Федеральное государственное автономное образовательное учреждение
высшего образования «Балтийский федеральный университет имени
Иммануила Канта»

На правах рукописи
УДК 512.772

Новоселов Семен Александрович

Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом.

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
кандидат физико-математических наук
Малыгина Екатерина Сергеевна

Калининград — 2022

Оглавление

Стр.

Стр.

Стр.

Введение

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 Фробениуса 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

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

Для якобианов кривых граница Хассе-Вейля принимает вид:

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

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

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

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 $A[\ell]$

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

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;

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 $\pmod p$ для случая $p \nmid g$ и $p > 2$.
4. Получены списки всех возможных характеристических многочленов $\pmod p$ 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 $\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q)$ 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 получены 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:

1. Семинар Института проблем передачи информации имени А. А. Харкевича РАН по алгебраической геометрии. Доклад «Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом». 2021.
2. Семинары «Дискретный анализ», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ (г. Новосибирск, 2021). Доклад: «Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом».
3. Семинар «Математические методы криптографического анализа» (МГУ им. М.В. Ломоносова, 2021). Доклад: «Подсчёт точек на гиперэллиптических кривых и приложения в криптографии».[2]
4. 14th Algorithmic Number Theory Symposium, ANTS-XIV (University of Auckland, New Zealand, 2020). Стендовый доклад: «Counting points on hyperelliptic curves with geometrically split Jacobians». [3]
5. 23rd Workshop on Elliptic Curve Cryptography (Rump Session) (г. Бохум, Германия, 2019). Доклад: «Point-counting on families of curves with geometrically split Jacobian».[4]
6. XVIII Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» (г. Томск, Россия, 2019). Доклад: «Характеристические многочлены кривой $y^2 = x^7 + ax^4 + bx$ над конечным полем». [5]
7. XVII Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» (г. Абакан, Россия, 2018). Доклад: «Подсчёт числа точек на гиперэллиптических кривых вида $y^2 = x^{2g+1} + ax^{g+1} + bx$».[5]
8. XVI Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» (г. Красноярск, Россия, 2017). Доклад: «Гиперэллиптические кривые, матрицы Картье-Манина и многочлены Лежандра». [5]

[2] http://mcrypto.ru/
[3] https://www.math.auckland.ac.nz/~sgal018/ANTS/posters.html
[4] https://ecc.2019.rump.cr.yp.to/
[5] http://sibecrypt.tsu.ru/

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 переодических журналах, индексируемых Web of Science и Scopus, 3 — в тезисах докладов.

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

Первая глава носит обзорный характер и содержит предварительные сведения из теории абелевых многообразий и кривых над конечным полем, методах разложения якобианов гиперэллиптических кривых и методах подсчёта точек.

Вторая глава содержит основные теоретические результаты работы. В случае геометрически разложимых якобианов задача подсчёта точек над расширением сводится к подсчёту точек (нахождению характеристических многочленов) абелевых многообразий или якобианов меньшей размерности, поэтому нам необходимо разработать метод для спуска к базовому полю. Соответствующий метод для нахождения характеристического многочлена над базовым полем из характеристического многочлена над расширением представлен в §2.1. Он заключается в решении задачи по шагам, спускаясь по относительным расширениям поля. Это существенно упрощает задачу, так как в общем случае необходимо решать систему полиномиальных уравнений от нескольких переменных, и решение задачи по шагам позволяет снизить степени многочленов в уравнениях. Тем не менее, в общем случае сложность задачи остаётся двойной экспоненциальной от степени расширения и экспоненциальной от битового размера поля. Однако для случая якобианов кривых рода $g = 3$ и степени расширения $k = 2^r 3^s$, а также случая $g = 4$ и степени расширения $k = 2^r$, мы доказываем (Следствие 2.1.8.1, 2.1.9.1), что задача имеет (вероятностную) сложность $\widetilde{\mathcal{O}}(k^4 \log^4 q)$ битовых операций, т. е. является полиномиальной от степени расширения k и битового размера поля $\log q$.

В разделе §2.2 методы для нахождения характеристического многочлена из §2.1 применены для решения задачи подсчёта точек на геометрически

разложимых абелевых многообразиях. Для якобианов гиперэллиптических кривых рода 3 и 4, которые раскладываются на якобианы гиперэллиптических кривых меньшего рода над расширениями степени $k = 2^r 3^s$ и $k = 2^r$, доказана сложность решения задачи подсчёта точек, равная $\widetilde{\mathcal{O}}(k^8 \log^8 q)$ для $g = 3$ и $\widetilde{\mathcal{O}}(k^{14} \log^{14} q)$ для $g = 4$.

Раздел §2.3 посвящён приложению методов из предыдущих разделов к гиперэллиптическим кривым вида $y^2 = x^{2g+1} + ax^{g+1} + bx$. На основе работ [33; 41—43; 45] получено точное разложение якобиана кривой над расширением степени g для нечётного рода и $2g$ для чётного рода. На основе разложения получен общий алгоритм подсчёта точек. Исследование структуры матриц Картье-Манина кривой позволило получить списки всех возможных характеристических многочленов якобиана кривой по модулю характеристики поля p, выраженные в многочленах Лежандра.

В разделе §2.4 получены полные списки характеристических многочленов по модулю p для кривых уже с абсолютно простым якобианом, которые являются фактор-кривыми по автоморфизмам кривых из §2.3.

Третья глава содержит специализированные алгоритмы и формулы для кривых вида $y^2 = x^7 + ax^4 + bx$ и $y^2 = x^9 + ax^5 + bx$. Доказано, что сложность подсчёта точек на данных кривых равна $\widetilde{\mathcal{O}}(\log^4 q)$ и $\widetilde{\mathcal{O}}(\log^8 q)$ соответственно.

Четвёртая 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.

Глава 1. Предварительные сведения

Данная глава содержит предварительные сведения обзорного характера, необходимые для доказательства результатов из последующих глав.

1.1 Абелевы многообразия над конечным полем

В данном разделе собраны необходимые нам в дальнейшем результаты и определения по абелевым многообразиям над конечными полями.

Определение 1.1.1. *Абелевым многообразием* над полем k называется проективное алгебраическое многообразие, обладающее структурой группы.

Пусть A — абелево многообразие над полем k размерности $\dim A = g$.

Определение 1.1.2. *Изогенией* абелевых многообразий A и B называется сюръективный (над $\overline{k}$) гомоморфизм абелевых многообразий с конечным ядром. Два абелева многообразия называются изогенными $A \sim B$, если существует изогения между ними.

Абелево многообразие называется *простым*, если оно не содержит подмногообразия, которое является абелевым. Для абелевых подмногообразий имеет место следующая теорема.

Теорема 1.1.1 (Пуанкаре о полной приводимости)**.** *Пусть A — абелево многообразие, B — абелево подмногообразие. Тогда существует абелево подмногообразие C в A такое, что $A = B + C$ и $B \cap C$ — конечная группа. Другими словами, A изогенно $B \times C$.*

Доказательство. См. [20, с. 173, Теорема 1] или [47, с. 28, Теорема 6]. □

Из теоремы Пуанкаре следует, что любое абелево многообразие A изогенно произведению простых абелевых многообразий:

$$A \sim A_1^{d_1} \times \cdots \times A_n^{d_n},$$

где d_i — целые положительные числа такие, что $d_1 + \ldots + d_n = g$. Обозначим $\mathrm{End}_k(A)$ — множество эндоморфизмов абелева многообразия A, определённых над k. Пусть $n \in \mathbb{N}$, определим отображение

$$[n] : A \to A, x \mapsto n \cdot x.$$

Для $n = 0$ определим $[0]$ как нулевое отображение, а при $n < 0$ положим $[n]$ равным $-[|n|]$. Таким образом, отображение $[n]$ определено для любого целого n и оно задаёт инъективный гомоморфизм из $\mathbb{Z}$ в $\mathrm{End}_k(A)$. Отображение $[n]$ для $n \neq 0$ является изогенией. Ядро $[n]$ над $\overline{k}$ обозначается как $A[n]$. Оно имеет следующую структуру.

Предложение 1 ([20, с. 64]). *Пусть A — абелево многообразие размерности g над полем k характеристики p. Тогда*

1. *если $p \nmid n$, то $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$;*
2. *если $p \mid n$, то существует целое число t, $0 \leqslant t \leqslant g$, такое, что для всех $m \geqslant 1$ имеем*

$$A[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^t.$$

Число t из предложения называется *p-рангом* абелева многообразия A. В случае $t = g$ абелево многообразие называется *обычным*. Эллиптическая кривая (т. е. абелево многообразие размерности $g = 1$) называется *суперсингулярной*, если она имеет p-ранг $t = 0$. Абелево многообразие называется *суперсингулярным*, если оно изогенно над $\overline{k}$ произведению суперсингулярных эллиптических кривых. Если абелево многообразие суперсингулярно, то оно имеет p-ранг 0, но обратное утверждение верно только в случае $g \leqslant 2$ [48, с. 61, Замечание 4.75].

Пусть теперь $k = \mathbb{F}_q$. Тогда можем определить отображение $\varphi_q : x \mapsto x^q$, которое индуцирует тождественное отображение на многочленах над $\mathbb{F}_q$. Поэтому $\varphi_q(A) = A$ и $\varphi_q \in \mathrm{End}_{\mathbb{F}_q}(A)$. Это отображение называется *эндоморфизмом Фробениуса*.

Пусть $\ell \neq p$ – простое число. Определим *модуль Тэйта* как

$$T_\ell(A) = \varprojlim A[\ell^k].$$

Модуль Тэйта как $\mathbb{Z}_\ell$-модуль изоморфен $(\mathbb{Z}_\ell)^{2g}$ [48, с. 61, Cor. 4.80], где $\mathbb{Z}_\ell$ — целые ℓ-адические числа. Т. е. модуль Тэйта является свободным $\mathbb{Z}_\ell$-модулем ранга $2g$. Пусть $G = \mathrm{Gal}(\overline{k}/k)$. Тэйтом и Хондой в работах [21; 22] было доказано, что для любых абелевых многообразий A, B существует биекция

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \to \mathrm{Hom}_G(T_\ell(A), T_\ell(B)).$$

Поэтому $\mathrm{Hom}_k(A,B)$ — конечно порождённый свободный $\mathbb{Z}$-модуль ранга меньше либо равного $4\dim A \cdot \dim B$ (следует из $T_\ell(A) \simeq (\mathbb{Z}_\ell)^{2g}$). Соответственно, $\mathrm{End}_k(A)$ — конечно порожденный свободный $\mathbb{Z}$-модуль ранга $\leqslant 4(\dim A)^2$ и $\mathrm{End}_k(A) \otimes \mathbb{Q}$ — конечномерная полупростая алгебра над $\mathbb{Q}$.

Каждому эндоморфизму $\varphi \in \mathrm{End}_k(A)$ соответствует эндоморфизм $T_\ell(\varphi)$ действующий на модуле Тэйта. Поэтому можно определить характеристический многочлен эндоморфизма φ как характеристический многочлен матрицы оператора, соответствующего $T_\ell(\varphi)$, т. е.

$$\chi_\varphi(T) = \det(M_{T_\ell(\varphi)} - TI).$$

При этом многочлен χ_φ не зависит от выбора ℓ, имеет степень $2g$, унитарный, с коэффициентами из $\mathbb{Z}$. Доказательства утверждений и детали можно найти в [20, Гл. IV.19] и [48, §4.3.6]. Будем обозначать характеристический многочлен эндоморфизма Фробениуса φ_q абелева многообразия A над полем $\mathbb{F}_q$ как $\chi_{A,q}(T)$. Пусть B — другое абелево многообразие, а $\chi_{A,q}(T) = \prod P^{a(P)}$ и $\chi_{B,q}(T) = \prod P^{b(P)}$ — разложения многочленов $\chi_{A,q}$, $\chi_{B,q}$ на неприводимые многочлены над $\mathbb{Q}$. Тогда определим

$$r(\chi_{A,q}, \chi_{B,q}) = \sum_P a(P)b(P)\deg P.$$

Имеет место следующее утверждение [21, Теор.1].

Теорема 1.1.2. *Пусть A, B — абелевы многообразия над конечным полем $k = \mathbb{F}_q$. Тогда:*

1. $\mathrm{rank}(\mathrm{Hom}_k(A,B)) = r(\chi_{A,q}, \chi_{B,q})$.
2. *Следующие утверждения эквивалентны:*
   - *а) B изогенно абелеву подмногообразию A над k.*
   - *б) $\chi_{B,q}$ делит $\chi_{A,q}$.*
3. *Следующие утверждения эквивалентны:*
   - *а) A и B изогенны над k.*
   - *б) $\chi_{A,q} = \chi_{B,q}$.*
   - *в) дзета-функции A и B совпадают.*
   - *г) A и B имеют одно и тоже число точек в любом расширении поля k.*

Из теоремы следует, что характеристический многочлен непростого абелево многообразия равен произведению характеристических многочленов абелевых

подмногообразий. Соответственно, вычислив характеристический многочлен абелева многообразия с помощью алгоритмов подсчёта точек, можно определить, является ли абелево многообразие разложимым, сопоставив делителям характеристического многочлена соответствующие абелевы многообразия (при условии, что они существуют).

1.2 Гиперэллиптические кривые

Гиперэллиптической кривой C рода g над конечным полем $\mathbb{F}_q$ характеристики p называется гладкая кривая, задаваемая уравнением

$$y^2 + h(x)y = f(x),$$

где $f, h \in \mathbb{F}_q[x]$, f — унитарный многочлен степени $2g+1$ или $2g+2$, $\deg h \leqslant g+1$. Условие гладкости означает, что кривая не имеет сингулярных точек, т.е. точек в которых обе частные производные обращаются в 0 одновременно.

Если $\deg f = 2g + 1$, то кривая называется мнимой гиперэллиптической кривой. В противном случае кривая называется действительной гиперэллиптической кривой. Мнимые кривые могут быть преобразованы бирациональным преобразованием в действительные и обратно при некоторых ограничениях (см. [49, Prop. 2.1]). В нашей работе мы ограничиваемся в основном мнимыми гиперэллиптическими кривыми, так как они наиболее часто используются в приложениях.

Изоморфизмы гиперэллиптической кривой имеют вид [48, с. 308]:

$$(x, y) \mapsto (u^2x + v, u^{2g+1}y + u_g x^g + \ldots + u_1 x + u_0),$$

где $u \in \mathbb{F}_q^\times, v \in \mathbb{F}_q$. В случае $p \neq 2$ изоморфное преобразование $y \mapsto y - h(x)/2$ позволяет привести уравнение кривой в краткую форму

$$C : y^2 = f(x).$$

В случае $p \neq 2g + 1$ отображение $x \mapsto x - \frac{f_{2g}}{2g+1}$ позволяет убрать из f одночлен $f_{2g}x^{2g}$. Такая форма кривой называется краткой формой Вейерштрасса. При $p = 2$ имеем $h(x) \neq 0$, иначе кривая будет иметь сингулярную точку.

Якобиан кривой над полем k определяется как

$$\mathrm{Jac}_C(k) = \mathrm{Div}_C^0 \,/\, \mathrm{Princ}_C,$$

где Div_C^0 — группа дивизоров степени 0 на кривой C, а Princ_C — множество главных дивизоров, т. е. дивизоров составленных из нулей и полюсов некоторой функции на кривой.

Якобиан кривой является абелевым многообразием. Для арифметики в якобиане используются координаты Мамфорда (см. [48, §4.4.7]), в которых групповой закон задаётся алгоритмом Кантора [31].

Заметим, что для якобианов кривых возможно также получение явных уравнений, задающих якобиан как абелево многообразие. Для гиперэллиптических кривых рода 2 такие уравнения можно найти в работах Гранта [50] и Флинна [51; 52]. Данные работы основываются на теории тета-функций и общей конструкции якобиана Мамфорда [53, Гл. IIIa].

В виду большого числа уравнений и переменных явное представление якобианов обычно не используется в исследованиях и для арифметики на гиперэллиптических кривых. Взамен, используются координаты Мамфорда. Однако, в связи с развитием систем компьютерной алгебры, явное представление абелевых многообразий имеет определённый интерес, в частности, для нахождения изогений [54]. Кроме того, алгоритм Пилэ [5] для подсчёта точек в абелевых многообразиях над конечными полями требует для своей работы явное представление абелевого многообразия и группового закона на нём.

1.3 Оператор Картье и матрицы Картье-Манина

Оператор Картье, а точнее нахождение матрицы, задающей оператор как полулинейное отображение, позволяет найти характеристический многочлен $\chi_{C,q}(T)$ гиперэллиптической кривой C по модулю характеристики поля p. За определением и свойствами оператора Картье, отсылаем к работам [55; 56]. Само определение нам не потребуется, так как метод для подсчёта точек на основе оператора Картье может быть сформулирован в элементарном виде. Пусть гиперэллиптическая кривая C над конечным полем $\mathbb{F}_q$, $q = p^n$, $p > 2$ задана

уравнением

$$C : y^2 = f(x).$$

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 $1 \leqslant i,j \leqslant g$. А матрица $H = W^t$ называется матрицей Хассе-Витта. Данные матрицы являются матрицами дуальных операторов, поэтому чтобы получить одну из другой их достаточно транспонировать. За подробностями отсылаем к работе [56].

Тот факт, что оператор Картье представляется матрицей W, был показан Маниным в работе [57, §4], а в [58, Теорема 1] им же было доказано следующее соотношение матрицы H с характеристическим многочленом $\chi_{C,q}(T)$. 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. Данная матрица представляет собой матрицу n-кратного применения оператора Фробениуса. Тогда имеет место следующая формула:

$$\chi_{C,q}(T) \equiv (-1)^g T^g \det(W_p - TI) \pmod{p}. \tag{1.1}$$

Заметим, что наибольшую известность формула (1.1) получила благодаря работе Юи [55], которая изложила результаты Манина в цельном и детальном виде с дополнительными результатами для гиперэллиптических кривых.

Таким образом, для вычисления $\chi_{C,q}(T) \pmod{p}$ достаточно возвести многочлен f в степень $\frac{p-1}{2}$, составить из коэффициентов матрицу Картье-Манина и применить формулу (1.1). Найти многочлен $\chi_{C,q}(T)$ по многочлену $\chi_{C,q}(T) \pmod{p}$ можно перебором с помощью известных неравенств для коэффициентов характеристического многочлена:

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

Такой метод в случае кривой рода 2 и $q = p$ позволяет восстановить многочлен $\chi_{C,q}(T)$ за время $\mathcal{O}(1)$. Однако в остальных случаях данный метод уже имеет экспоненциальную сложность от $\log q$, и для восстановления $\chi_{C,q}(T)$ следует использовать алгоритмы, основанные на парадоксе дней рождения [6; 7; 44].

Помимо подсчёта точек матрица Картье-Манина позволяет определить p-ранг кривой, так как p-ранг кривой равен рангу матрицы W_p ([55, Lemma E] применённая как описано в [56, §5.1]).

Для нахождения матрицы Картье-Манина есть более эффективные методы, чем возведение многочлена $f(x)$ в степень $\frac{p-1}{2}$. Данная матрица может быть вычислена за время $\widetilde{\mathcal{O}}(\sqrt{p})$ в худшем случае с помощью алгоритма из работы [59]. В среднем её вычисление имеет полиномиальную сложность [25; 26].

В последующих разделах мы покажем, что для специального вида кривых матрицы Картье-Манина имеют особый вид и свойства, что позволит нам разложить характеристический многочлен $\chi_{C,q}(T) \pmod p$ на множители, частично или полностью, и составить полные списки возможных многочленов, чтобы затем использовать их для подсчёта точек.

1.4 Методы разложения якобианов гиперэллиптических кривых

По теореме Пуанкаре о полной приводимости якобиан гиперэллиптической кривой C, как и любое абелево многообразие, раскладывается в произведение простых абелевых многообразий:

$$\mathrm{Jac}_C \sim A_1 \times \ldots \times A_n.$$

Благодаря теореме Тэйта (Теорема 1.1.2), известно, что такому разложению соответствует разложение характеристического многочлена

$$\chi_{C,q}(T) = \chi_{A_1,q}(T) \cdot \ldots \cdot \chi_{A_n,q}(T).$$

Поэтому для определения существования разложения якобиана достаточно разложить характеристический многочлен на множители над полем $\mathbb{Q}$ и сопоставить многочлены в разложении с абелевыми многообразиями. В случае, если характеристический многочлен неприводим, то якобиан кривой простой. Однако, в общем случае не для каждого многочлена в разложении существует соответствующее ему абелево многообразие.

Отдельной задачей также является описание характеристических многочленов, соответствующих якобианам кривых. Для эллиптических кривых и

кривых рода 2 [60] данная задача решена. Поэтому, рассчитав характеристический многочлен кривой C, можно определить, есть ли в разложении её якобиана эллиптические кривые и якобианы кривых рода 2.

Однако сопоставление явных уравнений кривых характеристическим многочленам в общем случае является открытой непростой задачей, так как для её решения требуется найти в явном виде представитель класса изогений абелевого многообразия.

Есть два основных метода для получения разложения якобиана без необходимости вычисления характеристического многочлена: из накрытий (по теореме Клаймана-Серра) и с помощью метода Кани-Роузена [45].

Мы опишем только два основных метода и затем применим их к интересующему нас классу кривых. Заметим, что также есть и альтернативные [61] методы разложения якобианов, но мы их не используем.

1.4.1 Разложения из накрытий

В случае кривых известно, что любой морфизм кривых (геометрически) либо сюръективен, либо представляет собой константную функцию [62, Prop. 6.8, с. 137]. Соотвестенно, в якобианах кривых такой морфизм индуцирует изогению. Следующая теорема [61, Th. 3] позволяет получить разложение якобиана при наличии неконстантого морфизма кривых.

Теорема 1.4.1 (Клайман-Серр)**.** *Если существует неконстантный морфизм кривых $C \to D$, определённый над $\mathbb{F}_q$, то $L_D(T)$ делит $L_C(T)$.*

Из теоремы можно вывести несколько следствий, позволяющих в некоторых случаях по уравнению кривой получить разбиение её якобиана на абелевы многообразия.

Следствие 1.4.1.1. *Пусть $C : y^2 = f(x)$ — гиперэллиптическая кривая рода g над конечным полем $\mathbb{F}_q$ такая, что $f(x) = xg(x^d)$ для некоторого $g(x) \in \mathbb{F}_q[x]$ и нечётного целого числа $d > 2$. Тогда отображение $\nu : (x, y) \mapsto (x^d, yx^{\frac{d-1}{2}})$ — это морфизм кривых $C \to D$, где $D : y^2 = xg(x)$. Кроме того,*

1. $\chi_{D,q} \mid \chi_{C,q}$,

2. $\mathrm{Jac}_D \subset \mathrm{Jac}_C$,

3. $\mathrm{Jac}_C \sim \mathrm{Jac}_D \times A$, *где* A — *абелево многообразие.*

Доказательство. Первый пункт следует из теоремы 1.4.1. Второй пункт эквивалентен первому по теореме Тэйта [21, Th.1.b]. Так как Jac_D – абелево подмногообразие Jac_C, то по теореме Пуанкаре о полной приводимости [20, с. 173] существует абелево подмногообразие A такое, что $\mathrm{Jac}_C \sim J_D \times A$. □

Заметим, что в случае, если d раскладывается на множители, то существует несколько морфизмов и, соответственно, разбиений.

Следствие 1.4.1.2. *Пусть* $C : y^2 = f(x)$ – *гиперэллиптическая кривая рода* g *над конечным полем* $\mathbb{F}_q$ *такая, что* $f(x) = g_1(g_2(x))$, *где* $\deg g_1, \deg g_2 \geqslant 2$. *Тогда* $\nu : (x, y) \mapsto (g_2(x), y)$ – *морфизм кривых* C *и* $D : y^2 = g_1(x)$.

Многочлены f, подходящие под условия следствия, называются (функционально) разложимыми. Многочлен может иметь несколько разложений, которые позволяют получить несколько разбиений якобиана кривой. Существуют полиномиальные алгоритмы, позволяющие получить все возможные функциональные разложения [63]. Однако, так как все разложимые многочлены имеют степень, раскладывающуюся на простые множители, то следствие полезно только для кривых с $\deg f = 2g + 1$ рода $g \geqslant 4$, либо для кривых с чётной степенью f.

Замечание. *Кривые с нечётной степенью* f *можно преобразовать в кривые с чётной степенью. Возможно также обратное преобразование, но оно определено только над некоторым расширением базового поля. Соответствующие рациональные отображения можно найти в работе [49, Предложение 2.1].*

Замечание. *По следствию 1.4.1.2 гиперэллиптические кривые с простым якобианом могут задаваться только уравнением с функционально неразложимым многочленом* f.

1.4.2 Метод Кани-Роузена

Метод Кани-Роузена [45] позволяет найти разложение абелева многообразия A при наличии в алгебре эндоморфизмов $\mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes \mathbb{Q}$

определённых соотношений эквивалентности между идемпотентами (элементами ε такими, что $\varepsilon^2 = \varepsilon$). Два элемента $a, b \in \mathrm{End}_k^0(A)$ называются эквивалентными $a \sim b$, если для любого $\mathbb{Q}$-рационального характера $\chi \in \mathrm{ch}(\mathrm{End}_k^0(A))$ выполняется $\chi(a) = \chi(b)$, где $\mathrm{ch}(V)$ для конечномерной $\mathbb{Q}$-алгебры V обозначает кольцо, состоящее из линейных комбинаций с целыми коэффициентами из неприводимых $\mathbb{Q}$-характеров. В основе метода разложения абелева многообразия лежит следующая теорема [45, Th. A]:

Теорема 1.4.2. *Пусть $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon'_1, \ldots, \varepsilon'_m \in \mathrm{End}_k^0(A)$ — идемпотенты. Тогда соотношение*

$$\varepsilon_1 + \ldots + \varepsilon_n \sim \varepsilon'_1 + \ldots + \varepsilon'_m$$

выполняется тогда и только тогда, когда существует изогения

$$\varepsilon_1(A) \times \ldots \times \varepsilon_n(A) \sim \varepsilon'_1(A) \times \ldots \times \varepsilon'_m(A).$$

Применимость метода к якобианам кривых зависит от способности находить такие соотношения для заданной кривой. Для этого в случае кривых с автоморфизмами может использоваться следующая теорема [45, Теор. B].

Теорема 1.4.3. *Пусть $G \leqslant \mathrm{Aut}(C)$ — (конечная) подгруппа, для которой выполняется $G = H_1 \cup \ldots \cup H_t$, где подгруппы $H_i \leqslant G$ 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).

Как следует из теоремы, метод Кани-Роузена позволяет найти разложение якобиана кривой Jac_C при наличии у кривой нетривиальной группы автоморфизмов с подгруппой, допускающей разбиение в объединение непересекающихся подгрупп. Как только по теореме получено разложение якобиана, нам остаётся найти фактор-кривые C/G и C/H_i. Заметим, что в явном виде в координатах Мамфорда изогения может быть построена с помощью методов из работы [42]. Такой вид может использоваться для ускорения подсчёта точек, как это сделано в [44; 64; 65] для кривых с действительным умножением, но в нашей работе нам потребуются только уравнения фактор-кривых. Для подгруппы $H \leqslant \mathrm{Aut}(C)$ найти фактор-кривую C/H можно следующим образом. Сначала нужно определить род кривой C/H. Это можно сделать по следующей теореме, используя отображение $\varphi_H : C \to C/H$.

Теорема 1.4.4 (Риман-Гурвиц). *Предположим, что* $\varphi : C_1 \to C_2$ *— неконстантный сепарабельный морфизм кривых над полем* k *рода* g_1 *и* g_2 *соответственно. Пусть* $e_\varphi(P)$ *— индекс ветвления* φ *в точке* P*. Тогда*

$$2g_1 - 2 \geqslant (\deg \varphi)(2g_2 - 2) + \sum_{P \in C_1} (e_\varphi(P) - 1),$$

где равенство выполняется в случае $\mathrm{char}(k) = 0$ *или* $\mathrm{char}(k) \nmid e_\varphi(P)$ *для всех* P*.*

Зная род кривой C/H, для нахождения уравнения кривой необходимо найти образующие поля $k(C)^H$, состоящего из функций $k(C)$, неподвижных относительно действия группы H. Затем по образующим составить уравнение кривой (см. пример в доказательстве Теоремы 2.3.2).

В случае гиперэллиптических кривых все возможные группы автоморфизмов над алгебраически замкнутым полем описаны в работе [66]. Для гиперэллиптических кривых (над $\overline{k}$) с автоморфизмами разложения по описанному выше методу получены в работах [33—35] для случая малого рода. Так как метод Кани-Роузена работает для любого поля, данные разбиения так же имеют место и в случае конечного поля. Однако, сами автоморфизмы и модели фактор-кривых будут отличаться, и их ещё требуется найти.

Таким образом, метод Кани-Роузена позволяет найти разложения абелевых многообразий или якобианов кривых при условии, что мы можем построить нетривиальные соотношения между идемпотентами в кольце эндоморфизмов абелева многообразия (якобиана кривой). В случае якобианов кривых, для этой цели мы можем использовать автоморфизмы. Для кривой вида $y^2 = x^{2g+1} + ax^{g+1} + bx$ разложения по данному методу получим в §2.3.2.

1.5 Сложность операций в конечном поле

В теоретических доказательствах сложности работы алгоритмов будем использовать арифметику в конечных полях, представленную в Таблице 1. При этом считаем, что размер поля $q \to \infty$. Заметим, что на практике могут использоваться и другие алгоритмы, но их асимптотическая сложность хуже.

Таблица 1 — Сложность операций в конечном поле $\mathbb{F}_q$, в битовых операциях

Операция	Сложность	Ссылки
умножение, $M(\log q)$	$\mathcal{O}(\log q \log\log q)$	[67]
деление	$\mathcal{O}(\log q (\log\log q)^{2+o(1)})$	[68, §1.4]
извлечение квадратного корня	$\mathcal{O}(\log q) M(\log q)$	[69]
факторизация многочлена степени d из $\mathbb{F}_q[x]$	$\widetilde{\mathcal{O}}(d^2 \log q) M(\log q)$	[70, с. 390]

1.6 Методы подсчёта точек на абелевых многообразиях

В общем случае для подсчёта точек на абелевом многообразии A над конечным полем $\mathbb{F}_q$ может использоваться алгоритм Пилэ [5], который представляет собой обобщение алгоритма Схоофа [4; 27] для подсчёта точек на эллиптических кривых. Алгоритм имеет полиномиальную сложность от битового размера поля $\log q$. Соответственно, получаем следующую общую оценку для подсчёта точек на абелевых многообразиях.

Предложение 2. *Пусть A — абелево многообразие размерности g над конечным полем $\mathbb{F}_q$ и N — целое число такое, что $A \subset \mathbb{P}^N$. Тогда нахождение характеристического многочлена эндоморфизма Фробениуса $\chi_{A,q}(T)$ занимает время $\widetilde{\mathcal{O}}(\log^{\Delta} q)$ битовых операций, где $\Delta = \mathcal{O}(g^3 N 2^N)$. Более точно, $\Delta = c g^3 N 2^N$, где $c = 172$ при $g \geqslant 2$.*

Доказательство. Нахождение характеристического многочлена абелева многообразия с помощью алгоритма Пилэ [5] занимает время $\mathcal{O}(\log^{\Delta} q)$ операций в поле $\mathbb{F}_q$ или $\widetilde{\mathcal{O}}(\log^{\Delta+1} q)$ битовых операций при использовании алгоритма [67] для выполнения умножения в поле. При этом для Δ выполняется:

$$\Delta \leqslant 6(2g+2)(2\log R)\max(2g, 1+2\log D) N 2^N, \tag{1.2}$$

где R — число формул задающих групповой закон, а D — степень многочленов в формулах. Из работы [71] следует, что всегда существуют системы групповых законов степени $D \leqslant 5$. В работе [72, с. 312] было показано, что такие системы имеют число уравнений $R \in [g+1, 3^g]$. Подставляя эти данные в (1.2) получаем, что

$$\Delta \leqslant 24 \cdot \log 3 \cdot g^2 \left(1 + \frac{1}{g}\right) \max(2g, 1+2\log 5) N 2^N.$$

Таким образом, $\Delta = O(g^3 N 2^N)$ при $g \to \infty$ и, учитывая, что $\Delta + 1 \subset \mathcal{O}(g^3 N 2^N)$, получаем сложность в битовых операциях. При $g \geqslant 2$ имеем $\max(2g, 1 + 2\log 5) \leqslant 3g$, поэтому $\Delta < 172 g^3 N 2^N$. □

Размерность N проективного пространства в общем случае, как минимум, экспоненциальная от размерности абелева многообразия. Например, в случае гиперэллиптических кривых $N = 4^g - 1$ [73]. Поэтому подсчёт точек на общих абелевых многообразиях имеет суперэкспоненциальную сложность от размерности g. Однако, в частном случае якобианов гиперэллиптических кривых задача упрощается — имеем $\Delta = O(g)$ [30; 44], так как в этом случае вместо использования явного представления якобиана как абелева многообразия (используя вложение в проективное пространство), есть возможность использовать групповой закон, работающий в координатах Мамфорда [31]. Кроме того, для многих специальных классов кривых существуют оптимизированные алгоритмы. Текущее состояние сложности решения задачи подсчёта точек на абелевых многообразиях и гиперэллиптических кривых (ГЭК) представлено в Таблице 2 в сравнении с новыми результатами из данной работы. Значение $\mathcal{O}_D$ в таблице обозначает сложность спуска (см. §2.1) с $\mathbb{F}_{q^k}$ в $\mathbb{F}_q$; Δ_1, Δ_2 — экспонента в сложности подсчёта точек для абелевых многообразий A_1, A_2. Предполагается также, что $q \to \infty$.

Таблица 2 — Сложность подсчёта точек на абелевых многообразиях и якобианах гиперэллиптических кривых

g	Условия	Сложность	Ссылки
g	абелево многообразие	$\widetilde{\mathcal{O}}(\log^{\Delta} q), \Delta = \mathcal{O}(g^3 N 2^N)$	[5]
g	ГЭК	$\widetilde{\mathcal{O}}(\log^{\Delta} q), \Delta = \mathcal{O}(g)$	[30]
g	ГЭК с действительным умножением	$\widetilde{\mathcal{O}}(\log^9 q)$	[74]
g	ГЭК, $y^2 = x^{2g+1} + ax^{g+1} + bx$	$\widetilde{\mathcal{O}}(\log^{\Delta} q) + \mathcal{O}_D$, $\Delta = \mathcal{O}(\frac{g}{2})$	§2.3.3
1	ЭК	$\widetilde{\mathcal{O}}(\log^4 q)$	[4; 27]
2	ГЭК	$\widetilde{\mathcal{O}}(\log^8 q)$	[75]
2	ГЭК с действительным умножением	$\widetilde{\mathcal{O}}(\log^5 q)$	[76]
2	ГЭК, $y^2 = x^5 + ax^3 + bx$	$\widetilde{\mathcal{O}}(\log^4 q)$	[37; 39]
3	абелево многообразие A, $A(\mathbb{F}_{q^k}) \sim A_1 \times A_2, k = 2^r \cdot 3^s$	$\widetilde{\mathcal{O}}(\log^{\Delta_1} q^k + \log^{\Delta_2} q^k)$	§2.1.5
3	ГЭК	$\widetilde{\mathcal{O}}(\log^{14} q)$	[64, с. 3]
3	ГЭК с действительным умножением	$\widetilde{\mathcal{O}}(\log^6 q)$	[64]
3	ГЭК, $y^2 = x^7 + ax^4 + ax$	$\widetilde{\mathcal{O}}(\log^4 q)$	§3.1, §3.2
4	абелево многообразие A, $A(\mathbb{F}_{q^k}) \sim A_1 \times A_2, k = 2^r$	$\widetilde{\mathcal{O}}(\log^{\Delta_1} q^k + \log^{\Delta_2} q^k)$	§2.1.6
4	ГЭК	$\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q), \varepsilon \geqslant 0$	[44], §3.3, с. 113
4	ГЭК, $y^2 = x^9 + ax^5 + ax$	$\widetilde{\mathcal{O}}(\log^8 q)$	§3.3

Глава 2. Основные теоретические результаты

2.1 Восстановление характеристического многочлена $\chi_{A,q}$ по χ_{A,q^k}

Пусть A — абелево многообразие размерности g над конечным полем $\mathbb{F}_q$. В ряде случаев задача нахождения характеристического многочлена эндоморфизма Фробениуса χ_A и, соответственно, подсчёта числа точек $\#A = \chi_A(1)$, может быть решена проще над расширением поля $\mathbb{F}_q$, чем над базовым полем. Например, это верно в случае, если A раскладывается над расширением в произведение абелевых многообразий меньшей размерности, но при этом остаётся простым над базовым полем. Тогда мы можем найти характеристический многочлен χ_{A,q^k} и попытаться восстановить по нему многочлен $\chi_{A,q}$. Заметим, что обратная задача проста — зная многочлен $\chi_{A,q}$, можно найти χ_{A,q^k} по известным рекуррентным формулам (см. ниже). По этим же формулам можно составить систему уравнений относительно коэффициентов $\chi_{A,q}$ для решения обратной задачи. Однако, в общем случае решение такой системы не простая задача — асимптотическая сложность решения известными методами, основанными на вычислении базиса Грёбнера — не лучше простого перебора. В данном разделе мы опишем метод решения задачи, основанный на спуске по башне конечных полей, и покажем, в каких случаях задачу можно решить эффективным образом, отличным от простого перебора. Метод основан на работе Сато [37] для якобианов кривых вида $y^2 = x^5 + ax^3 + bx$. Мы обобщаем его на любые абелевы многообразия над конечным полем.

2.1.1 Общая схема

Общий метод нахождения многочлена $\chi_{A,q}$ на основе вычисления χ_{A,q^k} выглядит следующим образом:

1. Вычислить многочлен χ_{A,q^k}.
2. Разложить k на простые множители: $k = k_1 \cdot \ldots \cdot k_s$.

