ОТЗЫВ официального оппонента
о диссертации 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»

Актуальность избранной темы

Вопросы, исследованные в диссертационной работе, относятся к трудным задачам. Это – проблема существования и поиска фундаментальных единиц в гиперэллиптических полях, проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел, проблему периодичности разложения в функциональную непрерывную дробь элементов гиперэллиптических полей. Эти проблемы тесно связаны с важными прикладными задачами, например, с защитой информации.

В этих направлениях работают многие исследователи в России и за рубежом, опубликовано много работ. Важно отметить роль школы академика В.П. Платонова, работы представителей которой внесли заметный вклад в развитие этого направления.

Оценка полученных результатов, их достоверность и новизна

В диссертационной работе Г.В. Федорова построена новая теория функциональных непрерывных дробей обобщенного типа. Основные

результаты, относящиеся к этой теме, приведены в главе 6 и заключаются в следующем:

1. 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;

2. 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;

3. 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.

Кратко опишем основную ценность полученных результатов по этой теме. Пусть K — некоторое совершенное поле, которое мы рассматриваем в качестве поля констант. Рассмотрим вложение Альбанезе φ гиперэллиптической кривой C в ее якобиево многообразие J (якобиан), при котором точка $P \in C$ переходит в класс дивизора $[P - \mathcal{O}]$, где $\mathcal{O}$ — некоторая фиксированная точка на кривой C. Тогда точки якобиана J, которые являются образами точек $P \in C$ при вложении φ, называются рациональными точками в якобиане J. Множество K-точек якобиана J является конечно порожденной абелевой группой (теорема Мордела-Вейля), изоморфной $\mathbb{Z}^r \times J_{tors}(K)$, где $J_{tors}(K)$ — подгруппа K-точек конечного порядка (подгруппа кручения) — один из основных объектов, к которому относятся исследования в представленной

диссертации. В алгебраической теории чисел и в арифметической геометрии важное место занимают следующие две фундаментальные проблемы:

1. проблема описания возможных подгрупп $J_{tors}(K)$для различных гиперэллиптических кривых, определённых над фиксированным полем K и имеющих род g;

2. проблема описания гиперэллиптических кривых, определенных над фиксированным полем K и имеющих род g, реализующих в качестве $J_{tors}(K)$ одну из групп предыдущей проблемы.

Необходимо отметить, что кроме эллиптического случая, результаты в этом направлении на данный момент в основном ограничиваются частными случаями, а также связаны с высокопроизводительными компьютерными вычислениями. Эти проблемы имеют большой интерес и большую историю, поскольку они связаны со многими приложениями, в том числе в криптографии.

Еще по классическим работам Н. Абеля, П. Дирихле, Е. Артина известно (используя современный математический язык и соответствующие обозначения), что наличие рациональной точки кручения (точки конечного порядка) в якобиане гиперэллиптической кривой, заданной уравнением C : $y^2 = f(x)$, связано с периодичностью функциональной непрерывной дроби для элемента $\sqrt{f(x)}$, разложенного в поле $K((1/x))$. В дальнейшем развитие этого подхода в работах многих математиков позволило существенным образом продвинуться в изучении арифметических свойств якобианов гиперэллиптических кривых, а также сформулировать важные для прикладных областей (криптографии) алгоритмы (например, алгоритм Кантора сложения дивизоров, 1987 г., и его обобщения).

Если кривая C имеет род g, то точки на якобиане можно представить в виде классов дивизоров $[D] = [\sum_{i=1}^{g} P_i - gO]$, где P_i — необязательно

различные точки кривой C. Если $P_2 = \ldots = P_g = O$, то $[D] = [P_1 - O]$ — рациональная точка якобиана J. При $g > 1$ якобиан не ограничивается рациональными точками, поэтому возникает естественный вопрос: можно ли связать конечность порядка нерациональной точки $[D]$ якобиана J с периодичностью функциональных дробей некоторых элементов соответствующего гиперэллиптического поля (по аналогии, как это выше указано для рациональных точек).

Аппарат обычных функциональных непрерывных дробей оказывается недостаточным. Поэтому в диссертационной работе Г.В. Федорова было впервые предложено использовать функциональные непрерывные дроби обобщенного типа, когда в числителе вместо 1 может стоять некоторое регулярное выражение — обычно это многочлены определенного вида, связанные с классом дивизора $[D]$ (являющегося точкой конечного порядка в якобиане J или потенциальной точкой конечного порядка). Этот подход позволил ответить на поставленный вопрос, сформулировать теорию, в которой свойство периодичности связано с кручением более общего вида (нерациональным), а также открыл новую область исследований, поскольку в теории функциональных непрерывных дробей обобщенного типа можно по аналогии ставить те же задачи и проблемы, которые изучались для числовых цепных дробей и для обыкновенных функциональных непрерывных дробей. Важно, что эти проблемы будут не просто аналогом в “какой-то искусственной теории”, а будут связаны с такими важными и глубокими темами, как кручение в якобианах гиперэллиптических кривых, проблемой разрешимости диофантовых уравнений в кольце многочленов, теорией аппроксимации и приближения, поиском фундаментальных единиц и S-единиц соответственно в кольцах целых и S-целых элементов функциональных полей.

