ОТЗЫВ официального оппонента

на диссертацию на соискание ученой степени
доктора физико-математических наук
Федорова Глеба Владимировича
на тему: «Теория функциональных непрерывных дробей в гиперэллиптических полях и ее приложения»
по специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика»

Основное направление проведённых исследований — теория функциональных непрерывных дробей. На основании доказанных в диссертационной работе фундаментальных результатов предложен новый подход к изучению арифметических свойств гиперэллиптических кривых и гиперэллиптических полей, а также связанных с ними теоретико-числовых, алгебраических и геометрических объектов. К последним относятся функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения.

Диссертация состоит из аннотации, пяти глав и заключения.

Первая глава диссертации представляет собой введение в круг рассматриваемых вопросов. В ней даётся общее описание работы, описываются методы исследования, излагаются решаемые задачи. Кроме того, в первой главе приводится история рассматриваемых вопросов, их актуальность и формулируются основные результаты диссертации.

Во второй главе (Основы теории алгебраических кривых) даётся краткое изложение необходимых базовых понятий и теорем, которые в дальнейшем используются в диссертации. Для этого, как и в остальной части диссертации, используется язык алгебры и алгебраической теории чисел. В частности здесь излагаются необходимые сведения о гиперэллиптических кривых, S-единицах, и дивизорах на произвольных алгебраических кривых.

Глава 3 посвящена функциональным непрерывным дробям. Здесь строится

подробная теория, которая, с одной стороны, схожа с теорией классических числовых непрерывных дробей, с другой стороны, с технической точки зрения оказывается существенно более сложной. Кроме того выясняется, что функциональные непрерывные дроби обладают некоторыми неожиданными особенностями, которые принципиально отличают их от числовых непрерывных дробей. В начале исследуется вопрос построения функциональных непрерывных дробей в различных полях формальных степенных рядов. Затем изучаются свойства наилучших приближений, их связь с уравнениями типа Пелля, с нетривиальными единицами и S-единицами гиперэллиптического поля. Отдельное внимание уделено свойствам периодов и квазипериодов (симметрия, оценки на длины предпериодов, квазипериодов и периодов). Все результаты иллюстрируются примерами и контрпримерами. Оказывается, что теория функциональных непрерывных дробей даёт эффективные арифметические инструменты для поиска и построения фундаментальных S-единиц гиперэллиптического поля и для решения проблемы кручения в якобиане соответствующей гиперэллиптической кривой.

Отдельный интерес представляет собой раздел 3.3, в котором получены оценки сверху на длины периодов и квазипериодов функциональных непрерывных дробей произвольных элементов гиперэллиптического поля. Там же исследуются и другие свойства периодов и квазипериодов. Некоторые факты весьма неожиданны, например, длина квазипериода непрерывной дроби квадратичной иррациональности гиперэллиптического функционального поля может быть значительно больше порядка подгруппы кручения якобиана соответствующей гиперэллиптической кривой.

Четвёртая глава диссертации посвящена проблеме классификации эллиптических полей вида $K(x)(\sqrt{f})$ по признаку периодичности непрерывных дробей, построенных в поле $K((x))$ для ключевых элементов вида $\sqrt{f}/x^s$, где K — алгебраическое расширение поля $\mathbb{Q}$, f — свободный от квадратов многочлен и $s \in \mathbb{Z}$. Проблема сводится к нахождению полей, в которых элемент $\sqrt{f}$ обладает периодическим разложением в непрерывную дробь. Эта задача в диссертации полностью решена для случаев, когда $\deg f = 3$ и $K = \mathbb{Q}$, $\deg f = 4$ и $K = \mathbb{Q}$ или K — квадратичное расширение поля рациональных чисел (с некоторыми дополнительными

техническими условиями). На основе полученных результатов автором выдвигаются гипотезы, показывающие направления для дальнейшего развития исследований.

В пятой главе диссертации построена новая теория обобщенных функциональных непрерывных дробей. В частности, 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. Найден эффективный алгоритм поиска и построения фундаментальных S-единиц в гиперэллиптических полях для множеств S более общего вида по сравнению с ранее известными подходами. Полученные результаты позволяют существенно продвинуться в проблеме кручения в якобианах гиперэллиптических кривых для соответствующих точкам кручения эффективных дивизоров степени два и выше.

В диссертации Г. В. Федорова разработаны теоретические положения, совокупность которых можно квалифицировать как новое крупное достижение в развитии теории чисел. Результаты диссертации важны сами по себе и могут быть использованы в дальнейшем в теории кодирования, в алгоритмической теории чисел, в эллиптической и гиперэллиптической криптографии.

Содержание диссертации соответствует специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика», а именно таким направлениям как арифметическая геометрия и алгебраическая теория чисел. Диссертация соответствует также критериям, определенным пп. 2.1–2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М. В. Ломоносова, а также оформлена согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М. В. Ломоносова.

Соискатель, Федоров Глеб Владимирович, несомненно заслуживает присуждения ученой степени доктора физико-математических наук по специальности 1.1.5 «Математическая логика, алгебра, теория чисел и дискретная математика».

Официальный оппонент:

Профессор департамента больших данных и информационного поиска Факультета компьютерных наук, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», д. ф.-м. н.

УСТИНОВ Алексей Владимирович

16 декабря 2024 года

Контактные данные:

e-mail:

Телефон:

Специальность, по которой официальным оппонентом защищена диссертация: 01.01.06 «Математическая логика, алгебра и теория чисел»

Адрес места работы: 109028, г. Москва, Покровский бульвар, д. 11,
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики»

Подпись А. В. Устинова удостоверяю