3. Выполнить спуск по башне конечных полей

$$\mathbb{F}_q \subset \mathbb{F}_{q^{k_1}} \subset \mathbb{F}_{q^{k_1 k_2}} \subset \ldots \subset \mathbb{F}_{q^k},$$

последовательно вычисляя $\chi_{A,q^{k/k_s}}$ из χ_{A,q^k}, затем $\chi_{A,q^{k/(k_s k_{s-1})}}$ из $\chi_{A,q^{k/k_s}}$ и так далее пока не получим искомый многочлен $\chi_{A,q}$.

4. Для вычисления многочленов на каждом шаге спуска составить систему уравнений для коэффициентов по рекуррентным формулам (см. ниже) и решить её с помощью методов на основе вычисления базисов Грёбнера или результантов.
5. Для отсева лишних решений уравнений для каждого промежуточного расширения $\mathbb{F}_{q^i}$ использовать условие: $\chi_{A,q^i}(1) = \#A(\mathbb{F}_{q^i})$. Соответственно, выбрать несколько случайных точек P из $A(\mathbb{F}_{q^i})$ и отсеять те кандидаты χ'_{A,q^i} на χ_{A,q^i}, для которых $\chi'_{A,q^i}(1) \cdot P \neq 0$.

Описанная схема позволяет свести задачу нахождения $\chi_{A,q}$ по χ_{A,q^k} к аналогичным задачам для расширений простой степени. Эффективность метода зависит от размера k, сложности вычисления χ_{A,q^k} по сравнению с $\chi_{A,q}$ и сложности выполнения спуска в п. 4 для расширений простой степени. Заметим, что в ряде случаев (для якобианов кривых из последующих глав) можно вместо χ_{A,q^k} вычислить $\chi_{\widetilde{A},q}$, где $\widetilde{A}$ — кручение абелева многообразия A, определённое над $\mathbb{F}_q$, и быстро восстановить χ_{A,q^k} из $\chi_{\widetilde{A},q}$ по рекуррентным формулам (см. далее Лемму 2.1.1).

2.1.2 Составление системы уравнений

Многочлен $\chi_{A,q^k}(T)$ можно получить по многочлену $\chi_{A,q}(T)$ по известным рекуррентным формулам, которые для якобианов кривых можно найти в [10, с. 110] или [48, с. 410]. Приведём данные формулы для случая абелевых многообразий. Обозначим

$$\chi_{A,q^k}(T) = T^{2g} + a_{1,k}T^{2g-1} + \cdots + a_{g,k}T^g + a_{g-1,k}q^k T^{g-1} + \cdots + a_{1,k}q^{(g-1)k}T + q^{gk}.$$

Кроме того, коэффициенты $a_{i,1}$ будем сокращённо обозначать a_i. Если $\chi_{A,q}(T) = \prod_{i=1}^{2g}(T - \lambda_i)$, то известно [20, с. 205], что $\chi_{A,q^k}(T) = \prod_{i=1}^{2g}(T - \lambda_i^k)$. Коэффициенты любого многочлена представляют собой элементарные симметрические

многочлены от его корней с соответствующим знаком [77, Предложение 2.1.4, с. 28]. Тогда

$$a_{1,k} = -\sum_{i=1}^{2g} \lambda_i^k.$$

Применяя формулы Ньютона-Жирара [77, с. 38] для выражения сумм $\lambda_1^k + \ldots + \lambda_{2g}^k$ через суммы вида $a_{1,m} = \lambda_1^m + \ldots + \lambda_{2g}^m$, $m < k$, получаем рекуррентные соотношения:

$$ka_k = a_{1,k} + \sum_{j=1}^{k-1} a_j a_{1,k-j}, \tag{2.1}$$

где $a_0 = 1$, $a_{g+j} = q^j a_{g-j}$ для $j = 1, \ldots, g$ и $a_j = 0$ для $j > 2g$. Или в более подробном виде относительно $a_{1,k}$:

$$a_{1,k} = \begin{cases} ka_k - \sum\limits_{j=1}^{k-1} a_j a_{1,k-j}, & 1 \leqslant k \leqslant g \\ kq^{k-g} a_{2g-k} - \sum\limits_{j=1}^{g} a_j a_{1,k-j} - \sum\limits_{j=1}^{k-1-g} q^j a_{g-j} a_{1,k-g-j}, & g < k \leqslant 2g \\ -\sum\limits_{j=1}^{g} \left(a_j a_{1,k-j} + q^j a_{g-j} a_{1,k-g-j}\right) & k > 2g. \end{cases} \tag{2.2}$$

Для получения выражений для $a_{i,k}$ заменим в формуле (2.1) индекс k на i и расширим поле $\mathbb{F}_q$ до $\mathbb{F}_{q^k}$ (соответственно, a_k становится $a_{i,k}$, а $a_{1,k}$ становится $a_{1,ik}$), получим общую формулу

$$a_{i,k} = \begin{cases} 1, & i = 0 \\ ka_k - \sum\limits_{j=1}^{k-1} a_j \cdot a_{1,k-j}, & i = 1 \\ \frac{1}{i}\left(a_{1,ik} + \sum\limits_{j=1}^{i-1} a_{j,k} \cdot a_{1,(i-j)k}\right), & 1 < i \leqslant g \\ q^{(i-g)k} \cdot a_{2g-i,k}, & g < i \leqslant 2g \\ 0, & i > 2g. \end{cases} \tag{2.3}$$

Из данных рекуррентных формул можно получить следующую оценку сложности для нахождения коэффициентов χ_{A,q^k} по известным коэффициентам $\chi_{A,q}$.

Лемма 2.1.1. *Пусть $\chi_{A,q}$ — характеристический многочлен абелева многообразия размерности g над конечным полем $\mathbb{F}_q$. Тогда многочлен χ_{A,q^k} может быть построен за $\widetilde{\mathcal{O}}(g^3 k^2 \log q)$ битовых операций.*

Доказательство. Для нахождения коэффициента $a_{1,k}$ по формуле (2.2) требуется не более $2g$ умножений при условии, что все $a_{1,j}$ для $j = 1, \ldots, k-1$ уже найдены. Заметим также, что выражения вида $q^j a_{g-j} = a_{g+j}$ уже известны, так как это коэффициенты многочлена $\chi_{A,q}$, который нам известен по условиям леммы. Нахождение всех $a_{1,j}$ для $j = 1, \ldots, k$ занимает время $\leqslant \sum\limits_{j=1}^{k} 2g = 2gk$ умножений.

Коэффициент $a_{i,k}$ для $i = 1, \ldots, g$ можно найти за i умножений и 1 деление при условии, что известны $a_{j,k}$ для $j = 1, \ldots, i-1$ и $a_{1,jk}$ для $j = 1, \ldots, i$. Все коэффициенты $a_{1,jk}$ можно найти за не более чем $2g^2k$ умножений. После их нахождения все $a_{i,k}$ можно найти за $g-1$ деление и не более чем $\sum\limits_{i=2}^{g-1} i = \frac{(g-1)g}{2}$ умножений.

Так как известно, что $|a_{i,k}| \leqslant \binom{2g}{i} q^{\frac{i}{2}k} \leqslant \binom{2g}{g} q^{\frac{g}{2}k}$, то вычисления можно выполнять по модулю простого числа $\ell \geqslant 2\binom{2g}{g} q^{\frac{g}{2}k}$. Одна операция в поле $\mathbb{F}_\ell$ занимает время $\widetilde{\mathcal{O}}(\log \ell)$ (Таблица 1), т. е. $\widetilde{\mathcal{O}}(gk \log q)$ битовых операций. Тогда нахождение χ_{A,q^k} занимает время $2g^2k + \frac{(g-1)g}{2}$ умножений и $g-1$ делений в поле $\mathbb{F}_\ell$ или $\widetilde{\mathcal{O}}(gk(2g^2k + \frac{(g-1)g}{2}) \log q) = \widetilde{\mathcal{O}}(g^3k^2 \log q)$ битовых операций. □

Предположим теперь, что нам известны коэффициенты $a_{1,k}, \ldots, a_{g,k}$. Например, мы их вычислили из разложения абелева многообразия над полем $\mathbb{F}_{q^k}$ с помощью алгоритма Пилэ или специализированных методов для якобианов кривых. Требуется найти $a_1, \ldots, a_g$. Рекуррентное соотношение, выражающее $a_{1,k}$ через $a_1, \ldots, a_g$, задано формулой (2.2), а $a_{i,k}$ для $i \geqslant 2$ задано (2.4). Составим по данным формулам систему уравнений от неизвестных $a_1, \ldots, a_g$.

$$\begin{aligned} a_{1,k} &= ka_k - \sum_{i=1}^{k-1} a_i a_{1,k-i}, \\ 2a_{2,k} &= a_{1,2k} + a_{1,k}^2, \\ 3a_{3,k} &= a_{1,3k} + a_{1,k}a_{1,2k} + a_{2,k}a_{1,k}, \\ &\ldots \\ ga_{g,k} &= a_{1,gk} + \sum_{i=1}^{g-1} a_{i,k} a_{1,(g-i)k}. \end{aligned} \tag{2.4}$$

При этом выражения вида $a_{i,j}$ разворачиваются в многочлены от $a_1, \ldots, a_g$ степени $\deg a_{i,j} = ji$. Сложность построения данной системы задаётся следующей леммой.

Лемма 2.1.2. *Правая часть системы уравнений* (2.4) *в виде многочленов из* $\mathbb{Q}[a_1, \ldots, a_g]$ *может быть построена за время* $\mathcal{O}(gkB \log^2 B \log\log B)$ *операций в* $\mathbb{Q}$, *где* $B = \binom{g(k+1)}{g}$. *В случае, если* g — *фиксированное, имеем* $\widetilde{\mathcal{O}}(k^{g+1})$ *операций в* $\mathbb{Q}$.

Доказательство. Обозначим через $M(d_1, d_2)$ и $A(d_1, d_2)$ сложности умножения и сложения двух многочленов из $\mathbb{Q}[a_1, \ldots, a_g]$ со степенями d_1 и d_2 соответственно. Одно умножение занимает время [78, с. 124, Теорема 1]:

$$M(d_1, d_2) = \mathcal{O}(B \log^2 B \log\log B)$$

операций в поле $\mathbb{Q}$ при использовании в процессе работы алгоритма из [79] для перемножения многочленов от одной переменной. Здесь $B = \binom{d_1+d_2+g}{g}$ — число одночленов в произведении многочленов.

Если хранить многочлены в виде списка одночленов, отсортированного относительно некоторого порядка переменных, то сложение в $\mathbb{Q}[a_1, \ldots, a_g]$ занимает время $A(d_1, d_2) = \binom{\min(d_1,d_2)+g}{g}$ сложений в поле $\mathbb{Q}$. Заметим, что асимптотически $M(d_1, d_2) + A(d_1, d_2) \sim M(d_1, d_2)$. В дальнейшем мы будем использовать данный факт для упрощения оценок.

Для построения правой части (2.4) будем последовательно находить и запоминать в таблице сначала все $a_{1,j}$ для $j = 1, \ldots, gk$, а затем по очереди вычислять и запоминать все $a_{j,k}$ для $j = 2, \ldots, g$.

Имеем $a_{1,1} = a_1, a_{1,2} = 2a_2 - a_1^2$ и так далее. На j-ой итерации имеем $a_{1,j} = ja_j - \sum_{i=1}^{j-1} a_i a_{1,j-i}$, где многочлены $a_{1,j-i}$ уже найдены из предыдущих шагов и $\deg(a_{1,j-i}) = j - i$. Поэтому сложность каждой итерации равна

$$\sum_{i=1}^{j-1} (M(1, j-i) + A(j-i+1, j-i)) \sim (j-1)M(1, j-1).$$

Нахождение всех $j = 1, \ldots, gk$ занимает время $\sim (gk-1)M(1, gk-1)$. Найдём теперь все искомые $a_{j,k}$ для $j = 2, \ldots, g$. Имеем

$$ja_{j,k} = a_{1,jk} + \sum_{i=1}^{j-1} a_{i,k} a_{1,(j-i)k},$$

где многочлены $a_{1,jk}$, $a_{i,k}$ и $a_{1,(j-i)k}$ получены на предыдущих шагах. Поэтому общая сложность нахождения суммы равна:

$$\sum_{i=1}^{j-1} (M(ik,(j-i)k) + A((j-i+1)k,(j-i)k)) \sim (j-1)M(k,(j-1)k).$$

Следовательно, сложность нахождения всех $a_{j,k}$ равна $(g-1)M(k,(g-1)k)$. В итоге получаем общую сложность построения системы (2.4):

$$(gk-1)M(1,gk-1) + (g-1)M(k,(g-1)k) \sim (gk-1)M(k,(g-1)k).$$

□

Подставляя в (2.4) вместо $a_{i,k}$ коэффициенты известного нам многочлена χ_{A,q^k}, получаем систему диофантовых уравнений от g переменных степени gk. Формулы для размерностей $2-6$, полученные по данному методу, приводим в Приложении B.

Замечание. *Для якобианов кривых, есть альтернативный подход для построения системы уравнений, используя следующую формулу [80, с. 195] для L-многочленов (взаимных многочленов к многочленам χ):*

$$L_{C,q^k}(T^k) = \prod_{\zeta^k=1} L_{C,q}(\zeta T). \tag{2.5}$$

В этом случае система уравнений получается сравнением коэффициентов в левой и правой частях. При этом, на практике, степени многочленов и сложность вычисления системы получается хуже, чем составление системы по формулам (2.1) и (2.3). Однако, формула (2.5) может быть полезна для вывода аналитических формул.

2.1.3 Решение системы уравнений

В общем случае диофантовы системы уравнений неразрешимы (десятая проблема Гильберта, алгоритмическая неразрешимость доказана Матиясевичем). Однако у нас есть дополнительные ограничения в виде неравенств для $a_1,\ldots,a_g$ из границы Хассе-Вейля, и систему можно решить, например,

перебором. Для решения нашей системы уравнений могут использоваться методы, основанные на вычислении базисов Грёбнера [81, §2], или последовательное исключение переменных с помощью результантов [81, §3]. Базис Грёбнера может быть вычислен с помощью алгоритмов F_4/F_5 [82; 83], [84, Гл. 10]. Для случая $k = 2^r$ из алгоритмов, основанных на базисах Грёбнера, лучше всего подходит алгоритм M4GB [85], так как он оптимизирован для вычислений базисов Грёбнера систем уравнений второй степени, которые получаются при спуске по расширениям степени 2. Вычисление результантов может быть выполнено с помощью вариации алгоритма Евклида [86, Алгоритм 3.3.7]. Решение системы уравнений данными методами имеет двойную экспоненциальную сложность от g и экспоненциальную сложность от $\log q$. В дальнейшем для частных случаев мы докажем полиномиальную сложность, используя метод результантов. А базисы Грёбнера будем использовать для оценки сложности в общем случае.

Обозначим нашу систему уравнений, составленную в §2.1.2, как

$$h_1 = a_{1,k} - (ka_k - \sum_{i=1}^{k-1} a_i a_{1,k-i}) = 0,$$

$$\dots,$$

$$h_g = ga_{g,k} - (a_{1,gk} + \sum_{i=1}^{g-1} a_{i,k} a_{1,(g-i)k}) = 0.$$

Так как имеются неравенства $|a_i| \leqslant \binom{2g}{i} q^{i/2}$, и нас интересуют только целые решения, то для ограничения роста коэффициентов при вычислениях, мы можем работать в конечном поле $\mathbb{F}_\ell$ для любого простого $\ell \geqslant 2\binom{2g}{g} q^{g/2}$. Используя неравенства, значения $(a_1, \dots, a_g)$ восстанавливаются однозначно по $(a_1, \dots, a_g) \bmod \ell$.

Решением данной системы считаем её преобразование в объединение систем уравнений в треугольной форме или в общем случае в трапециевидной. В первом случае, с точностью до порядка переменных, получаем одну или несколько систем вида:

$$\begin{aligned} \widetilde{h}_1(a_1, \dots, a_g) &= 0, \\ \widetilde{h}_2(a_2, \dots, a_g) &= 0, \\ &\dots \\ \widetilde{h}_{g-1}(a_{g-1}, a_g) &= 0, \\ \widetilde{h}_g(a_g) &= 0. \end{aligned} \tag{2.6}$$

Известно, что любая 0-мерная система уравнений (т. е. система с конечным числом решений над замыканием) из g уравнений от g неизвестных над полем приводится к такому виду [87, с. 121, Proposition 2]. При этом, если соответствующее системе многообразие является неприводимым, то получаем одну систему в треугольной форме, а в случае приводимых многообразий их может быть несколько [88, §2], причём такое представление не уникально.

В случае положительной размерности ситуация сложнее. Но также существует разбиение на трапециевидные системы уравнений и алгоритмы, которые позволяют такое разбиение получить [89, §7].

Для системы в треугольной форме можно быстро найти список решений $(a_1, \ldots, a_g)$ системы. Более точно, сложность получения полного списка решений из треугольной формы задаётся следующим утверждением.

Лемма 2.1.3. *Нахождение решений системы уравнений в форме* (2.6) *над конечным полем* $\mathbb{F}_\ell$ *имеет сложность*

$$\widetilde{\mathcal{O}}(\beta^{g+1} \log^2 \ell)$$

битовых операций, где β *— максимальная степень многочленов в системе.*

Доказательство. Для нахождения списка решений мы получаем список возможных a_g из факторизации последнего многочлена, затем подставляем все значения в предпоследний многочлен, получаем список (a_{g-1}, a_g) из факторизации и повторяем процесс пока не получим полный список решений. При этом для подстановки сразу множества значений в один многочлен от нескольких переменных можно использовать быстрый алгоритм из работы [90].

Для многочлена степени d над конечным полем $\mathbb{F}_q$ сложность факторизации равна $\widetilde{\mathcal{O}}(d^2 \log q)$ операций в поле [70, с. 390, Th. 14.14]. Поэтому факторизация $\widetilde{h}_g(a_g)$ занимает время $\widetilde{\mathcal{O}}\left(\beta^2 \log \ell\right)$ операций в $\mathbb{F}_\ell$.

Выполнив факторизацию, получаем список из не более чем β возможных коэффициентов a_g. Далее подставляем данные значения в $\widetilde{h}_{g-1}(a_{g-1}, a_g)$, факторизуем получившиеся многочлены и получаем список из не более чем β^2 пар (a_{g-1}, a_g). При построении списка из наборов $(a_{g-i}, \ldots, a_g)$ для $i = 1, \ldots, g-1$ требуется выполнить β^{i+1} подстановок в многочлен от $g - i + 1$ неизвестных и факторизаций получившегося многочлена от одной переменной степени β.

В итоге получаем список из не более чем β^g наборов $(a_1, \ldots, a_g)$, выполнив на последнем шаге β^{g-1} подстановок и факторизаций.

Вычисление подстановок N точек $(x'_1, \ldots, x'_g) \in \mathbb{F}_\ell^g$ в многочлен из $\mathbb{F}_\ell[x_1, \ldots, x_n]$ общей степени d и частичных степеней $d_1 - 1, \ldots, d_n - 1$ по каждой переменной занимает время [90, с. 19, Th. 1]:

$$(1 + o(1))^n (N + (\varphi \log \varphi)^n) \widetilde{\mathcal{O}}(n^2 \varphi^5 \log \ell),$$

где $\varphi = \min(d_1 + \ldots + d_n, d + 1 + \lceil \log_2 \binom{d+n-1}{n-1} \rceil)$. Или для $n < d^{o(1)}$ [91, с. 150, Cor. 3.3]:

$$((d^n + N) \log \ell)^{1+o(1)} \tag{2.7}$$

битовых операций.

Если хранить многочлены $\widetilde{h}_1, \widetilde{h}_2, \ldots, \widetilde{h}_g$ как элементы колец $\mathbb{F}_\ell[a_1][a_2, \ldots, a_g]$, $\mathbb{F}_\ell[a_2][a_3, \ldots, a_g]$, $\ldots$, $\mathbb{F}_\ell[a_g]$, то подстановка набора $(a_{g-i+1}, \ldots, a_g)$ в многочлен $\widetilde{h}_{g-i}(a_{g-i}, \ldots, a_g)$ представляет собой проход по коэффициентам при переменной a_{g-i} с подстановкой набора в многочлен от i переменных $a_{g-i+1}, \ldots, a_g$. Подставляя в (2.7) вместо d степень многочлена $\widetilde{h}_{g-i}$, равную β, в переменную N — число наборов $(a_{g-i-1}, \ldots, a_g)$, равное β^i, а также умножая получившуюся формулу на число коэффициентов многочлена $\widetilde{h}_{g-i}$ при переменной a_{g-i}, равное β, получаем время построения списка многочленов от одной переменной для последующей факторизации:

$$\gamma_i = \beta \left(\left(\beta^i + \beta^i \right) \log \ell \right)^{1+o(1)} = \beta^{i(1+o(1))+1} (2 \log \ell)^{1+o(1)}$$

битовых операций.

Факторизация многочленов занимает время $\widetilde{\mathcal{O}}(\beta^2 \log \ell)$ операций в поле $\mathbb{F}_\ell$, умноженное на количество многочленов β^i, всего

$$\widetilde{\mathcal{O}}(\beta^{i+2} \log \ell)$$

операций в поле $\mathbb{F}_\ell$ или $\widetilde{\mathcal{O}}(\beta^{i+2} \log^2 \ell)$ битовых операций. Последняя подстановка и факторизация занимает время

$$\gamma_{g-1} + \widetilde{\mathcal{O}}(\beta^{g+1} \log^2 \ell) = \widetilde{\mathcal{O}}(\beta^{g+1} \log^2 \ell)$$

и имеет наибольший порядок среди всех подстановок и факторизаций. Поэтому асимптотически время получения списка наборов $(a_1, \ldots, a_g)$ равно времени работы последней подстановки и факторизации. □

Степень β известна для базисов Грёбнера (см. ниже). Для нахождения размерности (в отличии от треугольной формы) достаточно найти базис Грёбнера относительно легковесного порядка переменных $grevlex$ (см. [92, с. 159, Corollary 11.14]). В нашем случае при фиксированных g, q, и k экспериментально (например, в системе компьютерной алгебры Magma [93]) можно убедится, что для случайно выбранной гиперэллиптической кривой соответствующая система уравнений будет практически всегда 0-мерной.

Далее будем использовать эвристическое предположение, что наша система 0-мерная и может быть представлена одной системой в треугольной форме. Заметим, что в 0-мерном случае получить полный список треугольных систем, которому эквивалентна исходная система, можно из базиса Грёбнера в lex-порядке переменных, применив алгоритм Лазара [87, §7]. Но в наших вычислениях это не потребовалось.

Рассмотрим теперь подробнее методы нахождения треугольной формы.

Базисы Грёбнера

Для исключения переменных и приведения системы в треугольную форму используется вычисление базиса Грёбнера относительно лексикографического порядка переменных. Так как вычисление такого базиса напрямую трудоёмко, используем следующий стандартный подход. Сначала вычисляем базис Грёбнера относительно $grevlex$-порядка с помощью алгоритма F_5, а затем переводим его в лексикографический порядок с помощью алгоритма $FLGM$ [94] для размерности 0 или Gröbner-Walk [95; 96] для положительной размерности. При этом размерность становится известной сразу после нахождения базиса Грёбнера в $grevlex$-порядке.

Базис Грёбнера относительно $grevlex$-порядка для системы из g уравнений степени d от g неизвестных может быть вычислен (с учётом гомогенизации) с помощью алгоритма F_5 за время $\mathcal{O}(gd\binom{g+d}{d}^{\omega})$ [97, Prop. 1] операций в поле, где ω — экспонента матричного умножения над $\mathbb{F}_\ell$. Так как у нас $d = gk$, имеем $\binom{g+d}{d}^{\omega} = \binom{g(1+k)}{gk}^{\omega} < \left(\frac{(1+k)e}{k}\right)^{gk\omega} < e^{g\omega(1+k)}$ и вычисление базиса Грёбнера за время $\mathcal{O}(g^2ke^{g\omega(k+1)}) = \mathcal{O}(e^{gk\omega(1+\frac{1}{k})(1+\frac{\log(g^2k)}{k+1})})$ операций в поле. Так

как $k \geqslant 2$ и $\max\left\{\frac{\log(g^2k)}{k+1}\right\} = \frac{1}{e}$ получаем итоговую сложность $\mathcal{O}(2^{gk\omega\varepsilon_1})$, где $\varepsilon_1 = 1.5(1+\frac{1}{e})\ln 2 \approx 1.422$. Или, если положить $g \leqslant \log q$ и перевести в битовые операции: $\mathcal{O}(2^{gk\omega\varepsilon_1} g\log q(\log(g\log q))^{2+o(1)}) = \widetilde{\mathcal{O}}(2^{gk\varepsilon_2}\log q)$, где $\varepsilon_2 = \omega\varepsilon_1 + \frac{1}{2e\ln 2} \approx 3.639$ для $\omega = 2.37286$ [98].

После вычисления базиса относительно *grevlex*-порядка становится известна размерность [92, с. 159, Corollary 11.14], и мы можем применить один из алгоритмов для конвертации базиса.

Алгоритм *FLGM* позволяет выполнить конвертацию базиса в лексикографический порядок за время $(g+1)d^{3(g+1)}$ операций в поле. При этом конвертация базиса не влияет на общую сложность вычисления базиса Грёбнера в лексикографическом порядке переменных, которая равна в этом случае сложности вычисления базиса в *grevlex*-порядке [97, с. 53]. Для Gröbner-Walk каких-то хороших оценок сложности не известно, есть только оценки для степеней уравнений [99], как и в случае прямого вычисления базиса Грёбнера относительно лексикографического порядка переменных.

Предположим, что в результате получается базис Грёбнера, содержащий систему в треугольной форме (наиболее частый случай). Сложность получения полного списка решений тогда можно найти по Лемме 2.1.3. Имеем $\beta = 2\left(\frac{d^2}{2}+d\right)^{2^{g-1}}$ [100, Th. 2], если базис получен из системы многочленов степени d. В нашем случае $d = gk$ для $g \geqslant 1$ и $k \geqslant 2$, поэтому:

$$\beta = 2\left(\frac{(gk)^2}{2}+gk\right)^{2^{g-1}} = 2\left(\frac{(gk)^2}{2}\left(1+\frac{2}{gk}\right)\right)^{2^{g-1}} \leqslant 2(gk)^{2^g}.$$

Следовательно, общая сложность нахождения решений системы уравнений в треугольной форме равна $\widetilde{\mathcal{O}}(\beta^{g+1}\log^2\ell) = \widetilde{\mathcal{O}}(2^{g+1}(gk)^{2^g(g+1)}\log^2\ell) = \widetilde{\mathcal{O}}(2^{g+1+\log(gk)2^g(g+1)}\log^2\ell)$ битовых операций. Так как $g \geqslant 1$, $k \geqslant 2$ и $\ell = \mathcal{O}(g\log q)$ получаем:

$$\widetilde{\mathcal{O}}(2^{2^g g\log(gk)\varepsilon_3}\log^2 q)$$

битовых операций, где $\varepsilon_3 = \left(1+\frac{1}{g}+\frac{1}{2^g\log(gk)}+\frac{1}{g2^g\log(gk)}+\frac{2\log g}{g2^g\log(gk)}\right) \approx 3.25012$.

Складывая сложности всех шагов, получаем оценку сложности нахождения списка решений для случая, когда система приводится в треугольный вид и имеет ненулевую размерность:

$$\widetilde{\mathcal{O}}\left(2^{gk\varepsilon_2}\log q + C_{gw}(g,\beta) + 2^{2^g g\log(gk)\varepsilon_3}\log^2 q\right),$$

где $C_{gw}(g, \beta)$ — сложность выполнения Gröbner-Walk для системы многочленов от g неизвестных степени $\beta = 2\left(\frac{(gk)^2}{2} + gk\right)^{2^{g-1}}$. Это ведёт к следующей итоговой оценке сложности для нахождения решений нашей системы уравнений.

Лемма 2.1.4. *Пусть система уравнений (2.4) имеет положительную размерность и приводится к треугольной форме, тогда сложность нахождения всех её решений равна:*

$$\widetilde{\mathcal{O}}\left(2^{g^2k2^g\varepsilon}\log^2 q + C_{gw}(g,\beta)\right)$$

битовых операций, где $\varepsilon = 3.545$.

Доказательство. Имеем

$$\widetilde{\mathcal{O}}\left(2^{gk\varepsilon_2}\log q + C_{gw}(g,\beta) + 2^{2^g g\log(gk)\varepsilon_3}\log^2 q\right) = \widetilde{\mathcal{O}}\left(2^{gk\varepsilon_2 + 2^g g\log(gk)\varepsilon_3}\log^2 q + C_{gw}(g,\beta)\right).$$

Далее: $gk\varepsilon_2 + 2^g g\log(gk)\varepsilon_3 = g^2k2^g\left(\frac{\varepsilon_2}{g2^g} + \frac{\log(gk)}{gk}\varepsilon_3\right) \leqslant g^2k2^g\left(\frac{\varepsilon_2}{2} + \frac{\varepsilon_3}{e\ln 2}\right) = \varepsilon g^2k2^g$, где $\varepsilon \approx 3.545$. □

Когда система имеет размерность 0, затраты на конвертацию базиса не влияют на общую сложность, поэтому оценка сложности решения системы следующая.

Лемма 2.1.5. *Пусть параметр g фиксирован. Если система уравнений (2.4) имеет размерность 0, то сложность нахождения всех её решений равна:*

$$\widetilde{\mathcal{O}}\left(2^{g^2k2^g\varepsilon}\log^2 q\right)$$

битовых операций, где $\varepsilon = 3.545$.

Как видим, в самом частом случае сложность решения системы уравнений полиномиальная от $\log q$, двойная экспоненциальная от g и экспоненциальная от k.

Метод результантов

Рассмотрим метод результантов более подробно. Вычисляя последовательность $\mathrm{Res}_{a_1}(h_1, h_2), \ldots, \mathrm{Res}_{a_1}(h_1, h_g)$ и заменяя $h_2, \ldots, h_g$ на результат

вычислений, получаем систему из g уравнений, в которой переменная a_1 присутствует только в первом уравнении. Аналогичным образом можно исключить из системы переменные $a_2, \ldots, a_{g-1}$. При этом система уравнений преобразуется к виду, в котором первое уравнение содержит переменные $a_1, \ldots, a_g$, второе уравнение — переменные $a_2, \ldots, a_g$ и так далее. Последнее уравнение зависит только от переменной a_g, то есть является многочленом от одной переменной. Так как a_g — целое число и $|a_g| \leqslant \binom{2g}{g} q^{g/2}$, то найти корни многочлена можно факторизацией в конечном поле $\mathbb{F}_\ell$, где ℓ — достаточно большое простое число. Если выбрать $\ell = 2\binom{2g}{g} q^{g/2}$, то a_g восстанавливается однозначно по $a_g \pmod{\ell}$. Найдя список возможных a_g (при таком выборе ℓ существует только одно целое число сравнимое с $a_g \bmod \ell$), подставляем их в предыдущее уравнение нашей системы, которое зависит только от a_{g-1} и a_g, получаем многочлены от переменной a_{g-1}, находим их корни с помощью факторизации и повторяем процесс пока не закончатся уравнения. В результате получается список возможных решений $(a_1, \ldots, a_g)$.

Заметим, что при исключении переменной a_i таким способом, мы получаем элемент из первого исключающего идеала $I_1 = \langle h_s, h_r \rangle \cap \mathbb{Q}[a_1, \ldots, \hat{a}_i, \ldots, a_g]$ [84, с. 167, (8)]. При этом не гарантируется, что этот элемент будет генератором идеала, в отличии от нахождения базиса Грёбнера относительно lex-порядка, который даёт нам образующие идеала I_1.

Поэтому алгоритмы с решением систем уравнений на основе результантов по своей природе вероятностные. Тем не менее, описанный метод результантов используется во многих известных алгоритмах подсчёта точек (см., например, [44; 75]) и общей оценке сложности для гиперэллиптических кривых [30, Proposition 5].

Выбор истинного решения

В результате решения системы уравнений методом результантов или вычислением базиса Грёбнера получается список решений, состоящий из наборов $(a_1, \ldots, a_g)$, из которого только одно решение истинно. Для нахождения истинного решения используем следующий стандартный эвристический метод, который используется с той же целью, например, в методе комплексного умно-

жения [48, с. 463]. Проверяем выполнение соотношения

$$[N]P = 0$$

для $N = 1+a_1+\ldots+a_g+a_{g-1}q+\ldots+a_1q^{g-1}+q^g$ и случайно выбранных точек P абелева многообразия A. Последнее соотношение должно выполняться для всех точек абелева многообразия, так как $\#A(\mathbb{F}_q) = \chi_{A,q}(1) = 1+a_1+\ldots+a_g+a_{g-1}q+\ldots+a_1q^{g-1}+q^g$. Если выбрать достаточно большое количество случайных точек, то в списке решений системы останется в большинстве случаев одно решение. Более точную оценку даёт следующая лемма.

Лемма 2.1.6. *Пусть A — абелево многообразие размерности g; $P_1, \ldots, P_s$ — случайные точки, равномерно распределённые в A, $s \geqslant 2$ и пусть $N_1, \ldots, N_m$ — целые числа, равномерно распределённые на отрезке $[(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$, и $m \geqslant 2$. Если $r = HOK(\operatorname{ord} P_1, \ldots, \operatorname{ord} P_s)$, то с вероятностью больше $\frac{1}{\zeta(s)}$ имеем $r \geqslant \sqrt{q}-1$. Кроме того, при $r \geqslant \sqrt{q}-1$ вероятность выполнения условия $[N_i]P_j = 0$ для всех $1 \leqslant j \leqslant s$ и $1 \leqslant i \leqslant m$ равна*

$$O\left(\frac{m}{\zeta(m)\sqrt{q}^{m-1}}\right)$$

при $q \to \infty$. Здесь $\zeta(s)$ и, соответственно $\zeta(m)$, — дзета-функция Римана.

Доказательство. Пусть G — любая конечная абелева группа и $\alpha_1, \ldots, \alpha_s$ — случайно выбранные равномерно распределённые элементы группы. Пусть также $r = \mathrm{HOK}(\operatorname{ord}\alpha_1, \ldots, \operatorname{ord}\alpha_s)$ и $\lambda(G)$ — экспонента группы G, т. е. целое число λ такое, что $[\lambda]\alpha = 0$ для любого элемента $\alpha \in G$. Тогда выполняется следующее неравенство:

$$\mathrm{Prob}(r = \lambda(G)) > \frac{1}{\zeta(s)}. \tag{2.8}$$

Случай $s = 2$ неравенства (2.8) — Теорема 8.1 из работы [101]. Случай $s > 2$ следует из [101, (8.6), с. 131]. Более того, для абелевого многообразия A имеем $\lambda(A) \geqslant \sqrt{q}-1$ (для якобианов — [48, с. 411], случай абелевых многообразий можно доказать аналогичным образом).

Чтобы выполнялось условие $[N_i]P_j = 0$ для всех $1 \leqslant j \leqslant s$ и $1 \leqslant i \leqslant m$, необходимо выполнение условия $\operatorname{ord} P_j \mid N_i$ для всех $1 \leqslant j \leqslant s$ и $1 \leqslant i \leqslant m$, или $r = \mathrm{HOK}(\operatorname{ord} P_1, \ldots, \operatorname{ord} P_s)$ должно делить одновременно все N_i.

Из неравенства 2.8 с вероятностью $> \frac{1}{\zeta(s)}$ наименьшее общее кратное r от порядков точек $P_1, \ldots, P_s$ равно экспоненте A и, в этом случае числа $N_1, \ldots, N_m$

должны иметь общий множитель $\geqslant \sqrt{q}-1$, чтобы выполнялось условие $[N_i]P_j = 0$. Оценим вероятность последнего условия.

Вероятность, что m целых чисел, равномерно распределённых на отрезке $[1, n]$, имеют наибольший общий делитель d стремится к $\frac{1}{d^m\zeta(m)}$ при $n \to \infty$ (для $d = 1$ доказательство в [102], для общего случая — [103]). К такому же значению стремится вероятность для m-чисел распределённых на отрезке $[a, b]$ в случае, если длина данного отрезка стремится к ∞. Следовательно, вероятность, что m-чисел из интервала Хассе-Вейля имеют наибольший общий делитель $d \geqslant \sqrt{q} - 1$, равна

$$p_1 = \sum_{d=\sqrt{q}-1}^{(\sqrt{q}+1)^{2g}} \frac{1}{d^m\zeta(m)} = \frac{1}{\zeta(m)} \cdot \left(\zeta(m, \sqrt{q} - 1) - \zeta(m, (\sqrt{q} + 1)^{2g} + 1)\right),$$

где $\zeta(m, a) = \sum\limits_{i=0}^{\infty} \frac{1}{i^m}$ — дзета-функция Гурвица. Применяя известные асимптотические оценки [104, (1.3)] для дзета-функции Гурвица, получаем $p_1 = \mathcal{O}\left(\frac{m}{\sqrt{q}^{m-1}\zeta(m)}\right)$ при $q \to \infty$. Имеем теперь

$$\mathrm{Prob}(d \geqslant \sqrt{q} - 1 \ \cap \ r \mid d) \leqslant \min\left(\mathrm{Prob}(d \geqslant \sqrt{q} - 1), \mathrm{Prob}(r \mid d)\right) \leqslant \mathrm{Prob}(d \geqslant \sqrt{q} - 1)$$

из чего и следует утверждение в лемме. □

Из леммы следует, что для отсева лишних решений системы (2.4) в случае, если соответствующие им $N_1, \ldots, N_m$ равномерно распределены, при больших значениях q, достаточно взять 10 случайных точек. Тогда в $\frac{1}{\zeta(10)} \approx 99.9\%$ случаев вероятность прохождения теста скалярным умножением довольно быстро стремится к нулю уже при $m = 2$. В случае $m > 2$ вероятность ещё меньше. Заметим, что m чисел, равномерно распределённых в границах Хассе-Вейля, с вероятностью $\frac{1}{\zeta(m)}$ будут взаимнопростыми, поэтому с ростом m вероятность прохождения теста стремится к 0.

Однако, множество решений $(a_1, \ldots, a_g)$ системы (2.4) включает в себя решения, соответствующие кручениям степени k абелева многообразия A. Распределение таких решений можно получить из гипотезы Сато-Тэйта. Для размерности 2 распределение нормализованных коэффициентов характеристического многочлена получено в [105, Таблица 5], введение в общий случай можно найти в [106], но точное распределение в общем случае неизвестно. Кроме того, в процессе решения системы могут появляется ложные решения (известная проблема для метода результантов), распределение которых неизвестно.

В связи с этим нам остаётся только полагаться на следующее эвристическое предположение.

Эвристика 2.1.1. Пусть A — случайно выбранное абелево многообразие над конечным полем $\mathbb{F}_q$ и $N_1, \ldots, N_m$ — целые числа, соответствующие решениям системы (2.4) для некоторого $k \geqslant 2$. Если $P_1, \ldots, P_s$ — случайно (равномерно) выбранные точки из A и $s \geqslant 2$, то вероятность выполнения условия $[N_i]P_j = 0$ для всех $1 \leqslant i \leqslant m$ и $1 \leqslant j \leqslant s$ стремится к 0 при $q \to \infty$.

Заметим, что эвристика выполняется только для случайных[1] абелевых многообразий и больших значений q. Существуют специальные виды абелевых многообразий, в частности, не простые, для которых эвристика не всегда работает. Однако, такие случаи встречаются редко относительно общего количества многообразий (для приводимых абелевых поверхностей оценки есть в [107]).

В общем случае, метод с умножением точки на число позволяет гарантировано найти большой делитель r числа точек $\#A$ и эвристически с большой вероятностью — само число $\#A$ или характеристический многочлен. Поэтому алгоритмы на его основе по своей природе являются вероятностными и эвристическими. Для отдельных размерностей ($g = 2, 3$) и при наличии у A квадратичного кручения $\widetilde{A}$ для избавления от эвристических предположений можно воспользоваться Леммой 4 из работы [108], которая позволяет определить χ_{A_q} уникальным образом по $\chi_{\mathcal{A}_q}(1)$ и $\chi_{\mathcal{A}_q}(-1)$ (умножая кандидаты на порядок групп A, $\widetilde{A}$ на точки из A и $\widetilde{A}$ для определения $\chi_{\mathcal{A}_q}(1)$, $\chi_{\mathcal{A}_q}(-1)$ с последующим применением Леммы 4).

2.1.4 Спуск

Теперь у нас есть всё необходимое для нахождения $\chi_{A,q}$ по χ_{A,q^k}. Если степень расширения k не простая, то, в соответствии с общей схемой из §2.1.1, мы можем решать систему уравнений, спускаясь по расширениям простой степени d, где $d \mid k$, т. е. относительно $A(\mathbb{F}_{q^{k/d}})$ и $A(\mathbb{F}_{q^k})$, как это сделано в работе [37] для якобианов гиперэллиптических кривых рода 2. Это существенно

[1] англ. «generic»

упрощает задачу, так как при вычислении результантов (или базисов Грёбнера) получаются уравнения большой степени. Следующий алгоритм может быть применён рекурсивно на каждом шаге спуска по расширениям конечного поля.

Алгоритм 1: Вычисление характеристического многочлена $\chi_{A,q}(T)$ по заданному $\chi_{A,q^k}(T)$.

Input: Абелево многообразие A над $\mathbb{F}_q$, характеристический многочлен $\chi_{A,q^k}(T)$.

Output: Список возможных коэффициентов $(a_1, ..., a_g)$ многочлена $\chi_{A,q}(T)$.

1 $\ell \leftarrow \text{nextprime}(\lceil (2\binom{2g}{g} q^{g/2} \rceil + 1)$;

2 Составить систему уравнений $\{h_1 = 0, ..., h_g = 0\}$ от неизвестных $a_1, ..., a_g$ над полем $\mathbb{F}_\ell$ по формулам (2.4);

3 Решить систему уравнений над полем $\mathbb{F}_\ell$ и построить список L возможных наборов $(a_1, ..., a_g)$, используя неравенства $|a_i| \leqslant \binom{2g}{i} q^{\frac{i}{2}}$;

4 Исключить из L решения, которые не удовлетворяют условию $[N]P = 0$ для нескольких случайно выбранных $P \in A(\mathbb{F}_q)$ и $N = 1 + a_1 + ...a_g + a_1 q + ... + a_g q^g$;

return L;

Теорема 2.1.7. *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*

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

битовых операций, где $\varepsilon = 3.545$, $\varepsilon' = 1.766$, 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 система (2.4) имеет размерность 0, полагаем $C_{gw} = 0$.

Доказательство. Для доказательства теоремы выполним анализ сложности Алгоритма 1. На Шаге 3 алгоритма требуется решать систему из g уравнений от g неизвестных степени k над конечным полем размера $\mathcal{O}(\binom{2g}{g} q^{g/2})$. Кроме того, в общем случае решать g-мерную систему уравнений требуется для нахождения случайной точки P на Шаге 4. Заметим, что для якобианов гиперэллиптических

кривых последняя задача не представляет особой сложности, так как она эквивалентна извлечению константного числа квадратных корней в поле и может быть выполнена за полиномиальное время.

В общем случае не известно оценок сложности для решения таких систем над простым конечным полем, лучших чем простой перебор (для непростых конечных полей есть лучший алгоритм [109]), за исключением систем уравнений размерности 0. Это связано с тем, что для систем уравнений положительной размерности не известны условия, при которых базис Грёбнера системы имеет треугольную форму, отличные от добавления в систему многочленов вида $x^q - x$. Из-за чего после вычисления базиса Грёбнера для получения всех решений может потребоваться полный перебор значений нескольких переменных. Тем не менее, базисы Грёбнера и результанты на практике позволяют упростить решение и получить некоторые точные оценки сложности для частных случаев. Рассмотрим подробно шаги алгоритма.

Шаг 1. Из теоремы о распределении простых чисел следует, что выбор простого числа ℓ может быть выполнен за $\mathcal{O}(g \log q)$ попыток. Тесты на простоту имеют полиномиальную сложность (см. [110]).

Шаг 2. Согласно Лемме 2.1.2 система может быть составлена за время $\widetilde{\mathcal{O}}\left(gk\binom{g(k+1)}{g}\right)$ операций в $\mathbb{F}_\ell$. При этом степени уравнений в системе $\leqslant gk$. Так как для любых целых чисел a, b имеем $\binom{a}{b} < \left(\frac{a\,\mathrm{e}}{b}\right)^b$ при $1 \leqslant b \leqslant a$, то $\binom{g(k+1)}{g} < ((k+1)\,\mathrm{e})^g = k^{g(1+o(1))}$. Следовательно, сложность шага равна $\widetilde{\mathcal{O}}(k^{g(1+o(1))})$ операций в $\mathbb{F}_\ell$. Чтобы получить сложность в битовых операциях, можно аналогичным образом показать, что $\ell = \mathcal{O}(2^{g(1+\log_2 \mathrm{e})+o(1)} q^{\frac{g}{2}})$ и $\log \ell = \mathcal{O}(g \log q)$. Тогда получаем сложность шага $\widetilde{\mathcal{O}}(k^{g(1+o(1))} \log q)$ битовых операций.

Шаг 3. В соответствии с Леммами 2.1.4 и 2.1.5 имеем сложность решения системы уравнений

$$\widetilde{\mathcal{O}}\left(2^{2^g g^2 k\varepsilon} \log^2 q + C_{gw}(g, \beta)\right)$$

в случае положительной размерности и

$$\widetilde{\mathcal{O}}\left(2^{2^g g^2 k\varepsilon} \log^2 q\right)$$

в случае размерности 0.

Шаг 4. Выбор случайной точки в общем случае непростая задача, так как требуется решать систему уравнений размерности g. Однако, для якобианов гиперэллиптических кривых эта задача эквивалентна извлечению g квадратных

корней и поэтому может быть решена за время $\widetilde{\mathcal{O}}(g\log^2 q)$ битовых операций. Обозначим сложность группового закона на абелевом многообразии как S битовых операций, а сложность нахождения случайной точки как R битовых операций. Из границы Хассе-Вейля следует, что $N = \mathcal{O}(q^g)$, поэтому умножение случайной точки на число занимает $\mathcal{O}(\log N) = \mathcal{O}(g\log q)$ сложений на абелевом многообразии при использовании быстрых алгоритмов скалярного умножения. Поэтому общая сложность шага равна $\mathcal{O}(R + gS\log q)$. Заметим, что нам не обязательно нужно перебирать весь список наборов $(a_1, \ldots, a_g)$, исключение решений может быть выполнено на предыдущем шаге сразу при нахождении набора $(a_1, \ldots, a_g)$, поэтому при получении общей оценки алгоритма мы можем включить сложность данного шага в оценку предыдущего. По Лемме 2.1.6 и принимая Эвристику 2.1.1 достаточно взять 10 точек для отсева лишних решений на каждом шаге с вероятностью 99,9%.

Складывая сложность всех шагов, получаем оценку времени работы алгоритма для случая, когда система приводится в треугольный вид и имеет ненулевую размерность:

$$\widetilde{\mathcal{O}}\left(k^{g(1+o(1))}\log q + 2^{2^g g^2 k\varepsilon}\log^2 q + C_{gw}(g,\beta) + R + g\beta^{g-1}S\log q\right),$$

где $\beta = 2\left(\frac{(gk)^2}{2} + gk\right)^{2^{g-1}} \leqslant 2(gk)^{2^g}$. Соответственно, имеем $\beta^{g-1} \leqslant 2^{2^g g\log_2(gk)\varepsilon_4}$ для $\varepsilon_4 = 1.5$ и $g\beta^{g-1} \leqslant 2^{2^g g\log_2(gk)\varepsilon'}$ для $\varepsilon' = \varepsilon_4 + \frac{1}{2e\ln 2} \approx 1.765$.

Опуская части малого порядка и подставляя значение $g\beta^{g-1}$, получаем следующую оценку:

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

В случае, когда система имеет размерность 0, затраты на конвертацию базиса не влияют на общую сложность, поэтому можно положить $C_{gw}(g,\beta) = 0$. □

Как видно из оценки, сложность спуска растёт как двойная экспоненциальная функция от размерности g и экспоненциальная функция от степени k, т. е. очень быстро. При этом мы рассматриваем благоприятный случай, когда соответствующая система уравнений приводится в треугольную форму. Поэтому на практике такой спуск осуществим только для небольших значений k и g. Далее в частных случаях мы докажем более точные оценки без допущений и приводимости в треугольную форму. В частности, покажем, что спуск можно

эффективно выполнить для $g = 3, k = 2^r 3^s$ и $g = 4, k = 2^s$. Для гиперэллиптических кривых рода 2 и $k = 2^r 3^s$ эта задача была решена в [37; 39]. Заметим, что в случае размерности 2 согласно классификации из [111] максимальная степень расширения поля, над которым обычное абелево многообразие разложимо, не превышает 6. Поэтому случай $k = 2^s \cdot 3^r$ покрывает все обычные геометрически разложимые абелевы многообразия размерности 2.

2.1.5 Случай $g = 3, k = 2^r \cdot 3^s$

Пусть A — абелево многообразие размерности 3 над конечным полем $\mathbb{F}_q$ и пусть $k = 2^r 3^s$. Рассмотрим решение систем уравнений в Алгоритме 1 для спуска по расширениям степеней 2, 3 и, соответственно, получения характеристического многочлена $\chi_{A,q}$ из χ_{A,q^k}.

Расширения степени 2. По формулам (2.4) получаем систему уравнений:

$$\begin{aligned} h_1 &= a_{1,2} - 2a_2 + a_1^2 = 0, \\ h_2 &= a_{2,2} - 2a_2 q + 2a_1 a_3 - a_2^2 = 0, \\ h_3 &= a_{3,2} - 2q^3 + 2a_1^2 q^2 - 2a_2^2 q + a_3^2 = 0, \end{aligned} \tag{2.9}$$

где $a_{1,2}$, $a_{2,2}$ и $a_{3,2}$ — известны. Выражаем a_2 из h_1 и подставляем в h_2, h_3, получаем:

$$h_2 = a_{1,2}(4q + 2a_1^2) + 4a_1^2 q - 8a_1 a_3 - 4a_{2,2} + a_{1,2}^2 + a_1^4 = 0$$

и

$$h_3 = 4q^3 - 4a_1^2 q^2 + a_{1,2}^2 q + 2a_1^2 a_{1,2} q + a_1^4 q - 2a_{3,2} - 2a_3^2 = 0.$$

Исключая переменную a_3 из h_3 вычислением результанта $\mathrm{Res}_{a_3}(h_2, h_3)$, получаем многочлен 8 степени от переменной a_1:

$$\begin{aligned} h_{23} =& a_1^8 - a_1^6(24q - 4a_{1,2}) - a_1^4(-144q^2 + 40a_{1,2}q + 8a_{2,2} - 6a_{1,2}^2) - \\ & - a_1^2(128q^3 - 32a_{1,2}q^2 + 32a_{2,2}q + 8a_{1,2}^2 q - 64a_{3,2} + 16a_{1,2}a_{2,2} - 4a_{1,2}^3) + \\ & + (4a_{1,2}q - 4a_{2,2} + a_{1,2}^2)^2. \end{aligned}$$

Для получения полного списка решений (2.9) мы факторизуем многочлен h_{23} над конечным полем $\mathbb{F}_\ell$ ($\ell > 2\binom{2g}{g} q^{g/2}$ — простое число), получив список

из не более чем 8 возможных значений a_1, так как в многочлене h_{23} значения $a_{1,2}, a_{2,2}, a_{3,2}, q$ известны и он имеет степень 8 относительно a_1. Затем мы подставляем каждое значение в многочлен h_1, получая значение a_2. Таким образом, у нас получается список из не более чем 8 пар (a_1, a_2). Для нахождения значений a_3 подставляем каждую пару в h_3 и извлекаем квадратный корень. Так как может быть всего до двух квадратных корней, в итоге получается список из не более чем 16 троек (a_1, a_2, a_3).

Таким образом, спуск для расширений степени 2 сводится к факторизации многочлена степени 8 и извлечению квадратного корня.

Расширения степени 3. В данном случае по формулам (2.4) получаем систему уравнений:

$$\begin{aligned} h_1 &= a_{1,3} - (a_1^3 - 3a_1a_2 + 3a_3) = 0, \\ h_2 &= a_{2,3} - (3a_1^2a_2q - 3a_1^2q^2 + a_2^3 - 3a_1a_2a_3 - 3a_2^2q + 3q^3 + 3a_3^2) = 0, \\ h_3 &= a_{3,3} - (6a_1a_2^2q^2 - 3a_1^2a_3q^2 - 6a_1a_2q^3 - 3a_2^2a_3q + 6a_3q^3 + a_3^3) = 0, \end{aligned} \tag{2.10}$$

где $a_{1,3}$, $a_{2,3}$ и $a_{3,3}$ — известны. Выражая a_3 в h_1 и подставляя в h_2, h_3 получаем:

$$h_2 = 9q^3 - 9a_1^2q^2 - 9a_2^2q + 9a_1^2a_2q - 3a_{2,3} + 3a_2^3 + 3a_1a_{1,3}a_2 - 3a_1^4a_2 + a_{1,3}^2 - 2a_1^3a_{1,3} + a_1^6 = 0$$

и

$$\begin{aligned} h_3 = &- a_1^9 + 9a_1^7a_2 + 3a_1^6a_{1,3} + a_1^5(27q^2 - 27a_2^2) - 18a_1^4a_{1,3}a_2 \\ &+ a_1^3(-54q^3 - 81a_2q^2 + 27a_2^2q + 27a_2^3 - 3a_{1,3}^2) + a_1^2(27a_{1,3}a_2^2 - 27a_{1,3}q^2) \\ &+ a_1(162a_2^2q^2 - 81a_2^3q + 9a_{1,3}^2a_2) - 27a_{1,3}a_2^2q - 27a_{3,3} + a_{1,3}^3 + 54a_{1,3}q^3 = 0. \end{aligned}$$

Для исключения переменной a_2 из h_3 вычисляем результант $\mathrm{Res}_{a_2}(h_2, h_3)$ — получаем многочлен степени 27 от переменной a_1, что даёт нам после факторизации до 27 возможных значений для a_1. После подстановки значения a_1 в h_2 получаем многочлен второй степени от переменной a_2. Решая квадратное уравнение получаем до двух целых корней — значений a_2. Подставляя пару (a_1, a_2) в h_1, получаем значение a_3. Всего получается до 54 возможных троек (a_1, a_2, a_3). Таким образом, решение системы уравнений при спуске по расширениям третьей степени сводится к факторизации многочлена степени 27 и решению квадратных уравнений.

В итоге, решение систем уравнений для расширений степени 2 и 3 в явном виде позволяет нам получить следующую оценку сложности.

Теорема 2.1.8. *Пусть A — абелево многообразие размерности 3 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{A,q}$ по известному χ_{A,q^k} для $k = 2^r 3^s$, где $r, s \geqslant 0$, 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.

Доказательство. Для нахождения $\chi_{A,q}$ выполним сначала r-раз спуск по расширениям степени 2, а затем s-раз спуск по расширениям степени 3. Каждый раз нам необходимо выполнять над полем $\mathbb{F}_\ell$ факторизацию многочлена степени $\mathcal{O}(1)$ и решать квадратичное уравнение, либо извлекать квадратный корень. При этом для квадратичных расширений на первом шаге получается до 16 возможных троек $(a_{1,d}, a_{2,d}, a_{3,d})$ для $d = 2^{r-1}3^s$, на втором шаге для каждой тройки из первого шага получается до 16 новых троек $(a_{1,d}, a_{2,d}, a_{3,d})$ для $d = 2^{r-2}3^s$ и так далее. На последнем шаге может получится до 16^r троек (a_1, a_2, a_3). Аналогично для расширений степени 3 на последнем шаге спуска получаем до 56^s троек для каждой тройки из 16^r троек, полученных на спуске по расширениям степени 2. По эвристике 2.1.1 для достаточно большого q и случайного многообразия A мы можем на каждом шаге с вероятностью больше 0.999 отсечь все лишние решения скалярным умножением на константное число случайных точек (10 для указанной вероятности). Тем не менее, так как существуют специальные многообразия, для которых это не выполняется, алгоритм является вероятностным. Далее предполагаем, что мы находимся в общем случае, и на каждом шаге спуска после отсева лишних решений остаётся одна тройка.

Факторизация многочлена может быть выполнена за время $\widetilde{\mathcal{O}}(\log^2 \ell)$ битовых операций, учитывая что степень — константа, такую же сложность имеют и решение квадратного уравнения и извлечение квадратного корня с помощью алгоритма Чиполы-Лемера [69]. Здесь $\ell = 2\binom{2g}{g} q^{\frac{g}{2}2^{r-i}3^s}$ на i-м шаге спуска по квадратичным расширениям $(i = 1, \ldots, r)$ и $\ell = 2\binom{2g}{g} q^{\frac{g}{2}3^{s-i}}$ на i-м шаге спуска по кубическим расширениям $(i = 1, \ldots, s)$. Асимптотически наибольшее количество операций занимает первый шаг спуска. Поэтому сложность будет равна $\widetilde{\mathcal{O}}(\log^2 \ell) = \widetilde{\mathcal{O}}(g^2 2^{2r-4}3^{2s-2}\log^2 q) = \widetilde{\mathcal{O}}(2^{2r-4}3^{2s-4}\log^2 q)$ битовых операций для квадратичных расширений и $\widetilde{\mathcal{O}}(\log^2 \ell) = \widetilde{\mathcal{O}}(3^{2(s-1)}\log^2 q)$ битовых операций для кубических расширений. Имеем $\widetilde{\mathcal{O}}(3^{2(s-1)}\log^2 q) \subset \widetilde{\mathcal{O}}(2^{2r-2}3^{2s}\log^2 q)$.