II. Другой важной теме посвящена глава 5 диссертационной работы. В ней решается проблема классификации эллиптических кривых по принципу

периодичности функциональных непрерывных дробей для ключевых элементов соответствующих эллиптических полей $L = K(x)(\sqrt{f(x)})$. Эта проблема была сформулирована академиком В.П. Платоновым, но долго не поддавалась решению. Даже нахождение частных примеров периодических элементов специального вида $\sqrt{f}/x^s$, для $s \in \mathrm{N}$ — являлось сложной задачей, требующей новых идей и больших компьютерных вычислений. Стоит отметить, что в проблеме классификации можно рассматривать разложение элементов в функциональную непрерывную дробь в различных полях формальных степенных рядов. При рассмотрении поля формальных степенных рядов $K((1/x))$, мы приходим к классической постановке (классическим функциональным непрерывным дробям), которая идет от Абеля, Чебышева и Артина, и с тех пор изучалась огромным количеством авторов. Если же рассмотреть поле формальных степенных рядов $K((x))$, то в проблеме классификации наиболее интересным является случай $s = 0$, то есть большой интерес представляет описание эллиптических полей $L = K(x)(\sqrt{f(x)})$, в которых элементы $\sqrt{f(x)}$ имеют периодическое разложение в непрерывную дробь, построенную в поле формальных степенных рядов $K((x))$. Этот интерес подчеркивается гипотезой, утверждающей, что при $s < 0$ не существует $L = K(x)(\sqrt{f(x)})$, для которых элемент $\sqrt{f}/x^s$ имеет периодическое разложение в в непрерывную дробь, построенную в поле $K((x))$. В 2018 году (аннотация этого результата появилась в 2017 году в короткой статье в ДАН) В.П. Платонов и Г.В. Федоров решили проблему классификации для кубических эллиптических полей над полем рациональных чисел (то есть, когда $f(x)$ — кубический многочлен, определенный над полем $K = \mathrm{Q}$) и доказали в этом случае приведенную гипотезу. А именно, было получено полное описание эллиптических полей, в которых элементы вида $\sqrt{f}/x^s$ имеют периодическое разложение в

функциональную непрерывную дробь. Оказалось, что при $s = 3$ или $s = 0$ за исключением тривиального семейства, существует только три попарно неизоморфных эллиптических поля L, обладающих указанным свойством периодичности ключевых элементов. В дальнейшем проблема классификации была решена для эллиптических полей, заданных многочленом $f(x)$ четвертой степени над полем Q (что полностью завершило проблему классификации эллиптических кривых над Q), а также совместно с коллегами из научной школы В.П. Платонова были получены существенные продвижения в проблеме классификации эллиптических полей над различными числовыми полями. В частности, для квадратичных числовых полей получено решение проблемы классификации для эллиптических полей, входящих в рациональную параметризацию модулярными кривыми. По этой теме в диссертационной работе Г.В. Федорова получены следующие важные результаты: 1. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем 3 рациональных чисел; 2. 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. III. Наконец, важное место в диссертационной работе занимает глава 3, посвященная изучению функциональных непрерывных дробей, построенных в различных полях степенных рядов, а также изучению связи функциональных непрерывных дробей с другими математическими объектами. В этой теме особенно можно выделить результаты, связанные с оценками длин периодов и квазипериодов функциональных непрерывных дробей. Хорошо известно, что даже для числовых цепных дробей вопросы об оценках длин периодов, а также о распределении длин периодов, являются сложными и актуальными. В функциональном случае эти вопросы также имеют большой интерес,

который подкреплен актуальными исследованиями. В диссертационной работе найдены точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля L, определенного над полем алгебраических чисел K. Особенностью полученных оценок является то, что они справедливы для произвольных элементов $\alpha \in L$, и существенным образом зависят от поля K, рода g и дискриминанта $D = D(\alpha)$. В частности, из найденных оценок получается неожиданный результат о том, что в любом гиперэллиптическом поле, определенным многочленом $f(x)$ четной степени над числовым полем K, и обладающим нетривиальной фундаментальной единицей, для любого числа $N \in \mathrm{N}$ найдется элемент α, длина периода которого не меньше N.

Все результаты диссертации строго доказаны и прошли надлежащую апробацию. Автореферат точно отражает содержание диссертации.

К замечаниям можно отнести некоторую краткость изложения, возможно связанную с желанием описать всё многообразие полученных важных результатов. При этом объём работы и так составляет 326 страниц. Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 1.1.5 «Математическая логика, алгебра, теория чисел и дискретная математика», а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, а также диссертация 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.

Таким образом, соискатель Фёдоров Глеб Владимирович заслуживает присуждения ученой степени доктора физико-математических наук по специальности 1.1.5 «Математическая логика, алгебра, теория чисел и дискретная математика».

Официальный оппонент:
Доктор физико-математических наук,
профессор кафедры математического анализа
механико-математического факультета
ФГБОУ Московского государственного университета имени М.В. Ломономова
Чирский Владимир Григорьевич
Дата подписания:

Контактные данные:
тел.: e-mail:
Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.06 Математическая логика, алгебра и теория чисел.
Адрес места работы:
119992, г. Москва, ул. Ленинские горы,
МГУ им. М.В. Ломоносова, механико-математический факультет, кафедра математического анализа.

Подпись сотрудника механико-математического факультета
МГУ имени М.В. Ломоносова, профессора В.Г. Чирского, удостоверяю:
Декан механико-математического факультета МГУ,
член-корреспондент РАН А.И. Шафаревич
Дата подписания: