительно гиперэллиптической инволюции) нормирований первой степени (глава 3);
- множество S состоит из единственного бесконечного нормирования (когда $v_\infty^- = v_\infty^+$) и конечного нормирования первой степени, не связанного с точками Вейерштрасса (нетрадиционный подход, основанный на рассмотрении непрерывных дробей обобщенного типа, см. в разделе 5.2);
- множество S состоит из двух несопряженных нормирований первой степени (см. раздел 5.3);
- множество S состоит из двух сопряженных нормирований второй степени (см. раздел 5.4).

В частности, из решения проблемы поиска и построения S-единиц в указанных случаях следует полное алгоритмическое решение проблемы кручения в якобианах гиперэллиптических кривых рода 2.

В разделе 5.2 теория функциональных непрерывных дробей обобщенного типа (h-дробей) была применена для традиционного случая, когда непрерывная дробь строится по нормированию v_h, $\deg h = 1$. В теореме 5.2.2.1 доказан критерий периодичности (квазипериодичности) функциональных непрерывных дробей обобщенного типа, дающий эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.2.3).

Теорема (5.2.2.1)**.** *Пусть K — поле характеристики, отличной от 2, и $h \in K[x]$, $\deg h = 1$. Пусть $f \in K[x]$ — свободный от квадратов многочлен нечетной степени $2g+1$, $g \geq 1$, и $S = \{v_h, v_\infty\}$. Пусть элемент $\alpha \in L = K(x)(\sqrt{f})$ имеет вид*

$$\alpha = \frac{\sqrt{f} + V}{U},$$

где $U = h^g$, $V = h^g \cdot \left[\sqrt{f} h^{-g}\right]_h$. Определим

$$R = \frac{f - V^2}{U \cdot h}, \quad a = [\alpha]_h, \quad W = aU - V, \quad T = \frac{f - W^2}{U \cdot h}, \quad \beta = \frac{\sqrt{f} + W}{T},$$
$$V_{-1} = V,\ U_{-1} = R,\ U_0 = U,\ V_0 = W,\ U_1 = T.$$

Существуют и однозначно определены эффективные дивизоры $D_R, D_U, D_T \in \mathrm{Div}(L)$ такие, что главные дивизоры многочленов $R, U, T \in K[x]$ и функций $\sqrt{f} - V, \sqrt{f} - W \in L$ имеют вид

$$\begin{aligned}
(R) &= D_R + \iota D_R + r\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(R) = r,\\
(U) &= D_U + \iota D_U + s\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(U) = s,\\
(T) &= D_T + \iota D_T + t\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(T) = t,\\
\left(\sqrt{f} - V\right) &= D_R + (r + s + 1)v_h + \iota D_U - (2g+1) \cdot \infty,\\
\left(\sqrt{f} - W\right) &= D_U + (s + t + 1)v_h + \iota D_T - (2g+1) \cdot \infty;
\end{aligned}$$

Положим

$$D_{-1} = D_R,\ D_0 = D_U,\ D_1 = D_T,\ s_{-1} = r,\ s_0 = s,\ s_1 = t.$$

Пусть справедливы построения

$$\begin{gathered}
\alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad f - V_j^2 = U_j \cdot h \cdot U_{j+1},\\
a_{j+1} = [\alpha_{j+1}]_h, \quad V_{j+1} = a_{j+1} U_{j+1} - V_j,\\
s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h(\alpha_{j+1}),\\
(U_j) = D_j + \iota D_j + s_j\big(v_h + \iota v_h\big) - 2g \cdot \infty,\\
\left(V_j - \sqrt{f}\right) = D_j + (s_j + s_{j+1} + 1)v_h + \iota D_{j+1} - (2g+1) \cdot \infty.
\end{gathered}$$

Тогда следующие условия эквивалентны

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = 0$;*

2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = ch^g$ для некоторой постоянной $c \in K^*$;*

3. *класс дивизора $\big(v_h - \infty\big)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*

4. *класс дивизора $\big(v_h - \iota v_h\big)$ имеет конечный порядок m_h в группе классов дивизоров $\Delta^\circ(L)$;*

5. *непрерывная дробь элемента α обобщенного типа квазипериодическая с длиной квазипериода n.*

Если существуют $n, m, m_h \in \mathbb{N}$, указанные в эквивалентных условиях 1.-5., то

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если в пункте 2. постоянная $c = 1$, либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*

- *справедливы соотношения*

$$m = \sum_{j=0}^{n-1}(2s_j + 1), \quad \text{где } s_j = -v_h\left(\alpha_j\right) = -v_h\left(a_j\right) = v_h\left(U_j\right), \ j \in \mathbb{N}_0;$$

- *для минимального $t \in \mathbb{N}$, такого, что $D_{2t} = 0$, справедливы соотношения $m_h = t + \sum_{j=0}^{2t-1} s_j$;*

- *если m четно, то $m_h = m/2$, если m нечетно, то $m_h = m$.*

В разделе 5.3 построена теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований. Особенность таких обобщенных непрерывных дробей в том, что они сходятся к элементу как по первому, так и по второму линейному нормированию (см. предложение 5.3.3.3). В теореме 5.3.4.1 для функциональных непрерывных дробей обобщенного типа, построенным по двум несопряженным линейным нормированиям, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

Теорема (5.3.4.1)**.** *Пусть K — поле характеристики, отличной от 2. Пусть свободный от квадратов многочлен $f \in K[x]$, такой, что линейные нормирования v_x и v_h поля $K(x)$ имеют по два неэквивалентных продолжения $v_x^- \neq v_x^+$ и $v_h^- \neq v_h^+$ на поле $L = K(x)(\sqrt{f})$. Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный* *дивизор, что* $r_0 = v_x^-(D_0) = g$ *или* $s_0 = v_h^-(D_0) = g$. *Пусть* $(U_{-1}xh, V_{-1})$ — *представление Мамфорда дивизора* $D_0 + (x)_\circ^- + (h)_\circ^-$ *и для* $j \in \mathbb{N}_0$ *справедливы построения*

$$U_j = T_j x^{s_j - r_j} h^{r_j - s_j}, \quad V_j = e_j T_j x^{-r_j} h^{-s_j} - V_{j-1},$$
$$f - V_j^2 = U_j x h T_{j+1}, \quad \deg U_j \le g, \quad \deg T_{j+1} \le g, \quad \deg V_j \le g+1,$$
$$(U_{j-1})_{[g]} = D_j + \iota D_j - g(\infty^- + \infty^+),$$
$$(T_j)_{[g]} = E_j + \iota E_j - g(\infty^- + \infty^+),$$
$$D_j = \operatorname{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]},\ (U_{j-1})_{[g]}\right),$$
$$E_j = \operatorname{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]},\ (T_j)_{[g]}\right),$$
$$\left(V_{j-1} - \sqrt{f}\right)_{[g+1]} = D_j + (x)_\circ^- + (h)_\circ^- + E_j,$$
$$D_{j+1} = \iota E_j - r_j((x)_\circ^+ - (h)_\circ^-) - s_j((h)_\circ^+ - (x)_\circ^-),$$

где $r_j = v_x(T_j)$, $s_j = v_h(T_j)$, $U_j, T_j, V_j, e_j \in K[x]$, $U_j \ne 0$, $T_j \ne 0$, $e_j \ne 0$, *дивизоры* $D_j, E_j \in \operatorname{Div}(L)$ *приведенные.*

Тогда следующие условия эквивалентны

1. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $D_n = D_0$;

2. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $U_{n-1} = cU_{-1}$ *для некоторой постоянной* $c \in K^*$;

3. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $V_{n-1} = V_{-1}$ *и* $T_n = c^{-1}T_0$ *для некоторой постоянной* $c \in K^*$;

4. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $E_n = E_0$;

5. *классы эквивалентных дивизоров* $(h)_\circ^- - (x)_\circ^+ \sim (x)_\circ^- - (h)_\circ^+$ *имеют конечный порядок* m *в группе классов дивизоров* $\Delta^\circ(L)$;

6. *непрерывные дроби обобщенного типа элементов* $\sqrt{f}/x^g$ *и* $\sqrt{f}/h^g$, *квазипериодические с длиной квазипериода* n;

7. *в гиперэллиптическом поле* L *существует фундаментальная* S*-единица степени* m, *где* $S = \{v_x^-, v_h^+\}$;

8. *для некоторого* $b \in K^*$ *уравнение*

$$\mu_1^2 - \mu_2^2 f = b x^m h^m, \qquad \max\bigl(2\deg\mu_1,\ 2\deg\mu_2 + \deg f\bigr) = 2m,$$

имеет решение $\mu_1, \mu_2 \in K[x]$ такое, что $v_x(\mu_2) = v_h(\mu_2) = 0$, $\mu_2 \neq 0$.

Если существуют $n, m \in \mathbb{N}$, указанные в эквивалентных условиях 1.-6., то они связаны соотношением

$$m = \sum_{j=0}^{n-1} (1 + r_j + s_j), \quad \text{где для } j \in \mathbb{N}_0$$

$$r_j = -v_x^-(\alpha_j) = -v_x(a_j) = v_x^-(E_j) = v_x(T_j) = v_h(U_j) = v_h^-(D_{j+1}),$$
$$s_j = -v_h^-(\alpha_j) = -v_h(a_j) = v_h^-(E_j) = v_h(T_j) = v_x(U_j) = v_x^-(D_{j+1}).$$

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.3.6 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух несопряженных линейных нормирований.

В разделе 5.3 построена теория непрерывных h-дробей — функциональных непрерывных дробей обобщенного типа, построенных по нормированию v_h, где $\deg h = 2$. Ранее теория непрерывных дробей не применялась для поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях, когда в множестве S содержалось нормирование второй степени. В теореме 5.4.4.1 для непрерывных h-дробей, $\deg h = 2$, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

Теорема (5.4.4.1)**.** *Пусть $h \in K[x]$ неприводимый многочлен второй степени. Пусть свободный от квадратов многочлен $f \in K[x]$, $\deg f \geq 5$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $s_0 = v_h^-(D_0) = [g/2]$. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $D_0 + (h)_\circ^-$ и для $j \in \mathbb{N}_0$ справедливы построения*

$$U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}, \quad \alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad a_{j+1} = [\alpha_{j+1}]_h^-,$$
$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h^-(\alpha_{j+1}), \quad V_{j+1} = a_{j+1}U_{j+1} - V_j,$$
$$D_j = (U_j)_\circ^- - s_j(h)_\circ^+ + s_j(h)_\circ^-, \quad \left(V_j - \sqrt{f}\right)_\circ = D_j + (h)_\circ^- + (U_{j+1})_\circ^+,$$
$$(U_{j+1})_\circ^- + (U_j)_\circ + (h)_\circ^- = \left(V_j + \sqrt{f}\right)_\circ + (U_j)_\circ^- + (s_j + 1)\big((h)_\circ^- - (h)_\circ^+\big).$$

Тогда следующие условия эквиваленты

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = D_0$;*

2. найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = cU_0$ для некоторой постоянной $c \in K^*$;

3. класс дивизора $\left((h)_\circ^- - \infty^- - \infty^+\right)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;

4. класс дивизора $\left((h)_\circ^- - (h)_\circ^+\right)$ в группе классов дивизоров $\Delta^\circ(L)$ имеет конечный порядок m_h;

5. для элемента α,

$$\alpha = \alpha_0 = \frac{\sqrt{f} - V_0}{U_0} + \left[\frac{\sqrt{f} + V_0}{U_0}\right]_h^-,$$

непрерывная дробь обобщенного типа квазипериодическая с длиной квазипериода n.

Если существуют $n, m, m_h \in \mathbb{N}$, указанные в эквивалентных условиях 1.-5., то

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если постоянная $c = 1$ из пункта 2., либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*
- *справедливы соотношения*

$$m = \sum_{j=0}^{n-1}(2s_j+1),\ \text{где}\ s_j = -v_h^-\left(\alpha_j\right) = -v_h\left(a_j\right) = v_h^-\left(D_j\right) = v_h\left(U_j\right),\ j \in \mathbb{N}_0;$$

- *для минимального $t \in \mathbb{N}$, такого, что $D_{2t} = D_0$, справедливы соотношения $m_h = t + \sum_{j=0}^{2t-1} s_j$;*
- *либо $m_h = m/2$, если m четно, либо $m_h = m$, если m нечетно.*

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.4.7 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух сопряженных нормирований второй степени.

