Краткое изложение заявки

Новоселов С.А.

Введение. Гиперэллиптические кривые представляют собой обобщение эллиптических кривых. Однако, в отличии от эллиптических кривых множество точек гиперэллиптических кривых группу не образует, поэтому групповой закон определяется в якобиане кривой, который является алгебраической группой и абелевым многообразием. Изогении якобианов кривых определяются как сюрьективные гомоморфизмы, имеющие конечное ядро. Степенью изогении называется количество элементов в её ядре.

Целью данного проекта является нахождение изогений якобианов гиперэллиптических кривых в явном виде. Более точно планируется разработка новых методов для решения следующих задач:

Задача 1. Для заданной подгруппы G якобиана Jac кривой построить изогению, действующую из Jac в фактор-многообразие Jac/G, и найти уравнение кривой, чей якобиан изоморфен Jac/G, при условии что такая кривая существует.

Задача 2. Для заданного числа n и двух кривых C, D с изогенными якобианами найти изогению степени n между якобианами этих кривых, при условии что такая изогения существует.

Мотивацией для решения данных задач служат приложения в алгебраической геометрии, теории кодирования и криптографии: нахождение модулярных многочленов с помощью графов изогений; получение новых классов оптимальных кривых из уже известных классов оптимальных кривых решением задачи 1; построение на основе сложности решения задачи 2 криптосистем, стойких к атакам на квантовом компьютере.

Проведенные исследования. Для класса кривых вида $y^2 = x^{2g+1} + ax^{g+1} + bx$ над конечным полем получено разбиение якобиана с точной степенью расширения поля, над которым оно имеет место, и явными уравнениями кривых, чьи якобианы присутствуют в разбиении. Результат получен по методу построения изогений Клаймана-Серра и Кани-Роузена. Кроме того, исследовалась матрица действия оператора Картье. Доказанные свойства матрицы – цетросимметричность, приведение в блочно-диагональную форму, связь с многочленами Лежандра – позволили получить полные списки возможных порядков якобиана по модулю характеристики поля p. Используя разбиение якобиана над расширением поля и свойства матрицы Картье, построены алгоритмы для подсчёта точек над базовым полем, где якобиан кривой может быть либо простым, либо содержать простые абелевы многообразия. Подсчёт точек на кривых позволяет ответить на вопрос, существует ли изогения между якобианами двух заданных кривых.

Проект будущих исследований. 1. Обобщение формул Велу[1], которые решают задачу 1 для эллиптических кривых, на кривые рода 2 и выше на основе теории функциональных полей, в отличии от существующих методов на тета-функциях, которые предполагают работу с громоздким явным представлением якобиана как абелева многообразия.

2. Обобщение ℓ-адического алгоритма [2] для решения задачи 2 на эллиптических кривых на кривые рода 2 и выше.

3. Применение полученных формул и методов для нахождения модулярных многочленов, построения оптимальных кривых и конструкции криптосистем.

[1] J. Vélu, «Isogénies entre courbes elliptiques», *CR Acad. Sci. Paris, Séries A*, т. 273, с. 305—347, 1971.

[2] L. De Feo, C. Hugounenq, J. Plût и É. Schost, «Explicit isogenies in quadratic time in any characteristic», *LMS Journal of Computation and Mathematics*, т. 19, № A, с. 267—282, 2016.