На правах рукописи

Новоселов Семен Александрович

Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2022

Работа выполнена в Балтийском федеральном университете имени Иммануила Канта.

Научный руководитель: кандидат физико-математических наук **Малыгина Екатерина Сергеевна**.

Официальные оппоненты: **Романьков Виталий Анатольевич,** доктор физико-математических наук, профессор, Омский государственный университет им. Ф.М. Достоевского, профессор.

Панкратова Ирина Анатольевна, кандидат физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет», заведующая лабораторией компьютерной криптографии.

Ведущая организация: Институт проблем передачи информации имени А. А. Харкевича РАН

Защита состоится 18 мая 2022 г. в 16 ч. 00 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академи наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук и на сайте http://math.nsc.ru.

Автореферат разослан «__» _____ 2022 г.

Ученый секретарь
диссертационного совета
Д 003.015.01,
к.ф.-м.н. Батуева Цындыма Чимит-Доржиевна

Общая характеристика работы

Актуальность темы. Алгебраические кривые над конечным полем имеют множество приложений в криптографии и теории кодирования. При этом в каждой области накладываются определенные требования на число точек как на кривой, так и в её якобиане.

В криптографии, основанной на сложности задачи нахождения дискретного логарифма, число точек в якобиане должно содержать большой простой делитель. В криптографии на изогениях [1; 2] число точек должно быть, наоборот, «гладким» — состоять из произведения малых простых чисел, что позволяет эффективно вычислять изогении большой составной степени как композицию изогений малых простых степеней. Кроме того, совсем недавно [3] было предложено использование якобианов гиперэллиптических кривых для построения групп с «неизвестным порядком», то есть групп с трудновычислимым на практике порядком. В частности, в [3] такие группы используются для построения криптографических верифицируемых функций задержки. При этом алгоритмы нахождения порядка группы, соответственно, для кривых — подсчёта точек, представляют собой методы криптоанализа таких криптосистем, т. е. проведения атаки. Несмотря на то, что задача вычисления числа точек имеет полиномиальную сложность $\widetilde{\mathcal{O}}(\log^{\Delta} q)$, где Δ — константа и q — размер конечного поля, над которым определена кривая, на практике алгоритмы с такой сложностью неприменимы, так как константа Δ может быть большой. Поэтому в реальных вычислениях применяется комбинированный алгоритм — сначала вычисляется число точек по модулю произведения как можно большего количества простых чисел ℓ, используя подход Схоофа-Пилэ [4; 5], затем запускаются экспоненциальные (от $\log q$) алгоритмы [6; 7] для восстановления точного числа точек. Необходимость запуска экспоненциального алгоритма на практике и позволяет в итоге основывать на сложности задачи подсчёта точек криптографические конструкции групп с неизвестным порядком. Также задача подсчёта точек на гиперэллиптических кривых имеет приложения в симметричной криптографии, где число точек влияет на нелинейность некоторых блоков подстановки, что позволяет доказать нижние границы нелинейности блока [8; 9]. В теории кодирования важную роль играют кривые с большим числом точек и нахождение уравнений таких кривых [10], [11, Глава 3.4].

При исследовании числовых последовательностей одним из самых мощных инструментов является метод производящих функций, который заключается в сопоставлении изучаемой последовательности чисел некоторого специально подобранного числового ряда, что позволяет исследовать дискретный объект (последовательность) аналитическими методами. Ряд подбирается так, чтобы он сходился к какой-либо удобной для работы функции. Например, если такой ряд сходится к рациональной функции, то его члены можно записать в виде выражения от корней многочленов в числителе и знаменателе, из чего можно вывести нетривиальные соотношения для членов исходной последовательности. Данная

работа посвящена задаче нахождения числа точек на кривой над конечным полем и в её якобиане, поэтому нас интересует последовательность, составленная из чисел точек на кривой над расширениями поля. Ключевую роль в подсчёте точек на кривой C рода g над конечным полем $\mathbb{F}_q$ характеристики p играет дзета-функция, которая определяется как производящая функция следующего вида:

$$\zeta_C(T) = Z_{C,q}(T) = \exp\left(\sum_{k=1}^{\infty} \frac{\#C(\mathbb{F}_{q^k})}{k} T^k\right),$$

где $\#C(\mathbb{F}_{q^k})$ — число точек на кривой над полем $\mathbb{F}_{q^k}$. Дзета-функция является рациональной функцией:

$$Z_{C,q}(T) = \frac{L_{C,q}(T)}{(1-T)(1-qT)},$$

где $L_{C,q}(T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$. Она удовлетворяет функциональному уравнению

$$Z_{C,q}(T) = q^{g-1} T^{2g-2} Z_{C,q}\left(\frac{1}{qT}\right),$$

из чего следует, что для коэффициентов многочлена $L_{C,q}(T)$ выполняется условие $a_{2g-i} = q^{g-i} a_i$ для $i = 0, \ldots, g$. Кроме того, для многочлена $L_{C,q}(T) = \prod_{i=1}^{2g}(1 - \alpha_i T), \alpha_i \in \mathbb{C}$ выполняется $|\alpha_i| = \sqrt{q}$. Данное утверждение представляет собой гипотезу Римана для функциональных полей кривых.

Данные три свойства дзета-функции — рациональность, функциональное уравнение и аналог гипотезы Римана — носят название «гипотез Вейля». При этом они были сформулированы Вейлем для общего случая алгебраических многообразий. В настоящее время все данные утверждения доказаны. Рациональность дзета-функции была доказана Вейлем для абелевых многообразий и кривых. Позже Дворк [12] доказал её для алгебраических многообразий с помощью p-адических методов. В отличии от известной гипотезы из теории чисел, её аналог для функциональных полей доказан: Хассе [13—15] — для эллиптических кривых, Вейлем [16] — для кривых и абелевых многообразий и, наконец, Делинем [17] — для общего случая алгебраических многообразий. Различные авторы также предоставили альтернативные доказательства данных утверждений на основе других методов, из которых можно отметить элементарное доказательство Степанова [18] и Бомбьери [19], которые представили обобщение результатов Хассе на кривые любого рода.

Дзета-функция тесно связана с эндоморфизмом Фробениуса якобиана кривой, который определяется для точек кривой C как отображение ϕ_q, возводящее каждую координату точки кривой в степень q. В якобиане Jac_C кривой C данное отображение индуцирует гомоморфизм, который и называется эндоморфизмом Фробениуса. Характеристический многочлен $\chi_{C,q}(T)$ эндоморфизма Фробени-

уса является взаимным многочленом для многочлена $L_{C,q}(T)$, т. е.

$$\chi_{C,q}(T) = T^{2g} L_{C,q}\left(\frac{1}{T}\right).$$

Число точек в якобиане определяется [20, с. 205] как $\#J_C(\mathbb{F}_q) = \chi_{C,q}(1) = L_{C,q}(1)$. Также для числа точек на кривой имеет место равенство

$$\#C(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k.$$

Соответственно, имеем $\#C(\mathbb{F}_q) = q + 1 + a_1$. Число $-a_1$ при этом называется следом эндоморфизма Фробениуса. Таким образом, число точек в якобиане и на кривой выражается через коэффициенты характеристического многочлена. Поэтому задача подсчёта точек сводится к его вычислению. Помимо числа точек данный многочлен также кодирует много важной арифметической информации о якобиане кривой. Согласно результатам Тэйта [21] и Хонды [22] характеристический многочлен является инвариантом относительно изогении абелевых многообразий и, кроме того, по факторизации данного многочлена можно определить, является ли якобиан кривой (или абелево многообразие) разложимым в произведение абелевых многообразий меньшей размерности.

В общем случае для числа точек на кривой и в якобиане нет явных формул, но существуют границы. Граница Хассе-Вейля-Серра для кривых утверждает, что

$$|\#C(\mathbb{F}_q) - q - 1| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Для якобианов кривых граница Хассе-Вейля принимает вид:

$$(\sqrt{q} - 1)^{2g} \leq \#J_C(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}.$$

Кроме того, для коэффициентов $a_1, \ldots, a_g$ многочлена $\chi_{C,q}(T)$ из гипотез Вейля следуют неравенства

$$|a_i| \leq \binom{2g}{i} q^{i/2}.$$

Однако для приложений недостаточно границ, и необходимо уметь считать точное число точек. Основные подходы для подсчёта точек можно разделить на p-адические, ℓ-адические и получение явных формул для специальных классов кривых. В основе p-адических методов, как правило, лежат различные методы для доказательства рациональности дзета-функции. В частности, доказательство Дворка [12] и построенные на его базе когомологии [23] легли в основу p-адического алгоритма Кедлаи [24]. Главным недостатком p-адических методов является сложность вычислений, равная $\widetilde{\mathcal{O}}(\sqrt{p})$ в худшем случае. Хотя в среднем случае достижима и полиномиальная сложность [25; 26], p-адические алгоритмы

обычно используются для подсчёта точек над полями малой характеристики. Методы на ℓ-адических числах включают в себя алгоритм Схоофа[1] [27] для эллиптических кривых, а также его оптимизации [28; 29] и обобщения на абелевы многообразия [5]. Идея алгоритма Схоофа и производных от него методов заключается в вычислении для числа $\ell \neq p$ характеристического многочлена χ_ℓ сужения эндоморфизма Фробениуса на группу ℓ-кручения $A[\ell]$ абелевого многообразия A. Так как $\chi_{A,q}(T) \equiv \chi_\ell(T) \pmod{\ell}$, получаем характеристический многочлен, редуцированный по модулю ℓ. Вычислив многочлен $\chi_\ell(T)$ для достаточно большого количества простых чисел ℓ, можно восстановить искомый характеристический многочлен $\chi_{A,q}(T)$ по китайской теореме об остатках. В случае эллиптических кривых оптимизированный алгоритм Схоофа-Элкиса-Аткина (SEA) [4; 27—29] имеет сложность $\widetilde{\mathcal{O}}(\log^4 q)$. Общий алгоритм Пилэ [5] для абелевых многообразий имеет сложность $\widetilde{\mathcal{O}}(\log^\Delta q)$. Однако, алгоритм требует для работы явные уравнения и групповой закон абелева многообразия, из чего следует, что константа Δ имеет суперэкспоненциальный рост от размерности g. Например, для якобианов гиперэллиптических кривых — $\Delta = \mathcal{O}(2^{4^g})$. Поэтому данный алгоритм имеет больше теоретический интерес. В случае гиперэллиптических кривых константа Δ может быть значительно уменьшена [30] до $\Delta = \mathcal{O}(g)$ благодаря использованию координат Мамфорда, алгоритма Кантора [31] для группового закона и другим оптимизациям. Таким образом, ℓ-адические алгоритмы лучше подходят для вычисления числа точек над полями большой характеристики по сравнению с p-адическими.

Для некоторых классов кривых возможно получение явных формул для числа точек. В частности, для кривых с геометрически разложимым якобианом (над замыканием поля $\overline{k}$) или в общем случае для геометрически разложимых абелевых многообразий возможно выражение числа точек над базовым полем через коэффициенты характеристических многочленов абелевых многообразий из разбиения над расширением. Это позволяет свести задачу подсчёта точек на одном абелевом многообразии размерности g к задаче вычисления числа точек на абелевых многообразиях меньших размерностей $g_1, \ldots, g_m$ таких, что $g = g_1 + \ldots + g_m$. Так как в меньшей размерности число точек считается асимптотически быстрее с помощью ℓ-адических или p-адических методов, это ведёт к снижению сложности решения задачи. Основными проблемами данного подхода являются:

1. определение геометрической разложимости якобиана для заданной кривой;
2. определение (минимальной) точной степени расширения, над которым имеет место разложение;
3. нахождение явных уравнений кривых, чьи якобианы присутствуют в разбиении;

[1] (гол.) Schoof = Схооф, в русскоязычной литературе больше известен как Шуф.

4. нахождение характеристического многочлена над базовым полем из характеристических многочленов абелевых многообразий над расширением.

Наибольшее ускорение достигается в случае, если якобиан кривой геометрически распадается на эллиптические кривые. В этом случае задача сводится к нахождению числа точек на эллиптических кривых, на которых она имеет сложность $\widetilde{\mathcal{O}}(\log^4 q)$ благодаря алгоритму Схоофа-Элкиса-Аткина. Проблема нахождения кривых с полностью разложимым якобианом над алгебраически замкнутым полем исследовалась Экедалем и Серром [32], где была поставлена задача нахождения для заданного рода g максимального числа t такого, что существует кривая X с якобианом $\mathrm{Jac}_X \sim E^t \times A$ для некоторой эллиптической кривой E и абелева многообразия A. Частичные ответы на данные вопросы для гиперэллиптических кривых даны в работах Паулюс и Рохас [33—36].

В работах [37—39] исследовались кривые с геометрически разложимым якобианом рода 2 вида $y^2 = x^5 + ax^3 + bx$. Было получено разбиение якобиана на эллиптические кривые над расширением, общие алгоритмы для подсчёта точек и явные формулы. Над базовым полем якобиан данной кривой может быть простым, поэтому кривая подходит, например, для использования в криптографии. В то же время разложение над расширением конечного поля позволяет в ряде случаев быстро считать число точек.

Однако неизвестно обобщения данных результатов на случай $g > 2$ и кривых $C : y^2 = x^{2g+1} + ax^{g+1} + bx$, а также на случай кривых с геометрически разложимым якобианом. Заметим, что в случае эллиптических кривых (род 1) имеем кривые в форме Лежандра. В этом случае есть давний результат Дойринга [40] — сравнение по модулю характеристики поля p, связывающее след Фробениуса кривой с многочленом Лежандра $P_{\frac{p-1}{2}}$ (инвариант Хассе-Витта). В данной диссертационной работе сравнения с многочленами Лежандра обобщаются на кривую C любого рода, а также на фактор-кривые C по автоморфизмам, т. е. кривые, задаваемые многочленами Диксона.

Целью данной работы является получение быстрых алгоритмов подсчёта точек и явных формул для характеристических многочленов класса гиперэллиптических кривых, задаваемых уравнением $C : y^2 = x^{2g+1} + ax^{g+1} + bx$, а также фактор-кривых по автоморфизмам данного класса кривых и кривых с геометрически разложимым якобианом.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Разработать алгоритм для восстановления характеристического многочлена $\chi_{A,q}$ над базовым полем $\mathbb{F}_q$ из характеристического многочлена χ_{A,q^k} над полем $\mathbb{F}_{q^k}$.
2. Разработать общий метод для нахождения числа точек на геометрически приводимом абелевом многообразии A, т. е. $A(\mathbb{F}_{q^k}) \sim A_1 \times \ldots \times A_m$, и его специализации к якобианам.

3. Применить полученные методы к классу кривых вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$. Для этого: получить разбиение якобиана кривой C, найти точную степень расширения, над которым разбиение имеет место, и явные уравнения кривых для якобианов в разбиении; построить алгоритмы на основе пунктов 1, 2. Для случая $g = 3$ и $g = 4$ получить оценки сложности алгоритма.

Научная новизна:

1. Было получено полное разложение якобиана кривой C с явными уравнениями для якобианов кривых в разложении и точными степенями расширений, обобщающее и объединяющее в одном месте результаты Топа, Смита, Сато, Паулюс и других [33; 37; 39; 41—43].
2. Предложен общий алгоритм для вычисления характеристических многочленов кривых C.
3. Предложен метод для получения полных списков характеристических многочленов $(\mathrm{mod}\ p)$ для случая $p \nmid g$ и $p > 2$.
4. Получены списки всех возможных характеристических многочленов $(\mathrm{mod}\ p)$ для кривых рода $g = 2 - 7$ в виде выражений от многочленов Лежандра.
5. Многочленам Лежандра сопоставлены кривые с абсолютно простыми якобианами, и предложен метод для вычисления числа точек на основе данного сопоставления.
6. Получены специализированные алгоритмы для родов 3, 4 на основе многочленов Лежандра и разложения якобиана с вероятностной эвристической сложностью $\widetilde{\mathcal{O}}(\log^4 q)$ и $\widetilde{\mathcal{O}}(\log^8 q)$ по сравнению со сложностью общего алгоритма [30; 44], равной $\widetilde{\mathcal{O}}(\log^{14} q)$ и $\widetilde{\mathcal{O}}(\log^{18+\epsilon} q)$ соответственно.

Практическая значимость. Полученные результаты могут использоваться для генерации кривых с большим простым сомножителем числа точек в якобиане, что требуется для криптографии. Полученные методы позволяют вычислить для геометрически разложимых абелевых многообразий инварианты относительно изогении (характеристические многочлены), что позволяет проверять якобианы и абелевы многообразия на изогенность. Так как сложность задачи подсчёта точек лежит в основе криптосистем на группах с неизвестным порядком [3], то полученные методы позволяют проводить оценки безопасности таких систем. В частности, показано что кривые рода 3 вида $y^2 = x^7 + ax^4 + bx$ и рода 4 вида $y^2 = x^9 + ax^5 + bx$ являются слабыми для построения криптосистем на группах с неизвестным порядком.

Методология и методы исследования. Основными методами исследования является теория алгебраических кривых и их функциональных полей. Для получения разложения якобиана кривой $y^2 = x^{2g+1} + ax^{g+1} + bx$ использовались частичные результаты из работ Топа, Смита, Паулюс и др. [33; 41—43] и метод Кани-Роузена [45]. Общий алгоритм является обобщением алгоритмов Сато [37], Гиевик и Верно [39] для рода 2 на произвольный род. Списки многочленов полу-

чены с использованием метода Картье-Манина, детальным изучением структуры матриц оператора Картье и применением формулы для характеристических многочленов мономиальных матриц из работы [46].

Основные положения, выносимые на защиту:

1. Общий алгоритм подсчёта точек на геометрически разложимых якобианах гиперэллиптических кривых, обобщающий работы Сато [37], Гиевик и Верно [39] для рода 2.
2. Алгоритм подсчёта точек для кривых вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$.
3. Соответствие многочленов Лежандра $P_m(x)$ кривым с абсолютно неприводимым якобианом, обобщающее связь эллиптических кривых с многочленами $P_{\frac{p-1}{2}}(x), P_{\frac{p-1}{3}}(x), P_{\frac{p-1}{4}}(x), P_{\frac{p-1}{6}}(x)$.
4. Методы для получения полного списка характеристических многочленов $(\mathrm{mod}\ p)$ кривой C и её фактор-кривых.
5. Специализированные алгоритмы и методы подсчёта точек для кривой C рода 3, 4 и их сложность.

Апробация работы. Основные результаты работы докладывались на следующих конференциях и семинарах: Международная конференция «Algorithmic Number Theory Symposium (ANTS-XIV)» (Новая Зеландия, г. Окленд, 2020 г.), Международная конференция «23rd Workshop on Elliptic Curve Cryptography» (Германия, г. Бохум, 2019 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография (SIBECRYPT)» (г. Красноярск, 2017 г.; г. Абакан, 2018 г.; г. Томск, 2019 г.), семинар «Математические методы криптографического анализа» (МГУ им. М.В. Ломоносова, 2021 г.), семинар Института проблем передачи информации имени А. А. Харкевича РАН по алгебраической геометрии (2021 г.), семинары «Дискретный анализ», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ (г. Новосибирск, 2021 г.).

Личный вклад. Все результаты были получены лично диссертантом, кроме явных формул для кривых рода 3 вида $y^2 = x^7 + ax^4 + bx$, которые были получены в соавторстве с Болтневым Ю. Ф.

Публикации. Основные результаты по теме диссертации изложены в 7 печатных изданиях, 4 из которых изданы в журналах, рекомендованных ВАК, или в периодических журналах, индексируемых Web of Science и Scopus, 3 — в тезисах докладов.

Объем и структура работы. Диссертация состоит из введения, четырех глав, заключения и четырех приложений. Полный объем диссертации 155 страниц текста, включая 2 рисунка и 10 таблиц. Список литературы содержит 158 наименований.

Содержание работы

Первая глава посвящена описанию предварительных сведений и методов, которые используются в последующих главах для получения результатов. Пусть C —

гиперэллиптическая кривая рода g над конечным полем $\mathbb{F}_q$ характеристики p, задаваемая уравнением $y^2 = f(x)$. Для получения разложения якобиана кривой в работе использовались следующие две теоремы и основанные на них методы.

Теорема (Клайман-Серр)**.** *Если существует неконстантный морфизм кривых $C \to D$, определённый над $\mathbb{F}_q$, то $L_{D,q}(T)$ делит $L_{C,q}(T)$.*

Данная теорема позволяет получить разложение якобиана в случае наличия морфизма кривых. Так как по теореме Тэйта [21] многочлен $L_{D,q}(T)$ делит $L_{C,q}(T)$ тогда и только тогда, когда $\mathrm{Jac}_C \sim \mathrm{Jac}_D \times A$. В случае если группа авторфизмов кривой C нетривиальна, т. е. помимо гиперэллиптической инволюции есть другие автоморфизмы, то может применяться следующая теорема.

Теорема (Кани-Роузен)**.** *Пусть $G \leq \mathrm{Aut}(C)$ — (конечная) подгруппа, для которой выполняется $G = H_1 \cup \ldots \cup H_t$, где подгруппы $H_i \leq G$ удовлетворяют условию $H_i \cap H_j = 1, i \neq j$. Тогда имеет место изогения*

$$\mathrm{Jac}_C^{t-1} \times \mathrm{Jac}_{C/G}^{g} \sim \mathrm{Jac}_{C/H_1}^{h_1} \times \ldots \times \mathrm{Jac}_{C/H_t}^{h_t},$$

где $g = |G|$, $h_i = |H_i|$ и Jac^n обозначает $\mathrm{Jac}^n = \mathrm{Jac} \times \ldots \times \mathrm{Jac}$ (n-раз).

Помимо разложения якобиана для подсчёта точек на кривой и получения списка всех возможных характеристических многочленов кривой по модулю p мы используем метод подсчёта точек на основе оператора Картье. Обозначим через c_i — коэффициенты при x^i в $f(x)^{\frac{p-1}{2}}$. Тогда *матрицей Картье-Манина* называется матрица $W = (c_{ip-j})_{i,j}$, для $1 \leq i,j \leq g$, а матрица $H = W^t$ называется матрицей Хассе-Витта. Введём матрицу $W_p = H \cdot H^{(p)} \cdot \ldots \cdot H^{(p^{n-1})}$, где $H^{(p^i)}$ обозначает возведение каждого элемента матрицы H в степень p^i. Тогда характеристический многочлен $\chi_{C,q}(T)$ кривой C связан с матрицей W_p формулой Манина [47—49]: $\chi_{C,q}(T) \equiv (-1)^g T^g \det(W_p - TI) \pmod p$.

Вторая глава содержит в себе основные общие теоретические результаты, состоит из 4-х подразделов.

Первый подраздел посвящён задаче восстановления характеристического многочлена эндоморфизма Фробениуса $\chi_{A,q}(T)$ абелева многообразия A по известному многочлену $\chi_{A,q^k}(T)$. Предлагаемый метод решения задачи представляет собой обобщение метода из работы Сато [37] для якобианов кривых вида $y^2 = x^5 + ax^3 + bx$ на случай любых абелевых многообразий. Он представляет собой спуск по относительным расширениям конечных полей, используя разложение $k = k_1 \cdot \ldots \cdot k_m$ и соответствующую башню конечных полей $\mathbb{F}_q \subset \mathbb{F}_{q^{k_1}} \subset \mathbb{F}_{q^{k_1 k_2}} \subset \ldots \subset \mathbb{F}_{q^k}$ с последовательным вычислением цепочки характеристических многочленов $\chi_{A,q^k} \mapsto \ldots \mapsto \chi_{A,q^{k_1 k_2}} \mapsto \chi_{A,q^{k_1}} \mapsto \chi_{A,q}$. В худшем случае при простом k метод ведёт к следующей оценке сложности решения задачи.

Теорема 1. *Пусть A — абелево многообразие размерности g над конечным полем $\mathbb{F}_q$. Вычисление характеристического многочлена $\chi_{A,q}(T)$ по заданному $\chi_{A,q^k}(T)$ занимает эвристическое вероятностное время*

$$\widetilde{\mathcal{O}}\left(2^{2^g g^2 k\epsilon}\log^2 q + C_{gw}(g,\beta) + R + 2^{2^g g\log_2(gk)\epsilon'} S\log q\right)$$

битовых операций, где $\epsilon = 3.545$, $\epsilon' = 1.766$, R — сложность выбора случайной точки, S — сложность группового закона, C_{gw} — сложность выполнения конвертации базиса Грёбнера из $grevlex$ порядка в lex для системы из многочленов степени $\beta = 2\left(\frac{(gk)^2}{2} + gk\right)^{2^{g-1}}$ от g — неизвестных. В случае, если соответствующая система уравнений имеет размерность 0, полагаем $C_{gw} = 0$.

Получение точных оценок для C_{gw} в случае положительной размерности является открытой проблемой теории сложности. Однако, в наших вычислениях такой случай не встречался. Более точные оценки доказываем для случаев $g = 3, k = 2^r 3^s$ и $g = 4, k = 2^s$, используя вместо базисов Грёбнера метод результантов.

Теорема 2. *Пусть A — абелево многообразие размерности 3 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{A,q}(T)$ по известному $\chi_{A,q^k}(T)$ для $k = 2^r 3^s$, где $r, s \geq 0$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{2r-4}3^{2s-4}\log^2 q(R + 2^{r-1}3^{s+1}S\log q))$ битовых операций. Здесь R — сложность выбора случайной точки из $A(\mathbb{F}_{q^{2^{r-1}3^s}})$, а S — сложность группового закона.*

Теорема 3. *Пусть A — абелево многообразие размерности 4 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{A,q}(T)$ по известному $\chi_{A,q^k}(T)$, где $k = 2^r$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{2r}\log^2 q(R + 2^{r+1}S\log q))$ битовых операций. Здесь R — сложность выбора случайной точки из $A(\mathbb{F}_{q^{2^{r-1}}})$, а S — сложность группового закона.*

Так как для якобианов гиперэллиптических кривых задача выбора случайной точки (в данном случае класса дивизоров) и групповой закон имеют полиномиальную сложность от $\log q$, получаем следующие оценки.

Следствие 3.1. *Пусть C — гиперэллиптическая кривая рода 3 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{C,q}(T)$ по известному $\chi_{C,q^k}(T)$, где $k = 2^r 3^s$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{4r}3^{4s}\log^4 q)$ битовых операций.*

Следствие 3.2. *Пусть C — гиперэллиптическая кривая рода 4 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{C,q}(T)$ по известному $\chi_{C,q^k}(T)$, где $k = 2^r$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{4r}\log^4 q)$ битовых операций.*

Применяя полученные оценки сложности нахождения $\chi_{A,q}(T)$ по известному $\chi_{A,q^k}(T)$ к геометрически приводимым абелевым многообразиям, получаем во втором подразделе второй главы следующие теоремы.

Теорема 4. *Пусть A — абелево многообразие размерности 3 над конечным полем $\mathbb{F}_q$ и $k = 2^r 3^s$. Тогда характеристический многочлен $\chi_{A,q}(T)$, а значит, и $\#A(\mathbb{F}_q)$, может быть найден за эвристическое вероятностное время (в битовых операциях):*

1. *$\widetilde{\mathcal{O}}(k^4 \log^4 q + \mathcal{O}_D))$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times E_2 \times E_3$.*
2. *$\widetilde{\mathcal{O}}(k^\Delta \log^\Delta q + \mathcal{O}_D))$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times A_2$.*
3. *$\widetilde{\mathcal{O}}(k^8 \log^8 q + \mathcal{O}_D))$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times A_2$ и A_2 — якобиан гиперэллиптической кривой рода 2.*

Здесь $\mathcal{O}_D = \widetilde{\mathcal{O}}(2^{2r}3^{2s} \log^2 q(R + 2^r 3^s S \log q))$ — сложность спуска. В случае, если A — якобиан гиперэллиптической кривой рода 3, то имеем:

1. *$\widetilde{\mathcal{O}}(k^4 \log^4 q)$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times E_2 \times E_3$.*
2. *$\widetilde{\mathcal{O}}(k^\Delta \log^\Delta q))$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times A_2$.*
3. *$\widetilde{\mathcal{O}}(k^8 \log^8 q)$, если $A(\mathbb{F}_{q^k}) \sim E_1 \times A_2$ и A_2 — якобиан гиперэллиптической кривой рода 2.*

Здесь Δ — экспонента из алгоритма Пилэ для абелевой поверхности A_2, R — сложность выбора случайной точки на A, S — сложность группового закона на A.

Теорема 5. *Пусть A — абелево многообразие размерности 4 над конечным полем $\mathbb{F}_q$ такое, что $A \sim A_1 \times \ldots \times A_m$ над $\mathbb{F}_{q^k}$, где $k = 2^r$ и $A_1, \ldots, A_m$ — абелевы многообразия размерности $g_1, \ldots, g_m$. Тогда характеристический многочлен $\chi_{A,q}(T)$, а значит, и число точек на A, может быть найден за эвристическое вероятностное время*

$$\widetilde{\mathcal{O}}(\log^{\Delta(g_1)} q^k + \ldots + \log^{\Delta(g_m)} q^k + \mathcal{O}_D)$$

битовых операций. Здесь $\mathcal{O}_D = 2^{2r} \log^2 q(R + 2^{r+1} S \log q)$, $\Delta(g_i)$ — экспоненты из алгоритма Пилэ для абелевых многообразий A_i, R — сложность выбора случайной точки на $A(\mathbb{F}_{q^{2^{r-1}}})$, S — сложность группового закона.

Третий подраздел второй главы посвящен исследованию специального класса гиперэллиптических кривых с геометрически разложимым якобианом, задаваемых уравнением $C : y^2 = x^{2g+1} + ax^{g+1} + bx$. Данные кривые имеют длинную историю изучения, которую можно проследить от работ Лежандра. Поэтому сначала даётся обзор известных результатов по данному классу кривых. Затем мы находим разбиение якобиана данной кривой, на основе частичных результатов из [33; 41; 42] и метода Кани-Роузена. Получаем, что $\mathrm{Jac}_C \sim \mathrm{Jac}_{C/\langle\sigma\rangle} \times \mathrm{Jac}_{C/\langle\sigma\iota\rangle}$, где уравнения фактор-кривых по автоморфизмам приводим в следующей теореме.

Теорема 6. *Пусть* $C : y^2 = x^{2g+1} + ax^{g+1} + \alpha^g x$ *— это гиперэллиптическая кривая рода* g*, определенная над конечным полем* $\mathbb{F}_q$*, и* ι *— гиперэллиптическая инволюция. Тогда кривая* C *имеет негиперэллиптическую инволюцию* $\sigma : (x, y) \mapsto (\frac{\alpha}{x}, y\frac{\alpha^{\frac{g+1}{2}}}{x^{g+1}})$ *и уравнения фактор-кривых кривой* X *по модулю инволюций* σ *и* $\iota\sigma$ *следующие.*

1. *Если род* g *нечётный, то* $C/\langle\sigma\rangle : y^2 = D_g(x,\alpha) + a$ *и* $C/\langle\iota\sigma\rangle : y^2 = (x^2 - 4\alpha)(D_g(x,\alpha) + a)$.
2. *Если род* g *чётный, то* $C/\langle\sigma\rangle : y^2 = (x+2\sqrt{\alpha})(D_g(x,\alpha)+a)$ *и* $C/\langle\iota\sigma\rangle : y^2 = (x - 2\sqrt{\alpha})(D_g(x,\alpha) + a)$.

Здесь $D_g(x, \alpha)$ *— многочлен Диксона степени* g.

Соответственно, якобиан кривой C раскладывается над полем $\mathbb{F}_q[\sqrt[g]{b}]$ в случае нечётного рода и над полем $\mathbb{F}_q[\sqrt[2g]{b}]$ в случае чётного рода. Таким образом, мы знаем точную степень расширения, над которым имеет место разложение якобиана, и явные уравнения кривых в разложении. Поэтому мы можем подсчитать характеристические многочлены кривых в разложении и восстановить характеристический многочлен кривой C по методам из предыдущих подразделов или по следующей формуле [50, с. 195] для L-многочленов: $L_{C,q^k}(T^k) = \prod_{\zeta^k=1} L_{C,q}(\zeta T)$.

Соответствующий алгоритм для рода 2 с разложениями якобиана, полученными другим методом, представлен в работах [37; 39]. Наш алгоритм и разложение якобиана работает для любого рода.

Другой метод для подсчёта точек на данных кривых, представленный в главе 2, основан на операторе Картье и его матрицах действия. Можно показать, что матрица Картье-Манина кривой C с параметром $b = 1$ состоит из многочленов Лежандра. Из свойств многочленов Лежандра следует, что данная матрица — центросимметрична. Кроме того, в работах [51; 52] было замечено, что данная матрица является ещё и мономиальной (обобщенной перестановочной) при $p \nmid g$. Данные свойства также можно частично распространить и на матрицу Картье-Манина кривой C в случае $b \neq 1$. Перечисленные свойства позволяют перебрать все характеристические многочлены кривой C, используя формулу Манина и разложение на циклы перестановки, которая соответствует нашей мономиальной матрице. В итоге получается список из g возможных многочленов, выраженных через многочлены Лежандра.

На основе данного метода нами были составлены списки характеристических многочленов $\pmod p$ для родов $1 - 7$. Но их можно получить для любого рода. Заметим, что для эллиптических кривых известны [53—55] сопоставления следов Фробениуса с многочленами Лежандра $P_{\frac{p-1}{2}}, P_{\frac{p-1}{3}}, P_{\frac{p-1}{4}}, P_{\frac{p-1}{6}}$. Поэтому данные многочлены в полученных нами списках характеристических многочленов можно рассчитать за время $\widetilde{\mathcal{O}}(\log^4 q)$ по эффективному алгоритму Схоофа-Элкиса-Аткина, что даёт нам эффективный алгоритм подсчёта точек для рода 3. В остальных случаях соответствие многочленов Лежандра коэффициентам характеристического многочлена кривых рода 2 и выше можно получить из раз-

ложения якобиана кривой C, которое мы используем для получения следующих утверждений в четвёртом подразделе второй главы.

Следствие 6.1. *Пусть g — чётное целое. Для матриц Картье-Манина $W' = (w'_{i,j}), \widetilde{W}' = (\widetilde{w}'_{i,j})$ гиперэллиптических кривых $X'_2 : y^2 = (x+2)(D_g(x)+c)$ и $\widetilde{X}'_2 : y^2 = (x-2)(D_g(x)+c)$ над конечным полем $\mathbb{F}_q$ выполняется:*

1. $w'_{i,j} = P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}) - P_{\frac{(g-i)p-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2})$;
2. $\widetilde{w}'_{i,j} = P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}) + P_{\frac{(g-i)p-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2})$.

Здесь $1 \le i,j \le \frac{g}{2}$ и P_m — многочлен Лежандра степени m, $D_g(x) = D_g(x,1)$ — многочлен Диксона степени g. При этом в случае $m \notin \mathbb{Z}$ полагаем $P_m = 0$.