Отсев лишних решений выбором случайной точки и скалярным умножением занимает время $R + gS\log q$ для $A(\mathbb{F}_q)$, соответственно, $R + g2^{r-1}3^sS\log q = R + 2^{r-1}3^{s+1}S\log q$ на первом шаге спуска. □

В случае, если A — якобиан гиперэллиптической кривой, то задача упрощается. В этом случае имеем быстрые алгоритмы как для группового закона, так и для выбора случайной точки. Кроме того, для отсечения лишних решений в случае рода 3 можно воспользоваться Леммой 4 из работы [108, с. 495], которая утверждает, что коэффициенты характеристического многочлена $\chi_{C,q}$ кривой C однозначно определяются значениями $\chi_{C,q}(1)$ и $\chi_{C,q}(-1)$. Здесь $\chi_{C,q}(-1)$ — число элементов $\#\operatorname{Jac}_{\widetilde{C}}$ в якобиане квадратичного кручения кривой C, поэтому при отсечении лишних решений мы можем дополнительно делать проверку умножением случайного элемента $\operatorname{Jac}_{\widetilde{C}}$ на $\chi_{C,q}(-1)$. Такая дополнительная проверка позволяет ещё больше снизить вероятность возникновения нескольких элементов на каждом шаге спуска за счёт отсечения лишних вариантов.

Следствие 2.1.8.1. *Пусть C — гиперэллиптическая кривая рода 3 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{C,q}$ по известному χ_{C,q^k}, где $k = 2^r3^s$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{4r}3^{4s}\log^4 q)$ битовых операций.*

Доказательство. Для гиперэллиптических кривых рода 3 над $\mathbb{F}_{q^{2^{r-1}3^s}}$ сложность группового закона в якобиане равна $S = \widetilde{\mathcal{O}}(g\log q^{2^{r-1}3^s}) = \widetilde{\mathcal{O}}(2^{r-1}3^{s+1}\log q)$ битовых операций при использовании алгоритма Кантора [31]. Выбор случайного элемента якобиана эквивалентен извлечению $\mathcal{O}(g)$-раз квадратного корня в поле $\mathbb{F}_{q^{2^{r-1}3^s}}$, т. е. $R = \widetilde{\mathcal{O}}(g2^{2r-2}3^{2s}\log^2 q) = \widetilde{\mathcal{O}}(2^{2r-2}3^{2s+1}\log^2 q)$. Тогда $R + 2^{r-1}3^{s+1}S\log q = \widetilde{\mathcal{O}}(2^{2r-2}3^{2s+1}\log^2 q) + 2^{r-1}3^{s+1}\widetilde{\mathcal{O}}(2^{r-1}3^{s+1}\log^2 q) = \widetilde{\mathcal{O}}(2^{2r-2}3^{2s+2}\log^2 q)$ и общая сложность равна $\widetilde{\mathcal{O}}(2^{2r-4}3^{2s-4}\log^2 q(R + 2^{r-1}3^{s+1}S\log q)) = \widetilde{\mathcal{O}}(2^{4r}3^{4s}\log^4 q)$ по Теореме 2.1.8. □

2.1.6 Случай $g = 4, k = 2^r$

Пусть теперь A — абелево многообразие размерности 4 и $k = 2^s$. Тогда многочлен $\chi_{A,q}$ можно найти по χ_{A,q^k} с помощью Алгоритма 1, спускаясь по

расширениям степени 2. При этом для каждого шага спуска требуется решать следующую систему уравнений, полученную по формуле (2.4)

$$\begin{aligned} h_1 &= a_{1,2} - (-a_1^2 + 2a_2) = 0, \\ h_2 &= a_{2,2} - (a_2^2 - 2a_1a_3 + 2a_4) = 0, \\ h_3 &= a_{3,2} - (-2a_1a_3q + 2a_2q^2 - a_3^2 + 2a_2a_4) = 0, \\ h_4 &= a_{4,2} - (-2a_1^2q^3 + 2a_2^2q^2 + 2q^4 - 2a_3^2q + a_4^2) = 0, \end{aligned} \tag{2.11}$$

где $a_{1,2}$, $a_{2,2}$, $a_{3,2}$ и $a_{4,2}$ — известны. Выражая переменную a_2 в h_1, подставляем её в h_2, h_3, h_4. В h_2 выражаем h_4 и подставляем в h_3, h_4. Получаем:

$$\begin{aligned} h_2 =& 8a_4 - 8a_1a_3 - 4a_{2,2} + a_{1,2}^2 + 2a_1^2a_{1,2} + a_1^4 = 0, \\ h_3 =& 8a_3^2 - a_3(-16a_1q + 8a_1a_{1,2} + 8a_1^3) - 8a_{1,2}q^2 - 8a_1^2q^2 + 8a_{3,2} \\ & - 4a_{1,2}a_{2,2} - 4a_1^2a_{2,2} + a_{1,2}^3 + 3a_1^2a_{1,2}^2 + 3a_1^4a_{1,2} + a_1^6 = 0, \\ h_4 =& a_3^2(64a_1^2 - 128q) + a_3(64a_1a_{2,2} - 16a_1a_{1,2}^2 - 32a_1^3a_{1,2} - 16a_1^5) \\ & + 128q^4 - 128a_1^2q^3 + 32a_{1,2}^2q^2 + 64a_1^2a_{1,2}q^2 + 32a_1^4q^2 - 64a_{4,2} \\ & + 16a_{2,2}^2 - 8a_{1,2}^2a_{2,2} - 16a_1^2a_{1,2}a_{2,2} - 8a_1^4a_{2,2} + a_{1,2}^4 + 4a_1^2a_{1,2}^3 \\ & + 6a_1^4a_{1,2}^2 + 4a_1^6a_{1,2} + a_1^8. \end{aligned} \tag{2.12}$$

Исключая из h_4 переменную a_3 вычислением результанта $\mathrm{Res}_{a_3}(h_3, h_4)$, получаем многочлен от одной переменной a_1 степени 14:

$$c_{14}a_1^{14} + c_{12}a_1^{12} + c_{10}a_1^{10} + c_8a_1^8 + c_6a_1^6 + c_4a_1^4 + c_2a_1^2 + c_0 = 0, \tag{2.13}$$

$$
\begin{aligned}
c_{14} =& -8(8q - a_{1,2}),\\
c_{12} =& 4(368q^2 - 88a_{1,2}q - 4a_{2,2} + 7a_{1,2}^2),\\
c_{10} =& -8(1920q^3 - 672a_{1,2}q^2 - 32a_{2,2}q + 96a_{1,2}^2q - 16a_{3,2} + 12a_{1,2}a_{2,2} - 7a_{1,2}^3),\\
c_8 =& 2(39552q^4 - 19072a_{1,2}q^3 + 256a_{2,2}q^2 + 3552a_{1,2}^2q^2 + 128a_{3,2}q\\
&+ 320a_{1,2}a_{2,2}q - 400a_{1,2}^3q - 1088a_{4,2} + 256a_{1,2}a_{3,2} + 48a_{2,2}^2\\
&- 120a_{1,2}^2a_{2,2} + 35a_{1,2}^4),\\
c_6 =& -8(25600q^5 - 17024a_{1,2}q^4 + 2048a_{2,2}q^3 + 3712a_{1,2}^2q^3 + 1536a_{3,2}q^2\\
&- 128a_{1,2}a_{2,2}q^2 - 512a_{1,2}^3q^2 - 2560a4_2q + 128a_{1,2}a_{3,2}q - 128a_{2,2}^2q\\
&+ 40a_{1,2}^4q + 320a_{1,2}a4_2 + 128a_{2,2}a_{3,2} - 96a_{1,2}^2a_{3,2} - 48a_{1,2}a_{2,2}^2\\
&+ 40a_{1,2}^3a_{2,2} - 7a_{1,2}^5),\\
c_4 =& 4(63488q^6 - 58368a_{1,2}q^5 + 11776a_{2,2}q^4 + 16256a_{1,2}^2q^4 + 14336a_{3,2}q^3\\
&- 6656a_{1,2}a_{2,2}q^3 - 1408a_{1,2}^3q^3 - 15360a_{4,2}q^2 - 3072a_{1,2}a_{3,2}q^2\\
&+ 1792a_{2,2}^2q^2 - 512a_{1,2}^2a_{2,2}q^2 + 336a_{1,2}^4q^2 + 5632a_{1,2}a_{4,2}q\\
&- 512a_{2,2}a_{3,2}q - 640a_{1,2}^2a_{3,2}q + 896a_{1,2}a_{2,2}^2q - 320a_{1,2}^3a_{2,2}q + 24a_{1,2}^5q\\
&- 1792a_{2,2}a_{4,2} + 320a_{1,2}^2a_{4,2} + 1024a_{3,2}^2 - 512a_{1,2}a_{2,2}a_{3,2} + 128a_{1,2}^3a_{3,2}\\
&- 64a_{2,2}^3 + 144a_{1,2}^2a_{2,2}^2 - 60a_{1,2}^4a_{2,2} + 7a_{1,2}^6),\\
c_2 =& -8(16384q^7 - 20480a_{1,2}q^6 + 4096a_{2,2}q^5 + 8192a_{1,2}^2q^5 + 10240a_{3,2}q^4\\
&- 5632a_{1,2}a_{2,2}q^4 - 640a_{1,2}^3q^4 - 8192a4_2q^3 - 6144a_{1,2}a_{3,2}q^3 + 2048a_{2,2}^2q^3\\
&+ 1536a_{1,2}^2a_{2,2}q^3 - 256a_{1,2}^4q^3 + 6144a_{1,2}a_{4,2}q^2\\
&- 512a_{1,2}^2a_{3,2}q^2 - 1024a_{1,2}a_{2,2}^2q^2 + 640a_{1,2}^3a_{2,2}q^2 - 96a_{1,2}^5q^2 - 2048a_{2,2}a_{4,2}q\\
&+ 2048a_{3,2}^2q - 512a_{1,2}a_{2,2}a_{3,2}q + 128a_{1,2}^3a_{3,2}q + 512a_{2,2}^3q - 512a_{1,2}^2a_{2,2}^2q\\
&+ 160a_{1,2}^4a_{2,2}q - 16a_{1,2}^6q - 1024a_{3,2}a_{4,2} + 768a_{1,2}a_{2,2}a4_2 - 192a_{1,2}^3a_{4,2}\\
&- 256a_{2,2}^2a_{3,2} + 128a_{1,2}^2a_{2,2}a_{3,2} - 16a_{1,2}^4a_{3,2} + 64a_{1,2}a_{2,2}^3 - 48a_{1,2}^3a_{2,2}^2\\
&+ 12a_{1,2}^5a_{2,2} - a_{1,2}^7,\\
c_0 =& (128q^4 - 128a_{1,2}q^3 + 32a_{1,2}^2q^2 + 128a_{3,2}q - 64a_{1,2}a_{2,2}q + 16a_{1,2}^3q - 64a_{4,2}\\
&+ 16a_{2,2}^2 - 8a_{1,2}^2a_{2,2} + a_{1,2}^4)^2.
\end{aligned}
$$

При факторизации многочлена получаем до 14 возможных значений a_1. Подставляя значение a_1 в h_3 и решая квадратное уравнение, получаем до 2 значений a_3. Всего 28 пар (a_1, a_3). Подставляя теперь пару в h_1, h_2, получаем по одному значению a_2, a_4. Таким образом, при решении (2.11) получаем до 28 наборов (a_1, a_2, a_3, a_4). При этом для решения требуется только факто-

ризация многочленов и решение квадратных уравнений над конечным полем. Соответственно, получаем следующую оценку сложности.

Теорема 2.1.9. *Пусть A — абелево многообразие размерности 4 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{A,q}$ по известному χ_{A,q^k}, 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.

Доказательство. Аналогично случаю размерности 3, выполнение r-раз спуска по расширениям степени 2 занимает время $\widetilde{\mathcal{O}}(2^{2r}\log^2 q)$, так как задача спуска эквивалентна факторизации многочлена степени 14. Отсев лишних решений с применением эвристики 2.1.1 (на первом шаге спуска) выбором случайной точки и скалярное умножение занимает время $R + gS\log q^{2^{r-1}} = R + 2^{r+1}S\log q$. □

Следствие 2.1.9.1. *Пусть C — гиперэллиптическая кривая рода 4 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{,q}$ по известному χ_{C,q^k}, где $k = 2^r$, имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}(2^{4r}\log^4 q)$ битовых операций.*

Доказательство. Для гиперэллиптических кривых сложность группового закона равна $S = \widetilde{\mathcal{O}}(g\log q^{2^{r-1}}) = \widetilde{\mathcal{O}}(2^{r+1}\log q)$ битовых операций при использовании алгоритма Кантора [31]. Выбор случайного элемента якобиана эквивалентен извлечению $\mathcal{O}(g)$-раз квадратного корня в поле $\mathbb{F}_{q^{2^{r-1}}}$, т. е. $R = \widetilde{\mathcal{O}}(g2^{2r-2}\log^2 q) = \widetilde{\mathcal{O}}(2^{2r}\log^2 q)$. Тогда $(R + 2^{r+1}S\log q) = \widetilde{\mathcal{O}}(2^{2r}\log^2 q) + \widetilde{\mathcal{O}}(2^{2r+2}\log^2 q) = \widetilde{\mathcal{O}}(2^{2r+2}\log^2 q)$. □

2.1.7 Выводы

В общем случае задача нахождения характеристического многочлена $\chi_{A,q}$ по известному χ_{A,q^k} имеет экспоненциальную сложность от степени k и двойную экспоненциальную сложность от размерности g (анализ Алгоритма 1).

В частных случаях ($g = 3, k = 2^r 3^s$ и $g = 4, k = 2^r$) мы доказали (Теоремы 2.1.8, 2.1.9), что задача может быть решена за полиномиальное время от k и $\log q$, при условии, что групповой закон и выбор случайной точки можно выполнить за полиномиальное время. Обобщение результатов на другие размерности и степени поля также возможно. В этом случае систему уравнений можно построить достаточно быстро (см. примеры в Приложении В), но приведение к треугольной форме уже занимает существенно больше времени, кроме того, сама система уравнений в треугольной форме уже становится громоздкой и может занимать много памяти для хранения.

2.2 Подсчёт точек на геометрически разложимых абелевых многообразиях.

2.2.1 Общая схема

Пусть A — абелево многообразие размерности g над конечным полем $\mathbb{F}_q$. Оно называется геометрически разложимым, если имеет место разложение

$$A \sim A_1 \times \ldots \times A_m$$

над некоторым расширением $\mathbb{F}_{q^k}$ конечного поля $\mathbb{F}_q$. Здесь A_i — абелевы многообразия и $m > 1$. Тогда по теореме Тэйта:

$$\chi_{A,q^k}(T) = \chi_{A_1,q^k}(T) \cdot \ldots \cdot \chi_{A_m,q^k}(T).$$

В данном разделе мы рассмотрим задачу нахождения характеристического многочлена $\chi_{A,q}(T)$ по известным многочленам $\chi_{A_1,q^k}(T), \ldots, \chi_{A_m,q^k}(T)$.

Общая схема решения, основанная на общем методе из §2.1.1, выглядит следующим образом:

1. Вычислить многочлены $\chi_{A_1,q^k}(T), \ldots, \chi_{A_m,q^k}(T)$.
2. Разложить k на простые множители: $k = k_1 \cdot \ldots \cdot k_s$.
3. Выполнить спуск по башне конечных полей

$$\mathbb{F}_q \subset \mathbb{F}_{q^{k_1}} \subset \mathbb{F}_{q^{k_1 k_2}} \subset \ldots \subset \mathbb{F}_{q^k},$$

последовательно вычисляя $\chi_{A,q^{k/k_s}}(T)$ из $\chi_{A,q^k}(T)$, затем $\chi_{A,q^{k/(k_s k_{s-1})}}(T)$ из $\chi_{A,q^{k/k_s}}(T)$ и так далее, пока не получим искомый многочлен $\chi_{A,q}(T)$.

4. Для вычисления многочленов на каждом шаге спуска использовать алгоритм из §2.1.4.

Заметим, что сложность подсчёта точек на абелевых многообразиях сильно зависит от размерности абелева многообразия — чем меньше размерность, тем эффективнее подсчёт точек. Более точно, для общих абелевых многообразий имеем суперэкспоненциальную сложность от размерности, а для якобианов гиперэллиптических кривых имеем сложность $\widetilde{\mathcal{O}}(\log^{cg} q)$ (см. сравнение в §1.6). Поэтому наличие разложения позволяет снизить сложность задачи подсчёта точек при условии, что спуск можно выполнить эффективно. Далее мы покажем, что это можно сделать для случаев размерности 3 и 4, используя результаты из §2.1.6 и §2.1.5.

2.2.2 Спуск

Рассмотрим теперь подробнее методику восстановления $\chi_{A,q}(T)$ по $\chi_{A,q^k}(T)$ или набору $\chi_{A_1,q^k}(T), \ldots, \chi_{A_m,q^k}(T)$ таких, что

$$\chi_{A,q^k}(T) = \chi_{A_1,q^k}(T) \cdot \ldots \cdot \chi_{A_m,q^k}(T). \tag{2.14}$$

Как видно из оценки, сложность спуска очень быстро растёт с ростом размерности g и степени k. При этом мы рассматриваем благоприятный случай, когда соответствующая система уравнений приводится в треугольную форму. Поэтому на практике такой спуск осуществим только для небольших значений k и g. Далее в частных случаях мы докажем более точные оценки без допущений и приводимости в треугольную форму. В частности, покажем, что спуск можно эффективно выполнить для $g = 3, k = 2^r 3^s$ и $g = 4, k = 2^s$. Для гиперэллиптических кривых рода 2 и $k = 2^r 3^s$ эта задача была решена в [37; 39]. Заметим, что в случае размерности 2 согласно классификации из [111] максимальная степень расширения поля, над которым обычное абелево многообразие разложимо, не превышает 6. Поэтому случай $k = 2^s \cdot 3^r$ покрывает все обычные геометрически приводимые абелевы многообразия размерности 2.

2.2.3 Случай $g = 3, k = 2^r \cdot 3^s$

Пусть A — абелево многообразие размерности 3 над конечным полем $\mathbb{F}_q$ и $A(\mathbb{F}_{q^k}) \sim A_1 \times A_2$ для некоторого k. Более точно, имеем два возможных случая для A_1, A_2 над $\mathbb{F}_{q^k}$:

1. $A(\mathbb{F}_{q^k}) \sim E_1 \times E_2 \times E_3$, где E_1, E_2, E_3 — эллиптические кривые над $\mathbb{F}_{q^k}$;
2. $A(\mathbb{F}_{q^k}) \sim E_1 \times A_2$, где A_2 — простая абелева поверхность над $\mathbb{F}_{q^k}$.

