ОТЗЫВ

официального оппонента на диссертацию
С. А. Новоселова
на тему:

"Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом"

по специальности 01.01.09 – "Дискретная математика и математическая кибернетика"
на соискание ученой степени кандидата физико-математеческихнаук
наук.

Диссертационная работа посвящена нахождению и разработке быстрых алгоритмов подсчёта точек и получению явных формул для характеристических многочленов некоторых классов гиперэллиптических кривых.

Алгебраические кривые широко изучались на протяжении всей истории математики. Их исследования уходят корнями еще в древнегреческие времена несмотря на то, что тогда кривые еще не записывались уравнениями. Основы современного подхода к этой области были заложены такими математиками, как Ферма и Эйлер, которые связывали алгебраические кривые с классической теорией чисел. В дальнейшем развитие теории алгебраических кривых связано с именами Римана, Хассе и Вейля. Стало уделяться больше внимания на алгебраические кривые над конечными полями. В 40-е годы прошлого столетия Хассе и Вейль дали оценку числа рациональных точек для кривой над конечным полем. Тем не менее, интерес к поиску кривых со многими рациональными точками оставался незначительным вплоть до 1980 года, когда Гоппа нашел важные приложения кривых над конечными полями в теории кодирования. С тех пор многие математики проявили интерес к алгебраическим кривым над конечными полями, и в этой области ведется интенсивная исследовательская деятельность.

В середине 70-х годов 20-го столетия Диффи и Хеллман высказали идущую от Меркля идею шифрования с открытым ключем. Тогда же они предложили использовать широко распространенный в настоящее время протокол распределения ключа, носящий их имена. В качестве платформы для этого протокола было предложено использовать мультипликативные группы конечных полей. Криптографическая стойкость протокола основывается на трудноразрешимой проблеме вычисления дискретного логарифма.

В теории алгебраических кривых особое внимание уделяляется важному классу эллиптических кривых. С каждой такой кривой связывается

абелева группа, которую можно выбрать в качестве платформы для построения систем и протоколов. Использование эллиптических кривых в криптографии было независимо предложено Нилом Коблицем и Виктором Миллером в 1985 году. Появилась эллиптическая версия дискретного логарифма и эллиптический аналог протокола Диффи-Хеллмана, имеющие ряд преимуществ по сравнению с оригиналами на платформах конечных полей. Впоследствии различные эллиптические системы и протоколы были зафиксированы в качестве стандартов, в том числе и в России.

Спустя несколько лет за этим последовало предложение использовать группы классов дивизоров гиперэллиптических кривых над конечным полем. Стали актуальными вычислительные проблемы, связанные с эффективной реализацией группового закона и нахождением дискретных логарифмов в группах классов дивизоров алгебраических кривых, также известных как группы Пикара. В последнее десятилетие в качестве платформ для криптографических примитивов все чаще стали предлагаться гиперэллиптические кривые. В основе этих примитивов, как и в случае эллиптических кривых, лежит трудноразрешимая задача вычисления дискретного логарифма. В настоящее время не известен субэкспоненциальный алгоритм для вычисления дискретных логарифмов даже на кривых малого рода. Поэтому необходимый уровень безопасности при использовании этих примитивов достигается при сравнительно небольших параметрах. Например, он требует ключи меньших размеров, чем это нужно для криптографической системы RSA.

В данной работе находятся и разрабатываются быстрые алгоритмы подсчёта точек и находятся явные формулы для характеристических многочленов класса $\mathcal{C}$ гиперэллиптических кривых над конечными полями, задаваемых уравнениями вида

$$y^2 = x^{2g+1} + ax^{g+1} + bx,$$

а также их фактор кривых по автоморфизмам и кривых с геометрически разложимым якобианом. Имеется большая потребность в построении кривых с теми или иными свойствами. В одних случаях (в протоколах, основанных на трудноразрешимости проблемы вычисления дискретного логарифма) требуется, чтобы порядок группы кривой делился на большое простое число. В других, напротив, нужно, чтобы порядок группы имел только небольшие простые делители, хотя и должен сам по себе быть большим. Известных оценок бывает недостаточно, нужно вычислять точные порядки. Эта тематика несомненно актуальна и востребована в криптографии, основанной на кривых. Она представляет интерес и сама по себе.

Основные результаты работы следующие:

1. Разработан алгоритм подсчёта точек на геометрически разложимых якобианах гиперэллиптических кривых произвольного рода, обобщающий результаты Сато, Гиевик и Верно для рода 2.

2. Разработан алгоритм подсчёта точек для кривых из класса $\mathcal{C}$.

3. Установлено соответствие многочленов Лежандра $P_m(x)$ и кривых с абсолютно неприводимым якобианом, обобщающее классическую связь эллиптических кривых с многочленами $P_{p-1/i}$ для $i = 2, 3, 4, 6$.

4. Методы для получения полного списка характеристических многочленов (mod p) кривой C и её факторкривых.

5. Разработаны специализированные алгоритмы и методы подсчёта точек для кривых из класса $\mathcal{C}$ рода $g = 3, 4$, исследована сложность полученных алгоритмов.

При этом решались соответствующие конкретные задачи. Например, для результата (1) показан алгоритм разбиения якобиана, предъявлен метод нахождения точной степени расширения, над которым разбиение имеет место, и указан вывод явных уравнений кривых в разбиении.

Научная новизна:

1. Новым результатом является получение полного разложения якобиана произвольной кривой из класса $\mathcal{C}$ и соответствующих явных уравнений для якобианов кривых в разложении, также вычисление точных степеней соответствующих расширений. Этот результат существенно обобщает и классифицирует результаты Топа, Смита, Сато, Паулюс и ряда других исследователей.

2. Новым является общий алгоритм вычисления характеристических многочленов кривых из класса $\mathcal{C}$.

3. Впервые получены полные списки характеристических многочленов (mod p) для случая, когда характеристика $p \geq 3$ не делит род кривой g, а также списки всех возможных характеристических многочленов (mod p) для кривых рода $2 \leq g \leq 7$ в виде выражений от многочленов Лежандра.

4. Многочленам Лежандра сопоставлены кривые с абсолютно простыми якобианами, и предложен метод для вычисления числа точек на основе данного сопоставления.

5. Получены специализированные алгоритмы для родов $g = 3$ и $g = 4$ на основе многочленов Лежандра и разложения якобиана с вероятностной эвристической сложностью $\tilde{O}(log^4 q)$ и $\tilde{O}(log^8(q)$, соответственно. Эти сложности существенно меньше, чем соответствующие сложности общего алгоритма.

Методы исследования:

Результаты диссертации опираются на классические теоремы теории абелевых многообразий, кривых высоких порядков, алгебраической геометрии в целом. Ключевым элементом в подсчёте точек на кривой класса $\mathcal{C}$ играет дзета функция, которая определяется как некоторая производящая функция. Ее основные свойства – рациональность, функциональное уравнение и аналог гипотезы Римана – доказаны Вейлем, Дворком, Хассе, Делинем, Степановым и Бомбьери. Используются также результаты Тейта, Хонды, координаты Мамфорда и другие элементы высокого уровня. Автор демонстрирует свое владение данной областью исследований. Он применяет как известные методы, развивая их, так и свои оригинальные подходы к решению сложных проблем. Использовались частичные результаты из работ Топа, Смита, Паулюс, метод Кани-Роузена, дано обобщение алгоритмов Сато, Гиевик и Верно для произвольного рода, использовался и получил развитие метод Картье-Манина.

Практические приложения:

Результаты, полученные в диссертации, имеют практическое приложение в криптографии. Их можно использовать для построения кривых, для которых число точек в якобиане делится на большое простое число, то есть не является "гладким" и поэтому не поддается известным методам его вычисления. Это позволяет использовать протоколы, основанные на трудноразрешимости дискретного логарифма и порядка группы. С другой стороны методы позволяют вычислять для геометрически разложимых абелевых многообразий инварианты относительно изогении. Сложность задачи подсчёта точек лежит в основе криптосистем на группах с неизвестным порядком, поэтому это позволяет оценивать уязвимость соответствующих систем. Построены конкретные примеры таких "слабых" кривых.

Все приведенные результаты правильно сформулированы и полностью доказаны. Результаты имеют значение как для теории алгебраических кривых над конечными полями, так и для криптографии на этих кривых. Они также имеют практическую значимость как для построения криптографических систем, так и для их анализа. Диссертация выглядит

завершенным трудом. Она хорошо оформлена, написана ясным языком, достаточно компактна. Публикации полностью соответствуют содержанию диссертации. Основные результаты работы неоднократно докладывались на Сибирской научной школе-семинаре с международным участием "Компьютерная безопасность и криптография (SIBECRYPT)", на международных конференциях в Новой Зеландии, Германии, научных семинарах в МГУ им. М.В. Ломоносова, Институте проблем передачи информации имени А. А. Харкевича РАН, Институте математики им. С. Л. Соболева СО РАН, НГУ.

Кандидатская диссертация С. А. Новоселова полностью соответствует Положению о порядке присуждения ученых степеней. А именно: она является научно-квалификационной работой, в которой содержится решение научной задачи, имеющей значение для развития соответствующей отрасли знаний.

Доктор физико-математических наук профессор
Романьков Виталий Анатольевич,
профессор Омского государственного университета
им. Ф.М. Достоевского
19.04.2022