Следствие 6.2. *Пусть g — нечётное целое. Для матриц Картье-Манина $W' = (w'_{i,j})$, $\widetilde{W}' = (\widetilde{w}'_{i,j})$ гиперэллиптических кривых $X'_1 : y^2 = D_g(x) + c$ и $X'_3 : y^2 = (x^2-4)(D_g(x)+c)$ над конечным полем $\mathbb{F}_q$ выполняется:*

1. $w'_{i,j} = P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}) - P_{\frac{(g-i)p-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2})$, $1 \le i,j \le \frac{g-1}{2}$;
2. $\widetilde{w}'_{i,j} = \begin{cases} P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}) + P_{\frac{(g-i)p-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}), & 1 \le i,j \le \frac{g-1}{2}; \\ P_{\frac{p-1}{2}}(-\frac{c}{2}), & i = \frac{g+1}{2} \text{ или } j = \frac{g+1}{2}. \end{cases}$

Здесь P_m — многочлен Лежандра степени m, $D_g(x) = D_g(x,1)$ — многочлен Диксона степени g. При этом в случае $m \notin \mathbb{Z}$ полагаем $P_m = 0$.

Изложенные во второй главе результаты опубликованы в [A1; A2; A5; A6].

Третья глава посвящена специализации общих алгоритмов и методов из главы 2 к случаю кривых $y^2 = x^7 + ax^4 + bx$ рода 3 и кривых $y^2 = x^9 + ax^5 + bx$ рода 4, что позволило получить более точные результаты. В частности, явные формулы для коэффициентов характеристического многочлена в случае рода 3 вместо алгоритма на основе разложения якобиана. Доказано также, что сложность подсчёта точек на данных кривых равна $\widetilde{\mathcal{O}}(\log^4 q)$ и $\widetilde{\mathcal{O}}(\log^8 q)$ соответственно.

Изложенные в третьей главе результаты опубликованы в [A1; A2; A7].

Четвертая глава посвящена применению полученных результатов в криптографии и других областях. Представлены алгоритмы для генерации кривых с заданным числом точек в якобиане. Получены сравнения для многочленов Лежандра. Показано, что полученные результаты делают гиперэллиптические кривые $y^2 = x^7 + ax^4 + bx$ и $y^2 = x^9 + ax^5 + bx$ слабыми для использования в криптографических конструкциях на группах с неизвестным порядком.

В **заключении** приведены основные результаты работы.

Публикации автора по теме диссертации

A1. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$ // Finite Fields and Their Applications. — 2020. — Vol. 68, no. 101757. — P. 1—27.

A2. *Novoselov S. A.* Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials // Прикладная дискретная математика. — 2017. — № 37. — С. 20—31.

A3. *Malygina E. S.*, *Novoselov S. A.* Division polynomials for hyperelliptic curves defined by Dickson polynomials // Математические вопросы криптографии. — 2020. — Т. 11, № 2. — С. 69—81.

A4. *Новоселов С. А.* Границы сбалансированной степени вложения для криптографии на билинейных спариваниях // Прикладная дискретная математика. — 2016. — Т. 32, № 2. — С. 63—86.

A5. *Novoselov S. A.* Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials // Прикладная дискретная математика. Приложение. — 2017. — С. 29—32.

A6. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$ // Прикладная дискретная математика. Приложение. — 2018. — С. 30—33.

A7. *Novoselov S. A.*, *Boltnev Y. F.* Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields // Прикладная дискретная математика. Приложение. — 2019. — С. 44—46.

Список литературы

1. *Flynn E.*, *Ti Y.* Genus two isogeny cryptography // Lect. Notes Comput. Sci. — 2019. — Vol. 11505. — P. 286—306.
2. *Costello C.*, *Smith B.* The supersingular isogeny problem in genus 2 and beyond // Lect. Notes Comput. Sci. — 2020. — Vol. 12100. — P. 151—168.
3. *Dobson S.*, *Galbraith S. D.*, *Smith B.* Trustless Groups of Unknown Order with Hyperelliptic Curves // IACR Cryptol. ePrint Arch. — 2020. — Vol. 2020. — P. 196.
4. *Schoof R.* Counting points on elliptic curves over finite fields // J. Théor. Nombres Bordeaux. — 1995. — Vol. 7, no. 1. — P. 219—254.
5. *Pila J.* Frobenius maps of abelian varieties and finding roots of unity in finite fields // Math. Comput. — 1990. — Vol. 55, no. 192. — P. 745—763.
6. *Matsuo K.*, *Chao J.*, *Tsujii S.* An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields // Lect. Notes Comput. Sci. — 2002. — Vol. 2369. — P. 461—474.
7. *Gaudry P.*, *Schost É.* A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm // Lect. Notes Comput. Sci. — 2004. — Vol. 3076. — P. 208—222.

8. *Cheon J. H.*, *Chee S.*, *Park C.* S-boxes with controllable nonlinearity // Lect. Notes Comput. Sci. — 1999. — Vol. 1592. — P. 286—294.

9. *Cheon J. H.*, *Chee S.* Nonlinearity of Boolean functions and hyperelliptic curves // SIAM J. Discrete Math. — 2003. — Vol. 16, no. 3. — P. 354—365.

10. *Hurt N. E.* Many rational points: coding theory and algebraic geometry. Vol. 564. — Springer, 2013.

11. *Tsfasman M.*, *Vladut S. G.* Algebraic-geometric codes. Vol. 58. — Springer Science & Business Media, 1991.

12. *Dwork B.* On the rationality of the zeta function of an algebraic variety // Amer. J. Math. — 1960. — Vol. 82, no. 3. — P. 631—648.

13. *Hasse H.* Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. // J. Reine Angew. Math. — 1936. — Vol. 175. — P. 55—62.

14. *Hasse H.* Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem. // J. Reine Angew. Math. — 1936. — Vol. 175. — P. 69—88.

15. *Hasse H.* Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. // J. Reine Angew. Math. — 1936. — Vol. 175. — P. 193—208.

16. *Weil A.* Numbers of solutions of equations in finite fields // Bull. Amer. Math. Soc. — 1949. — Vol. 55, no. 5. — P. 497—508.

17. *Deligne P.* La conjecture de Weil. I // Publ. Math. IHÉS. — 1974. — Vol. 43, no. 1. — P. 273—307.

18. *Степанов С.* О числе точек гиперэллиптической кривой над простым конечным полем // Изв. АН СССР. Сер. матем. — 1969. — № 5. — С. 1171—1181.