Обозначим характеристические многочлены кривых E_i для $i = 1, 2, 3$ и абелевой поверхности A_2 как

$$\chi_{E_i,q^k} = T^2 - t_{i,k}T + q^k$$

и

$$\chi_{A_2,q^k} = T^4 + b_{1,k}T^3 + b_{2,k}T^2 + b_{1,k}q^kT + q^{2k}$$

соответственно. Тогда из (2.14) получаем $\chi_{A,q^k} = \chi_{E_1,q^k} \cdot \chi_{E_2,q^k} \cdot \chi_{E_3,q^k}$ или $\chi_{A,q^k} = \chi_{E_1,q^k} \cdot \chi_{A_2,q^k}$. Поэтому для коэффициентов χ_{A,q^k} возможны следующие варианты:

$$\begin{aligned} a_{1,k} &= t_{1,k} + t_{2,k} + t_{3,k}, \\ a_{2,k} &= -t_{1,k}t_{2,k} - t_{1,k}t_{3,k} - t_{2,k}t_{3,k} - 3q^k, \\ a_{3,k} &= 2t_{3,k}q^k + 2t_{2,k}q^k + 2t_{1,k}q^k + t_{1,k}t_{2,k}t_{3,k} \end{aligned} \tag{2.15}$$

для первого случая и

$$\begin{aligned} a_{1,k} &= t_{1,k} - b_{1,k}, \\ a_{2,k} &= b_{1,k}t_{1,k} - b_{2,k} - q^k, \\ a_{3,k} &= b_{2,k}t_{1,k} - 2b_{1,k}q^k \end{aligned} \tag{2.16}$$

для второго случая.

Найти χ_{E_i,q^k} можно за время $\widetilde{\mathcal{O}}(k^4 \log^4 q)$ с помощью алгоритма Схоофа-Элкиса-Аткина [4], а χ_{A_2,q^k} можно найти за время $\widetilde{\mathcal{O}}(k^\Delta \log^\Delta q)$ с помощью алгоритма Пилэ-Схоофа (см. §1.6). Когда A_2 — якобиан гиперэллиптической кривой, то может использоваться алгоритм Годри-Шоста [75] с $\Delta = 8$.

Замечание. *Если для кривых E_i существуют кривые $\widetilde{E}_i$, определённые над $\mathbb{F}_q$ и такие, что $\widetilde{E}_i \sim E_i$ над $\mathbb{F}_{q^k}$ (например, $\widetilde{E}_i$ — кручение кривой E_i), то коэффициенты $a_{1,k}, a_{2,k}, a_{3,k}$ в (2.15) можно выразить через следы эндоморфизма Фробениуса $\widetilde{t}_i$ кривых $\widetilde{E}_i$, применяя формулу (2.3) для случая $g = 1$:*

$$\widetilde{t}_{i,1} = \widetilde{t}_i, \quad \widetilde{t}_{i,2} = \widetilde{t}_i^2 - 2q, \quad \widetilde{t}_{i,k} = \widetilde{t}_i \cdot \widetilde{t}_{i,k-1} - q\widetilde{t}_{i,k-2}$$

и положив $t_{i,k} = \widetilde{t}_{i,k}$ *(кривые изогенны). Это позволяет найти* χ_{A,q^k} *за время* $\widetilde{\mathcal{O}}(\log^4 q + k^2 \log q)$ *вместо* $\widetilde{\mathcal{O}}(k^4 \log^4 q)$ *(по Лемме 2.1.1).*

Аналогичным образом можно поступить и в случае $A \sim E_1 \times A_2$*, получив сложность* $\widetilde{\mathcal{O}}(\log^\Delta q + k^2 \log q)$ *вместо* $\widetilde{\mathcal{O}}(k^\Delta \log^\Delta q)$*.*

Получив таким образом χ_{A,q^k} и разложив k на множители, мы можем применить Алгоритм 1 для выполнения спуска по башне конечных полей и нахождения $\chi_{A,q}$. В случае $k = 2^r 3^s$ из результатов §2.1.5 получаем следующую оценку сложности.

Теорема 2.2.1. *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*.*

Доказательство. Согласно Теореме 2.1.8 восстановление $\chi_{A,q}$ по χ_{A,q^k} занимает время

$$\mathcal{O}_D = \widetilde{\mathcal{O}}(2^{2r-4} 3^{2s-4} \log^2 q(R + 2^{r-1} 3^{s+1} S \log q)) = \widetilde{\mathcal{O}}(2^{2r} 3^{2s} \log^2 q(R + 2^r 3^s S \log q))$$

битовых операций. Поэтому получаем общую сложность

$$\widetilde{\mathcal{O}}(k^4 \log^4 q + \mathcal{O}_D)$$

для первого случая и

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

для второго при использовании алгоритма Схоофа-Элкиса-Аткина и Схоофа-Пилэ для нахождения числа точек на E_1, E_2, E_3, A_2. Если A — якобиан гиперэллиптической кривой, то $\mathcal{O}_D = \widetilde{\mathcal{O}}(2^{4r}3^{4s}\log^4 q)$ по следствию 2.1.8.1. □

2.2.4 Случай $g = 4, k = 2^r$

Пусть теперь A — абелево многообразие размерности 4, такое что $A(\mathbb{F}_{q^k}) \sim A_1 \times A_2$, где $k = 2^s$. Тогда задача подсчёта точек на A может быть сведена к подсчёту точек на A_1 и A_2 следующим образом. Вычисляем $\chi_{A,q^k} = \chi_{A_1,q^k} \times \chi_{A_2,q^k}$, затем применяем Алгоритм 1 для нахождения $\chi_{A,q}$, спускаясь по расширениям степени 2. При этом для каждого шага спуска требуется решать систему уравнений, полученную в §2.1.6. Соответственно, имеем следующую оценку сложности.

Теорема 2.2.2. *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 $\chi_{A,q}$, а значит, и число точек на A, может быть найдено 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.

Доказательство. После вычисления $\chi_{A_1,q^k}, \ldots, \chi_{A_1,q^k}$ с помощью алгоритма Пилэ за время $\log^{\Delta(g_1)} q^k + \ldots + \log^{\Delta(g_m)} q^k$, находим $\chi_{A,q^k} = \chi_{A_1,q^k} \cdot \ldots \cdot \chi_{A_m,q^k}$. Затем по Теореме 2.1.9 получаем сложность нахождения $\chi_{A,q}$ по χ_{A,q^k}:

$$\widetilde{\mathcal{O}}(2^{2r}\log^2 q(R + 2^{r+1}S\log q)).$$

□

Также как и для размерности 3, сложность нахождения $\chi_{A_1,q^k}, \ldots, \chi_{A_1,q^k}$ снижается в случае, если существуют $\widetilde{A}_1, \ldots, \widetilde{A}_m$ определённые над $\mathbb{F}_q$ и такие, что

$\widetilde{A}_1 \sim A_1, \ldots, \widetilde{A}_m \sim A_m$ над $\mathbb{F}_{q^k}$. В этом случае мы можем найти $\chi_{\widetilde{A}_i,q}$ за время $\widetilde{\mathcal{O}}(\log^{\Delta(g_i)} q)$ и восстановить χ_{A_i,q^k} по $\chi_{\widetilde{A}_i,q}$ за время $\widetilde{\mathcal{O}}(g_i^3 k^2 \log q)$ (Лемма 2.1.1).

Оценки сложности также уменьшаются в случае, если одно или несколько из абелевых многообразий $A, A_1, \ldots, A_m$ являются якобианами гиперэллиптических кривых — тогда сложность спуска $\mathcal{O}_D = \widetilde{\mathcal{O}}(k^4 \log^4 q)$ по Следствию 2.1.9.1 и константа Δ известна. Все возможные случаи-следствия из Теоремы 2.2.2 для сложности подсчёта точек приводим в Таблице 3.

Таблица 3 — Сложность подсчёта точек для геометрически разложимых абелевых многообразиях размерности 4, $k = 2^r$.

$A(\mathbb{F}_{q^k})$	Условия	Сложность
$E_1 \times E_2 \times E_3 \times E_4$	—	$\widetilde{\mathcal{O}}(k^4 \log^4 q + \mathcal{O}_D)$
$E_1 \times E_2 \times E_3 \times E_4$	$A = \mathrm{Jac}_C$	$\widetilde{\mathcal{O}}(k^4 \log^4 q)$
$E_1 \times E_2 \times E_3 \times E_4$	$A = \mathrm{Jac}_C$, $\exists \widetilde{E}_i$	$\widetilde{\mathcal{O}}(k^4 \log^4 q)$
$E_1 \times E_2 \times A_2$, $A_2 \times A_2'$	—	$\widetilde{\mathcal{O}}(\log^{\Delta(2)} q^k + \mathcal{O}_D)$
$E_1 \times E_2 \times A_2$, $A_2 \times A_2'$	$A = \mathrm{Jac}_C$	$\widetilde{\mathcal{O}}(\log^{\Delta(2)} q^k)$
$E_1 \times E_2 \times A_2$, $A_2 \times A_2'$	$A = \mathrm{Jac}_C$, $\exists \widetilde{E}_i, \widetilde{A}_2, \widetilde{A}_2'$	$\widetilde{\mathcal{O}}(\log^{\Delta(2)} q + k^4 \log^4 q)$
$E_1 \times E_2 \times A_2$, $A_2 \times A_2'$	$A = \mathrm{Jac}_C$, $\exists \widetilde{E}_i, \widetilde{A}_2, \widetilde{A}_2'$, $\widetilde{A}_2 = \mathrm{Jac}_{C_1}$, $\widetilde{A}_2' = \mathrm{Jac}_{C_2}$	$\widetilde{\mathcal{O}}(\log^8 q + k^4 \log^4 q)$
$E_1 \times A_3$	—	$\widetilde{\mathcal{O}}(\log^{\Delta(3)} q^k + \mathcal{O}_D)$
$E_1 \times A_3$	$A = \mathrm{Jac}_C$	$\widetilde{\mathcal{O}}(\log^{\Delta(3)} q^k)$
$E_1 \times A_3$	$A = \mathrm{Jac}_C, \exists \widetilde{A}_3$	$\widetilde{\mathcal{O}}(\log^{\Delta(3)} q + k^4 \log^4 q)$
$E_1 \times A_3$	$A = \mathrm{Jac}_C$, $\exists \widetilde{A}_3$, $\widetilde{A}_3 = \mathrm{Jac}_{C_3}$	$\widetilde{\mathcal{O}}(\log^{14} q + k^4 \log^4 q)$

2.2.5 Выводы

Число точек на геометрически разложимом абелевом многообразии можно найти сведением задачи к многообразиям меньшей размерности, которые заданны над некоторым расширением поля степени k. Чем меньше размерность, тем меньше сложность подсчёта точек (см. §1.6), поэтому получаем уменьшение сложности задачи при условии, что спуск к базовому полю можно выполнить эффективно. Используя результаты из раздела §2.1, мы показали, что сложность задачи снижается для геометрически разложимых абелевых многообразий размерности 3 (степени расширения $k = 2^r 3^s$) и 4 (степени расширения $k = 2^r$), если групповой закон и выбор случайной точки выполняется за полиномиальное время.

2.3 Кривые вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$

2.3.1 Обзор известных результатов

Кривые вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ над полем комплексных чисел исследовались ещё Лежандром, поэтому иногда данный класс кривых называют также кривыми Лежандра.

В случае $a = 0$ проблема подсчёта числа точек изучалась в работах [112; 113]. В данном случае элементы матрицы Картье-Манина представляют собой биномиальные коэффициенты, для которых известны сравнения по модулю p, что позволяет получить явные формулы для коэффициентов характеристического многочлена по модулю p и использовать их для восстановления дзета-функции кривой и числа точек.

Случай $b = 1$ наиболее хорошо исследован. В работах [114; 115] были доказаны некоторые свойства матрицы Хассе-Витта W кривой C — обратимость для подходящего выбора параметра a, чётность ранга матрицы для чётного g и тот факт, что матрица является (обобщённой) перестановочной при $\gcd(g, p) = 1$. Так как p-ранг кривой равен рангу матрицы W_p, обратимость матрицы Хассе-Витта означает, что кривая является обычной и, соответственно, это наиболее частый случай.

Кривые с $b = 1$ имеют нетривиальную группу автоморфизмов, что позволяет для автоморфизма σ, несопряжённого гиперэллиптической инволюции, построить морфизм из кривой C в фактор-кривую $D = C/\langle\sigma\rangle$. Из чего следует, что $\mathrm{Jac}_D \subseteq \mathrm{Jac}_C$ по теореме Клеймана-Серра и $\mathrm{Jac}_C \sim \mathrm{Jac}_D \times A$ по теореме о полной приводимости Пуанкаре. Уравнения такой кривой D были получены в работе [41, Proposition 3]. Разложения якобиана для $g = 3, 4$ и некоторые другие общие разложения есть в [33] с моделями кривых в разбиении для алгебраически замкнутого поля.

Аналогичные уравнения для более общего случая, когда b является корнем степени g в поле $\mathbb{F}_q$ и g — нечётное, были получены Смитом в работе [42, §7.3]. Однако для чётного g подобных результатов неизвестно. Кроме того, авторы не приводят явных уравнений для многообразия A, несмотря на то, что в ряде случаев это многообразие — якобиан кривой. Полную информацию о разложе-

нии якобиана кривой C для любого рода g с уравнениями кривых в разбиении приводим в разделе §2.3.2.

В общем случае кривые изучались в работе [116], где авторы получили выражение числа точек через модулярные функции и суммы характеров. Однако, вычисление таких функций и сумм само по себе является сложной задачей. Известны только результаты для сумм специального вида (см. монографию [117]).

В случае рода $g = 2$ было доказано [37—39], что якобиан кривой распадается на эллиптические кривые над некоторым расширением базового поля, и были получены явные формулы для характеристического многочлена кривой, выражающие его коэффициенты через следы Фробениуса эллиптических кривых. Над базовым полем якобиан кривой при этом может быть прост, а для эллиптических кривых существуют эффективные алгоритмы для подсчёта точек (SEA). Поэтому такие кривые имеют практическое применение в криптографии. В работе Шу-Кани [111] явные формулы были обобщены и улучшены и была получена полная классификация характеристических многочленов для геометрически приводимых абелевых поверхностей.

В нашей работе, в последующих разделах, мы обобщаем алгоритмы и методы подсчёта точек с рода 2 на случай кривых рода 3 и выше. Более того, мы предлагаем новый метод для подсчёта точек на основе связи матриц Картье-Манина и многочленов Лежандра. Сравнение известных результатов с результатами из данной работы приведено в Таблице 4.

Таблица 4 — Сводка результатов по кривым $y^2 = x^{2g+1} + ax^{g+1} + bx$

g	Результат	Ссылки
2	алгоритм подсчёта точек, $\widetilde{\mathcal{O}}(\log^4 q)$	[37]
2	явные формулы для числа точек	[39]
3	алгоритм подсчёта точек над $\mathbb{F}_p$, $\widetilde{\mathcal{O}}(\log^4 p)$	§3.1, Алг. 3
3	явные формулы для числа точек над $\mathbb{F}_q$	§3.2
4	алгоритм для подсчёта точек, $\widetilde{\mathcal{O}}(\log^8 q)$	§3.3
g	декомпозиция якобиана, $b = 1$	[41]
g	декомпозиция якобиана, b — любое	[42; 43], §2.3.2
g	общий алгоритм подсчёта точек	§2.3.3
g	явные формулы для $\#\operatorname{Jac}_C(\mathbb{F}_p) \pmod p$	§2.3.4, Прил. §Б.

2.3.2 Разложение якобиана над расширением поля

Для нахождения разложения якобиана кривой $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ найдем сначала разложение якобиана кривой $C' : y^2 = x^{2g+1} + cx^{g+1} + x$. Так как при $c = \pm\frac{a}{\sqrt{b}}$ кривые изоморфны над $\mathbb{F}_q[\sqrt[4g]{b}]$, это даст разложение над данным полем.

Затем мы обобщим разложение Смита [42, §7.3] для нечетного рода и найдём все уравнения кривых в разложении. Это даст нам разложение якобиана над меньшим расширением: над полем $\mathbb{F}_q[\sqrt[2g]{b}]$ для чётного рода g и над полем $\mathbb{F}_q[\sqrt[g]{b}]$ для нечётного.

Случай $b = 1$

Некоторые разбиения якобиана кривой C' над алгебраически замкнутым полем были получены в работе [33], используя метод Кани-Роузена [45] и группу автоморфизмов кривой. Однако, метод Кани-Роузена не зависит от поля, для его применения нужно определить только группу автоморфизмов кривой. Причём все возможные группы автоморфизмов гиперэллиптических кривых над алгебраически замкнутым полем характеристики 0 известны [66; 118]. Более точная информация, включающая модели кривых с группами автоморфизмов и переход к алгебраически замкнутым полям положительной характеристики, имеется для рода $g = 2$ [119] и $g = 3$ [120, с. 612]. Так как автоморфизмы даны в явном виде, мы можем перейти к конечному полю, просто проверив, над каким расширением они определены. Следующая лемма позволяет определить подгруппы группы автоморфизмов кривой C' над конечным полем.

Лемма 2.3.1. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ – гиперэллиптическая кривая рода g, заданная над конечным полем $\mathbb{F}_q, q = p^n$.*

1. *$Aut_{C'}(\mathbb{F}_q)$ содержит негиперэллиптическую инволюцию $s : (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$ и подгруппу $\mathcal{C}_2 \times \mathcal{C}_2 = \langle s,\iota\rangle$.*
2. *Если $q \nmid 2g$ и $2g|q-1$, то $Aut_{C'}(\mathbb{F}_q)$ содержит автоморфизм $r : (x,y) \mapsto (\zeta_g x, \zeta_{2g} y)$ порядка $2g$ и диэдральную подгруппу $\mathcal{D}_{4g}$.*

Здесь ι — *гиперэллиптическая инволюция.*

Автоморфизмы s, r были найдены в работе [41]. Из первого пункта леммы и [33, с. 13, (3.5)] следует, что якобиан кривой C' всегда распадается

$$\mathrm{Jac}_{C'} \sim \mathrm{Jac}_{C'/\langle s\rangle} \times \mathrm{Jac}_{C'/\langle s\iota\rangle}\,.$$

Уравнения для фактор-кривых позволяет найти следующая теорема.

Теорема 2.3.2. *Пусть* $C' : y^2 = x^{2g+1}+cx^{g+1}+x$ — *гиперэллиптическая кривая рода* g, *заданная над конечным полем* $\mathbb{F}_q$, *где* $q = p^n$, $p > 2$, $\gcd(g, p) = 1$. *Обозначим через* $D_m(x, \alpha)$ *и* $D_m(x) := D_m(x, 1)$ *многочлены Диксона степени степени* m. *Тогда*

1. *фактор-кривая кривой* C' *по модулю инволюции* $s : (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$ *имеет уравнение:*

$$X_1' : y^2 = D_g(x) + c,$$

если род g *нечётный, и уравнение*

$$X_1' : y^2 = (x+2)(D_g(x) + c),$$

если род g *чётный.*

2. *фактор-кривая кривой* C' *по модулю инволюции* $s\iota : (x,y) \mapsto \left(\frac{1}{x}, -\frac{y}{x^{g+1}}\right)$ *имеет уравнение*

$$X_2' : y^2 = (x^2-4)(D_g(x) + c),$$

если род g *нечётный, и уравнение*

$$X_2' : y^2 = (x-2)(D_g(x) + c),$$

если род g *чётный.*

Доказательство. 1. Из [41, Prop. 3] имеем, что $C'/\langle s\rangle$ задаётся уравнением

$$y^2 = xf(x^2-2) + c,$$

если род g нечётный, и уравнением

$$y^2 = (x+2)(f(x^2-2) + c)$$

в случае чётного рода g. Здесь многочлен $f \in \mathbb{F}_q$ — уникальный унитарный многочлен, чьи корни — все числа $\zeta + \frac{1}{\zeta}$, где $\zeta \in \overline{\mathbb{F}}_q$, $\zeta^g = -1$, $\zeta \neq -1$.