Разработанные в диссертации теоретические методы и подходы подкреплены соответствующими компьютерными вычислениями. В частности, получены быстрые алгоритмы поиска и построения фундаментальных S-единиц с помощью метода функциональных непрерывных дробей и функциональных непрерывных дробей обобщенного типа. С применением больших символьных компьютерных вычислений построены многочисленные примеры и контрпримеры, подтверждающие основные результаты диссертации.

Заключение

В диссертационной работе представлено решение актуальных проблем в области алгебраической теории чисел и арифметической геометрии. Нами изучено строение и свойства гиперэллиптических кривых и гиперэллиптических полей, а также связанных с ними теоретико-числовых, алгебраических и геометрических объектов таких, как функциональные непрерывные дроби, функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. Отдельное внимание уделено изучению связей и зависимостей между этими объектами и их ключевыми свойствами. Приведенные объекты рассматривались как над произвольными полями K характеристики, отличной от 2, так и в отдельных случаях над полем рациональных чисел $\mathbb{Q}$ или над полями алгебраических чисел, являющимися конечными расширениями поля $\mathbb{Q}$.

В ходе исследования были использованы как традиционные методы алгебраической теории чисел, классических направлений алгебры и арифметической геометрии, так и возникшие недавно (в том числе в работах автора) новые арифметические методы из теории функциональных непрерывных дробей, теории единиц колец целых или S-целых элементов гиперэллиптических полей, теории дивизоров гиперэллиптических кривых. Ряд результатов получен с использованием систем компьютерной алгебры и символьных компьютерных вычислений.

Основные результаты диссертационной работы заключаются в следующем:

1. найдены точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных

чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. разработана теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

Результаты диссертации могут быть использованы в таких теоретических разделах математики, как алгебраическая теория чисел, алгебраическая геометрия, арифметическая геометрия, а также в области защиты информации и в прикладных разделах вычислительной математики.

Благодарности

Автор выражает глубокую благодарность научному консультанту, академику РАН, профессору Владимиру Петровичу Платонову за переданный неоценимый опыт в выборе задач, искусство ведения математических исследований и подготовки публикаций, постоянное внимание к работе, неугасимый математический энтузиазм и заразительный преданный интерес к науке.

Автор выражает благодарность коллективу отдела теоретической и прикладной алгебры и теории чисел НИИСИ РАН за замечательную научную и рабочую атмосферу.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова по специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика»
и входящих в базы цитирования RSCI, Scopus, Web of Science

1. *Платонов В. П., Федоров Г. В.* Непрерывные дроби в гиперэллиптических полях со сколь угодно большой длиной периода // Докл. РАН. Матем., информ., проц. упр. — 2024. — Т. 516. — С. 59—64. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.863 (2023); *Platonov V. P., Fedorov G. V.* Continued fractions in hyperelliptic fields with an arbitrarily large period length // Dokl. Math. — 2024. — Vol. 109, no. 2. — P. 147—151. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.5 (2023), SJR 0.458(2023). Вклад авторов равноценный и неделимый (50%/50%). 0,375 печ. л.

2. *Федоров Г. В.* О последовательностях многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь // Вестн. Моск. ун-та. Сер. 1 Математика. Механика. — 2024. — № 2. — С. 25—30. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.396 (2023); *Fedorov G. V.* On sequences of polynomials f with periodic expansion of $\sqrt{f}$ into continued fractions // Moscow University Mathematics Bulletin. — 2024. — no. 2. — P. 98–102. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.2 (2023), SJR 0.344 (2023). 0,375 печ. л.

3. *Федоров Г. В.* Об оценках длин периодов функциональных непрерывных дробей над алгебраическими числовыми полями // Чебышевский сб. — 2023. — Т. 24, № 3. — С. 162—189. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.498 (2021), SJR 0.296 (2023). 1,75 печ. л.