19. *Bombieri E.* Counting points on curves over finite fields // Lect. Notes Math. — 1974. — Vol. 383. — P. 234—241.

20. *Mumford D.* Abelian varieties. — Oxford University Press, 1974.

21. *Tate J.* Endomorphisms of abelian varieties over finite fields // Inventiones mathematicae. — 1966. — Vol. 2, no. 2. — P. 134—144.

22. *Honda T.* Isogeny classes of abelian varieties over finite fields // J. Math. Soc. Japan. — 1968. — Vol. 20, no. 1/2. — P. 83—95.

23. *Monsky P.*, *Washnitzer G.* Formal cohomology: I // Annals of Mathematics. — 1968. — P. 181—217.

24. *Kedlaya K.* Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology // J. Ramanujan Math. Soc. — 2001. — No. 16. — P. 318—330.

25. *Harvey D.*, *Sutherland A. V.* Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time // LMS J. Comput. Math. — 2014. — Vol. 17, A. — P. 257—273.

26. *Harvey D.*, *Sutherland A. V.* Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II // Contemporary Mathematics. — 2016. — Vol. 663. — P. 127—148.

27. *Schoof R.* Elliptic curves over finite fields and the computation of square roots mods p // Math. Comput. — 1985. — Vol. 44, no. 170. — P. 483—494.

28. *Elkies N. D.* Explicit isogenies // preprint. — 1991.

29. *Atkin A. O.* The number of points on an elliptic curve modulo a prime // Preprint. — 1988.

30. *Abelard S.*, *Gaudry P.*, *Spaenlehauer P.-J.* Improved Complexity Bounds for Counting Points on Hyperelliptic Curves // Foundations of Computational Mathematics. — 2019. — Vol. 19, no. 3. — P. 591—621.

31. *Cantor D. G.* Computing in the Jacobian of a hyperelliptic curve // Math. Comput. — 1987. — Vol. 48, no. 177. — P. 95—101.

32. *Ekedahl T.*, *Serre J.-P.* Exemples de courbes algébriques à jacobienne complètement décomposable // C. R. Acad. Sci. Série 1, Mathématique. — 1993. — Vol. 317, no. 5. — P. 509—513.

33. *Paulhus J. R.* Elliptic factors in Jacobians of low genus curves. — University of Illinois at Urbana-Champaign, 2007.

34. *Paulhus J.* Decomposing Jacobians of curves with extra automorphisms // Acta Arith. — 2008. — Vol. 132, no. 3. — P. 231—244.

35. *Paulhus J.* Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups // The Open Book Series. — 2013. — Vol. 1, no. 1. — P. 487—505.

36. *Paulhus J.*, *Rojas A. M.* Completely decomposable Jacobian varieties in new genera // Exp. Math. — 2017. — Vol. 26, no. 4. — P. 430—445.

37. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields // Lect. Notes Comput. Sci. — 2009. — Vol. 5479. — P. 536—553.

38. *Freeman D. M.*, *Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction // J. Number Theory. — 2011. — Vol. 131, no. 5. — P. 959—983.

39. *Guillevic A.*, *Vergnaud D.* Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions // Lect. Notes Comput. Sci. Vol. 7708. — Springer. 2012. — P. 234—253.

40. *Deuring M.* Die typen der multiplikatorenringe elliptischer funktionenkörper // Abh. Math. Semin. Univ. Hambg. — 1941. — Vol. 14, no. 1. — P. 197—272.

41. *Tautz W.*, *Top J.*, *Verberkmoes A.* Explicit hyperelliptic curves with real multiplication and permutation polynomials // Canad. J. Math. — 1991. — Vol. 43, no. 5. — P. 1055—1064.

42. *Smith B.* Explicit endomorphisms and correspondences. — University of Sydney, 2005.

43. *Kohel D. R.*, *Smith B. A.* Efficiently computable endomorphisms for hyperelliptic curves // Lect. Notes Comput. Sci. — 2006. — Vol. 4076. — P. 495—509.

44. *Abelard S.* Counting points on hyperelliptic curves in large characteristic: algorithms and complexity. — Université de Lorraine, 2018.

45. *Kani E.*, *Rosen M.* Idempotent relations and factors of Jacobians // Mathematische Annalen. — 1989. — Vol. 284, no. 2. — P. 307—327.

46. *Garcia-Planas M. I.*, *Magret M. D.* Eigenvalues and eigenvectors of monomial matrices // Proceedings of the XXIV Congress on Differential Equations and Applications. XIV Congress on Applied Mathematics. — Universidad de Cádiz. 2015. — P. 963—966.

47. *Манин Ю. И.* О матрице Хассе–Витта алгебраической кривой // Изв. АН СССР. Сер. матем. — 1961. — Т. 25, № 1. — С. 153—172.

48. *Манин Ю. И.* К теории абелевых многообразий над полем конечной характеристики // Изв. АН СССР. Сер. матем. — 1962. — Т. 26, № 2. — С. 281—292.

49. *Yui N.* On the Jacobian varieties of hyperelliptic curves over fields of characteristic p > 2 // J. Algebra. — 1978. — Vol. 52, no. 2. — P. 378—410.

50. *Stichtenoth H.* Algebraic function fields and codes. — Springer, 2009.

51. *Miller L.* The Hasse-Witt-matrix of special projective varieties // Pacific Journal of Mathematics. — 1972. — Vol. 43, no. 2. — P. 443—455.

52. *Miller L.* Curves with invertible Hasse-Witt-matrix // Mathematische Annalen. — 1972. — Vol. 197, no. 2. — P. 123—127.

53. *Sun Z.-H.* Congruences concerning Legendre polynomials II // J. Number Theory. — 2013. — Vol. 133, no. 6. — P. 1950—1976.

54. *Sun Z.-H.* Congruences involving $\binom{2k}{k}^2\binom{3k}{k}$ // J. Number Theory. — 2013. — Vol. 133, no. 5. — P. 1572—1595.

55. *Sun Z.-H.* Legendre polynomials and supercongruences // Acta Arith. — 2013. — Vol. 159, no. 2. — P. 169—200.

Новоселов Семен Александрович

Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Типография _____