4. *Федоров Г. В.* Непрерывные дроби и проблема классификации эллиптических полей над квадратичными полями констант // Матем. заметки. — 2023. — Т. 114, № 6. — С. 873—893. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.796 (2023); *Fedorov G. V.* Continued Fractions and the Classification Problem for Elliptic Fields Over Quadratic Fields of Constants // Math. Notes. — 2023. — Vol. 114, no. 6. — P. 1203–1219. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2023), SJR 0.418 (2023). 1,3125 печ. л.

5. *Федоров Г. В.* О проблеме описания элементов эллиптических полей с периодическим разложением в непрерывную дробь над квадратичными полями констант // Докл. РАН. Матем., информ., проц. упр. — 2022. — Т.

505. — С. 56—62. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: 0.943(2022); *Fedorov G. V.* On the problem of describing elements of elliptic fields with a periodic expansion into a continued fraction over quadratic fields // Dokl. Math. — 2022. — Vol. 106, no. 1. — P. 259–264. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2022), SJR 0.444 (2022). 0,4375 печ. л.

6. *Platonov V. P.*, *Fedorov G. V.* Periodicity Criterion for Continued Fractions of Key Elements in Hyperelliptic Fields // Dokl. Math. — 2022. — С. 262—269. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2022), SJR 0.444 (2022). The contribution of the authors is equal and indivisible (50%/50%). 0,5 печ. л.

7. *Федоров Г. В.* О фундаментальных S-единицах и непрерывных дробях, построенных в гиперэллиптических полях по двум линейным нормированиям // Докл. РАН. Матем., информ., проц. упр. — 2021. — Т. 498. — С. 65—70. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.556 (2021); *Fedorov G. V.* On fundamental S-units and continued fractions constructed in hyperelliptic fields using two linear valuations // Dokl. Math. — 2021. — Vol. 103, no. 3. — P. 151–156. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.486 (2021), SJR 0.385 (2021). 0,375 печ. л.

8. *Платонов В. П.*, *Федоров Г. В.* О проблеме классификации многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в гиперэллиптических полях // Изв. РАН. Сер. матем. — 2021. — Т. 85, № 5. — С. 152—189. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.804 (2021); *Platonov V. P., Fedorov G. V.* On the classification problem for polynomials f with a periodic continued fraction expansion of $\sqrt{f}$ in hyperelliptic fields // Izv. Math. — 2021. — Vol. 85, no. 5. — P. 972–1007. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.978 (2021), SJR 0.726 (2021). Вклад авторов равноценный и неделимый (50%/50%). 2,375 печ. л.

9. *Федоров Г. В.* О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков // Чебышевский сб. — 2020. — Т. 21, № 1. — С. 322—340. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.450 (2020), SJR 0.273 (2020). 1,1875 печ. л.

10. *Федоров Г. В.* О длине периода функциональной непрерывной дроби над числовым полем // Докл. РАН. Матем., информ., проц. упр. — 2020. — Т. 495. — С. 78—81. — Журнал индексируется в РИНЦ, Scopus, WoS. Им-

пакт фактор: РИНЦ 0.904 (2019); *Fedorov G. V.* On the period length of a functional continued fraction over a number field // Dokl. Math. — 2020. — Vol. 102, no. 3. — P. 513–517. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.619 (2020), SJR 0.765 (2020). 0,25 печ. л.

11. *Федоров Г. В.* Об S-единицах для нормирований второй степени в гиперэллиптических полях // Изв. РАН. Сер. матем. — 2020. — Т. 84, № 2. — С. 197—242. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.958 (2020); *Fedorov G. V.* On S-units for valuations of the second degree in hyperelliptic fields // Izv. Math. — 2020. — Vol. 84, no. 2. — P. 392–435. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 1.189 (2020), SJR 1.057 (2020). 2,875 печ. л.

12. *Платонов В. П.*, *Федоров Г. В.* О проблеме классификации периодических непрерывных дробей в гиперэллиптических полях // Успехи математических наук. — 2020. — Т. 75, 4(454). — С. 211—212. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 1.250 (2020); *Platonov V. P., Fedorov G. V.* On the problem of classification of periodic continued fractions in hyperelliptic fields // Russian Math. Surveys. — 2020. — Vol. 75, no. 4. — P. 785–787. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 1.909 (2020), SJR 0.891 (2020). Вклад авторов равноценный и неделимый (50%/50%). 0,125 печ. л.

13. *Федоров Г. В.* Об ограниченности длин периодов непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел // Чебышевский сб. — 2019. — Т. 20, № 4. — С. 357—370. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.599 (2019), SJR 0.236 (2019). 0,875 печ. л.

14. *Платонов В. П.*, *Федоров Г. В.* Критерий периодичности непрерывных дробей ключевых элементов гиперэллиптических полей // Чебышевский сб. — 2019. — Т. 20, № 1. — С. 248—260. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.599 (2019), SJR 0.236 (2019). Вклад авторов равноценный и неделимый (50%/50%). 0,75 печ. л.

15. *Платонов В. П.*, *Федоров Г. В.* S-единицы для линейных нормирований и периодичность непрерывных дробей обобщенного типа в гиперэллиптических полях // Докл. РАН. — 2019. — Т. 486, № 3. — С. 280—286. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.904 (2019); *Platonov V. P., Fedorov G. V.* On S-units for linear valuations and the periodicity of continued fractions of generalized type in hyperelliptic fields // Dokl. Math. — 2019. — Vol. 99, no. 3. — P. 277–281. — The journal is indexed in

RSCI, Scopus, WoS. Impact factor: JIF 0.548 (2019), SJR 0.607 (2019). Вклад авторов равноценный и неделимый (50%/50%). 0,4375 печ. л.

16. *Федоров Г. В.* Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях // Чебышевский сб. — 2018. — Т. 19, № 3. — С. 282—297. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.572 (2018), SJR 0.187 (2018). 1,0 печ. л.

17. *Платонов В. П., Федоров Г. В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. — 2018. — Т. 209, № 4. — С. 54—94. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 1.165 (2018); *Platonov V. P., Fedorov G. V.* On the problem of periodicity of continued fractions in hyperelliptic fields // Sb. Math. — 2018. — Vol. 209, no. 4. — P. 519–559. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: SJR 1.158(2020), JCR 1.274(2021). Вклад авторов равноценный и неделимый (50%/50%). 2,5625 печ. л.

18. *Платонов В. П., Федоров Г. В.* О периодичности непрерывных дробей в эллиптических полях // Докл. РАН. — 2017. — Т. 475, № 2. — С. 133—136. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.869 (2017); *Platonov V. P., Fedorov G. V.* On the periodicity of continued fractions in elliptic fields // Dokl. Math. — 2017. — Vol. 96, no. 1. — P. 332–335. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.534 (2017), SJR 0.427 (2017). Вклад авторов равноценный и неделимый (50%/50%). 0,25 печ. л.

19. *Платонов В. П., Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях // Докл. РАН. — 2017. — Т. 474, № 5. — С. 540—544. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.869 (2017); *Platonov V. P., Fedorov G. V.* On the periodicity of continued fractions in hyperelliptic fields // Dokl. Math. — 2017. — Vol. 95, no. 3. — P. 254–258. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.534 (2017), SJR 0.427 (2017). Вклад авторов равноценный и неделимый (50%/50%). 0,3125 печ. л.

20. *Платонов В. П., Федоров Г. В.* S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // Докл. РАН. — 2015. — Т. 465, № 5. — С. 537—541. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.831 (2015); *Platonov V. P., Fedorov G. V.* S-units and periodicity of continued fractions in hyperelliptic fields // Dokl. Math. — 2015. — Vol. 92, no. 3. — P. 752–756. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.445 (2015), SJR 0.358 (2015). Вклад авторов равноценный и неделимый (50%/50%). 0,3125 печ. л.

Федоров Глеб Владимирович

Теория функциональных непрерывных дробей
в гиперэллиптических полях и ее приложения

Автореф. дис. на соискание ученой степени д-ра физ.-мат. наук

Подписано в печать «23» октября 2024 г.
Формат 60×90/16. Объем: усл. печ. л. 2.0.
Тираж 100 экз. Заказ №   .
Отдел полиграфии Научной библиотеки МГУ имени М.В. Ломоносова
119192 Москва, Ломоносовский проспект, д. 27.