В работе [42, §7.3] было показано, что для нечётного g имеем $xf(x^2-2) = D_g(x)$. Для чётного g результат следует из факторизации многочленов Диксона [121, Th. 1] над $\overline{\mathbb{F}}_q$:

$$D_g(x,\alpha) = \prod_{k=1,\, k\equiv 1 \bmod 2}^{2g-1} (x - \sqrt{\alpha}(\zeta_{4g}^k + \zeta_{4g}^{-k})) = f(x^2-2),$$

где ζ_{4g} – примитивный корень из единицы степени $4g$.

2. Доказательство данного пункта аналогично доказательству [41, Prop. 2] с добавлением многочленов Диксона. Для доказательства будем использовать следующие соотношения:

$$x^{2g}+1 = x^g\left(x+\frac{1}{x}\right) f\left(x^2+\frac{1}{x^2}\right) = x^{g-1}\left(x+\frac{1}{x}\right) D_g\left(x+\frac{1}{x}\right)$$

для нечётного g и

$$x^{2g}+1 = x^g f\left(x^2+\frac{1}{x^2}\right) = x^g D_g\left(x+\frac{1}{x}\right)$$

для чётного g.

Функциональное поле кривой $C'/\langle s\iota\rangle$ — это поле, состоящее из инвариантных относительно $s\iota$ функций C'. Непосредственно можно проверить, что функции $\xi = \left(x+\frac{1}{x}\right)$, $\eta = \frac{y}{x^{\frac{g-1}{2}}}\left(1-\frac{1}{x^2}\right)$ в случае нечетного рода g и $\xi = \left(x+\frac{1}{x}\right), \eta = \frac{y}{x^{\frac{g}{2}}}\left(1-\frac{1}{x}\right)$ в случае чётного рода, являются инвариантными относительно $s\iota$. Кроме того, ξ и η порождают функциональное поле кривой $C'/\langle s\iota\rangle$, так как автоморфизм $s\iota$ индуцирует инъекцию функциональных полей $\mathbb{F}_q(C'/\langle s\iota\rangle) \subseteq \mathbb{F}_q(C')$ и кривая C' — гиперэллиптическая, т. е. имеем по определению $[\mathbb{F}_q(x) : \mathbb{F}_q(C')] = 2$ ([80, §6.2]).

Используя соотношения и следующее свойство многочленов Диксона:

$$D_g(x+1/x) = x^g + 1/x^g,$$

составим теперь уравнения фактор-кривых. Имеем $y^2 = x^{2g+1} + cx^{g+1} + x = x(x^{2g} + cx^g + 1)$. В случае нечётного рода g, подставляя $y = \eta x^{\frac{g-1}{2}}\left(1-\frac{1}{x^2}\right)^{-1}$, получаем

$$\eta^2 = x^2\left(1-\frac{1}{x^2}\right)^2\left(x^g+\frac{1}{x^g}+c\right) = x^2\left(1-\frac{1}{x^2}\right)^2\left(D_g\left(x+\frac{1}{x}\right)+c\right).$$

Так как $\xi^2 - 4 = x^2\left(1 - \frac{1}{x^2}\right)^2$, получаем следующее уравнение фактор-кривой $C'/\langle s\iota\rangle$ для нечетного рода g:

$$\eta^2 = (\xi^2 - 4)(D_g(\xi) + c).$$

Аналогично можно получить для чётного рода:

$$\eta^2 = (\xi - 2)(D_g(\xi) + c).$$

□

Заметим, что по Следствию 6 из [41], в случае нечётного рода g и $p \neq 5$, фактор-кривая $C'/\langle s\rangle$ является в большинстве случаев абсолютно неприводимой.

Случай $b \neq 1$

Кривая $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ изоморфна кривой C' с параметром $c = \frac{a}{\sqrt{b}}$ над конечным полем $\mathbb{F}_q[\sqrt[4g]{b}]$ посредством следующего изоморфизма

$$(x,y) \mapsto (b^{\frac{1}{2g}}x, b^{\frac{2g+1}{4g}}y).$$

Благодаря этому, мы можем получить разбиение Jac_C над $\mathbb{F}_q[\sqrt[4g]{b}]$ из разбиения $\mathrm{Jac}_{C'}$:

$$\mathrm{Jac}_C(\mathbb{F}_q[\sqrt[4g]{b}]) \simeq \mathrm{Jac}_{C'/\langle s\rangle}(\mathbb{F}_q[\sqrt[4g]{b}]) \times \mathrm{Jac}_{C'/\langle s\iota\rangle}(\mathbb{F}_q[\sqrt[4g]{b}]). \tag{2.17}$$

При этом, так как изоморфизм определён над расширением конечного поля, то над базовым полем якобиан может оставаться простым, что позволяет использовать его в приложениях, например, для криптографии.

Однако, якобиан Jac_C можно разложить над расширением меньшей степени, чем в разбиении (2.17), используя и обобщая результаты из работы [42]. Это позволяет получить разбиение 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.

Если параметр b является степенью g в поле $\mathbb{F}_q$ и род кривой нечётный, то на кривой C можно определить [42, §7.3] ещё до g автоморфизмов — по одному

для каждого b_i такого, что $b = b_i^g$:

$$\sigma_i : (x, y) \mapsto \left(\frac{b_i}{x}, \frac{y b_i^{\frac{g+1}{2}}}{x^{g+1}} \right).$$

Соответствующие фактор-кривые имеют уравнения

$$C/\langle \sigma_i \rangle : y^2 = D_g(x, b_i) + a,$$

где D_g — многочлен Диксона степени g. Фактор-отображения $s_i : C \to C/\langle \sigma_i \rangle$ при этом задаются как

$$(x, y) \mapsto \left(x + \frac{b_i}{x}, y x^{-\frac{g+1}{2}} \right).$$

Так как у нас имеется морфизм кривых, то $\mathrm{Jac}_{C/\langle \sigma_i \rangle}$ изогенен абелеву подмногообразию в Jac_C и, соответственно, $\mathrm{Jac}_C \sim \mathrm{Jac}_{C/\langle \sigma_i \rangle} \times A$. В следующей теореме мы обобщаем данный результат, а также теорему 2.3.2, на случай чётного рода и выводим полную информацию о фактор-кривых кривой C по автоморфизмам.

Теорема 2.3.3. *Пусть $X : y^2 = x^{2g+1} + a x^{g+1} + \alpha^g x$ — это гиперэллиптическая кривая рода g, определенная над конечным полем $\mathbb{F}_q$, и ι — гиперэллиптическая инволюция. Тогда кривая X 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 $\sigma\iota$ следующие.*

1. *Если род g нечётный, то*

$$X/\langle \sigma \rangle : y^2 = D_g(x, \alpha) + a \tag{2.18}$$

и

$$X/\langle \sigma\iota \rangle : y^2 = (x^2 - 4\alpha)(D_g(x, \alpha) + a), \tag{2.19}$$

2. *Если род g чётный, то*

$$X/\langle \sigma \rangle : y^2 = (x + 2\sqrt{\alpha})(D_g(x, \alpha) + a) \tag{2.20}$$

и

$$X/\langle \sigma\iota \rangle : y^2 = (x - 2\sqrt{\alpha})(D_g(x, \alpha) + a). \tag{2.21}$$

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

Доказательство. Случай (2.18) доказан в [42, §7.3]. В случае $b = 1$ уравнения (2.18) и (2.20) получены в [41], но без использования многочленов Диксона в явном виде. Для доказательства оставшихся случаев мы будем использовать аналогичный подход.

Заметим сначала, что многочлены Диксона имеют свойство $D_g\left(x + \frac{\alpha}{x}\right) = x^g + (\frac{\alpha}{x})^g$. Что позволяет записать уравнение X в виде:

$$y^2 = x^{g+1}\left(D_g\left(x + \frac{\alpha}{x}, \alpha\right) + a\right).$$

Далее, функциональное поле кривой $X/\langle\sigma\iota\rangle$ представляет собой поле инвариантных относительно инволюции $\sigma\iota$ функций на X. Для нахождения уравнения $X/\langle\sigma\iota\rangle$ требуется найти образующие её функционального поля и затем из соотношений между образующими составить уравнение кривой.

Можно показать, что функциональное поле кривой $X/\langle\sigma\iota\rangle$ порождается функциями $\xi = x + \frac{\alpha}{x}$ и $\eta = \frac{y}{x^{\frac{g-1}{2}}}\left(1 - \frac{\alpha}{x^2}\right)$ в случае нечетного рода g и функциями $\xi = x + \frac{\alpha}{x}$ и $\eta = \frac{y}{x^{\frac{g}{2}}}\left(1 - \frac{\sqrt{\alpha}}{x}\right)$ в случае четного рода g.

Теперь, используя свойство многочленов Диксона, выводим уравнения

$$\eta^2 = (D_2(\xi,b) - 2\alpha)(D_g(\xi,\alpha) + a) = (\xi^2 - 4\alpha)(D_g(\xi,\alpha) + a)$$

для нечетного рода g и

$$\eta^2 = (\xi - 2\sqrt{\alpha})(D_g(\xi,\alpha) + a)$$

для четного рода. Что и доказывает (2.19) и (2.21). Уравнение (2.20) находится аналогично, если взять $\xi = x + \frac{\alpha}{x}$ и $\eta = \frac{y}{x^{\frac{g}{2}}}\left(1 + \frac{\sqrt{\alpha}}{x}\right)$. □

В случае (2.20) и (2.21) автоморфизм σ определен над $\mathbb{F}_q[\sqrt{\alpha}]$, поэтому фактор-отображения и фактор-кривые также определены над данным полем. Заметим, что отображение $(x,y) \mapsto (-x, iy)$, где $i^2 = -1$, является изоморфизмом данных фактор-кривых, поэтому они являются кручениями степени 2 друг друга.

Так кривая X имеет негиперэллиптическую инволюцию, мы можем разбить якобиан по методу Кани-Роузена [33; 45]:

$$\mathrm{Jac}_X \sim \mathrm{Jac}_{X/\langle\sigma\rangle} \times \mathrm{Jac}_{X/\langle\sigma\iota\rangle}.$$

Уравнения фактор-кривых известны из нашей теоремы 2.3.3 и, таким образом, задача подсчёта точек на кривой X эквивалентна подсчёту точек на данных фактор-кривых.

Теперь вернёмся к нашей кривой C. Она представляет собой кривую X с параметром $\alpha = \sqrt[g]{b}$. Автоморфизмы определены над полем $\mathbb{F}_q[\sqrt[g]{b}]$ (нечетный род) и $\mathbb{F}_q[\sqrt[2g]{b}]$ (чётный род), поэтому имеет место разложение

$$\mathrm{Jac}_C(\mathbb{F}_q[\sqrt[g]{b}]) \sim \mathrm{Jac}_{X/\langle\sigma\rangle}(\mathbb{F}_q[\sqrt[g]{b}]) \times \mathrm{Jac}_{X/\langle\sigma\iota\rangle}(\mathbb{F}_q[\sqrt[g]{b}]) \tag{2.22}$$

для нечетного рода g и

$$\mathrm{Jac}_C(\mathbb{F}_q[\sqrt[2g]{b}]) \sim \mathrm{Jac}_{X/\langle\sigma\rangle}(\mathbb{F}_q[\sqrt[2g]{b}]) \times \mathrm{Jac}_{X/\langle\sigma\iota\rangle}(\mathbb{F}_q[\sqrt[2g]{b}]) \tag{2.23}$$

в случае чётного рода g.

В случае $g = 2$ разложение совпадает с разложением, полученным Сато [37], но метод получения и модели кривых другие.

Частичные разложения. Дополнительно, для нечётного рода имеется морфизм кривых $C \to E$, заданный как $(x,y) \mapsto (x^g, yx^{\frac{g-1}{2}})$, где E — эллиптическая кривая с уравнением

$$y^2 = x^3 + ax^2 + bx.$$

Это отображение является фактор-отображением по автоморфизму r^2, где r из Леммы 2.3.1. Так как у нас есть морфизм кривых, то по теореме Клаймана-Серра имеем $\mathrm{Jac}_C \sim E \times A$ для некоторого абелева многообразия A размерности $g-1$. Соответственно, в случае нечетного рода кривая C всегда имеет непростой якобиан. Подсчёт точек в данном случае сводится к нахождению числа точек на эллиптической кривой и абелевом многообразии A.

Более того, для каждого делителя m рода g можно определить два отображения: $(x,y) \mapsto (x^m, x^{\frac{m-1}{2}}y)$ и $(x,y) \mapsto (x^{\frac{g}{m}}, x^{\frac{\frac{g}{m}-1}{2}}y)$ из кривой C в кривые

$$C_{\frac{g}{m}} : y^2 = x^{2\frac{g}{m}+1} + ax^{\frac{g}{m}+1} + bx$$

и

$$C_m : y^2 = x^{2m+1} + ax^{m+1} + bx.$$

Это позволяет нам получить следующие частичные разложения якобиана над конечным полем $\mathbb{F}_q$.

Предложение 3. *Пусть $C_n : y^2 = x^{2n+1} + ax^{n+1} + bx$ — гиперэллиптическая кривая рода n и A_n – абелево многообразие размерности n, так что $C = C_g$. Тогда*

1. *если* $g = mk$ *для нечётных целых положительных чисел* m, k *таких, что* $m \neq k$, *то*

$$\mathrm{Jac}_C \sim \mathrm{Jac}_{C_m} \times \mathrm{Jac}_{C_k} \times A_{g-m-k};$$

2. *если* $g = m^2$ *для нечётного положительного целого* m, *то*

$$\mathrm{Jac}_C \sim \mathrm{Jac}_{C_m} \times A_{g-m};$$

3. *если* $g = 2^e m$ *для целого* $e > 0$ *и нечётного целого* $m > 0$, *то*

$$\mathrm{Jac}_C \sim \mathrm{Jac}_{C_{2^e}} \times A_{g-2^e}.$$

Предложение 3 можно применить рекурсивно к $\mathrm{Jac}_{C_m}, \mathrm{Jac}_{C_k}$ до тех пор, пока в разложении не получатся простые числа m, k. Однако, мы не знаем уравнений для абелевых многообразий в разложении, и более того, даже в случае, если они известны, общий алгоритм для подсчёта точек [5] не так эффективен на практике, как алгоритмы подсчёта точек в якобиане гиперэллиптической кривой. Таким образом, частичные разложения не дают нам достаточно информации для решения задачи подсчёта точек, однако они могут быть использованы для ускорения вычислений.

Наконец, в работе [43, Prop. 14, с. 505] для нечётного простого g и $b = 1$ авторы доказывают, что $\mathrm{Jac}_C \sim E \times \mathrm{Jac}^2_{X/\langle\sigma\rangle}$, но не указывают над каким полем. В то же время, легко найти примеры, когда $\mathrm{Jac}_C \sim E \times \mathrm{Jac}_{X/\langle\sigma\rangle} \times \mathrm{Jac}_{\tilde{X}/\langle\sigma\rangle}$ над конечным полем $\mathbb{F}_q$. Следующее утверждение обобщает данное разложение на случай $b \neq 1$ и явным образом задаёт поле.

Предложение 4. *Пусть* $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ *— гиперэллиптическая кривая нечётного рода* g *над конечным полем* $\mathbb{F}_q$. *Тогда* $\mathrm{Jac}_C \sim E \times \mathrm{Jac}^2_{X_1}$ *над полем* $\mathbb{F}_q[\sqrt[g]{b}, \zeta_g]$, *где* ζ_g *— примитивный корень из единицы степени* g, $E : y^2 = x^3 + ax^2 + bx$ *— эллиптическая кривая и* $X_1 : y^2 = D_g(x, \sqrt[g]{b}) + a$ *— гиперэллиптическая кривая рода* $(g-1)/2$.

Доказательство. На кривой C есть автоморфизм r^2 степени g, определённый над $\mathbb{F}_q[\zeta_g]$, где r из Леммы 2.3.1. Более того, на кривой имеется негиперэллиптическая инволюция σ, определённая над $\mathbb{F}_q[\sqrt[g]{b}]$. Поэтому группа автоморфизмов $\mathrm{Aut}_C(\mathbb{F}_q[\sqrt[g]{b},\zeta_g])$ содержит группу диэдра $\mathcal{D}_{2g}$ порядка $2g$, образованную r^2 и σ. Тогда мы можем применить теорему Кани-Роузена для

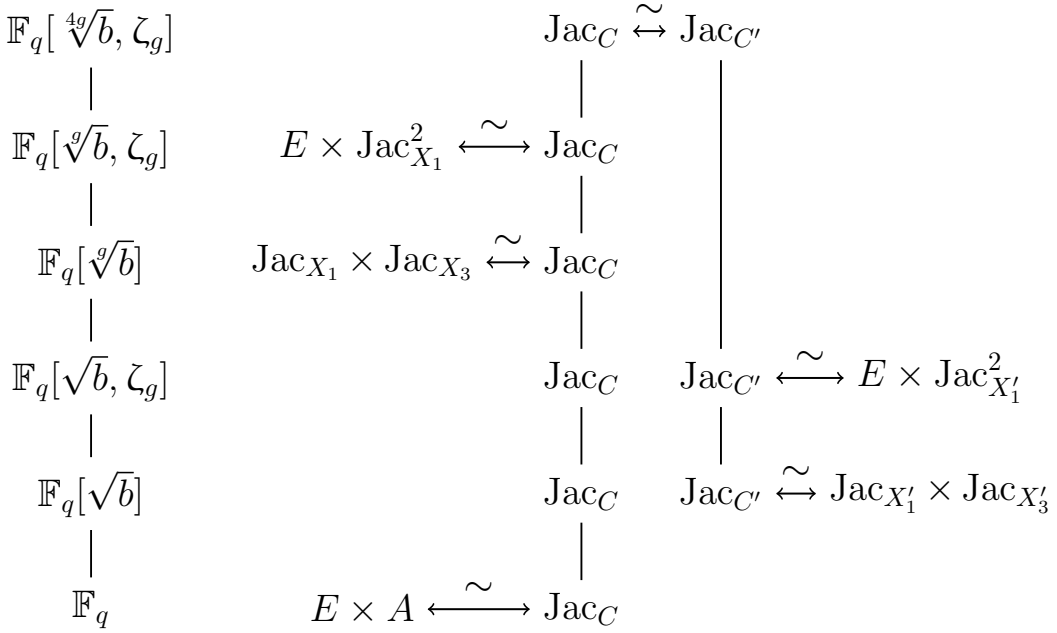
получения разложения

$$\mathrm{Jac}_C \sim \mathrm{Jac}_{C/\langle r^2\rangle} \times \mathrm{Jac}_{C/\langle \sigma\rangle} \times \mathrm{Jac}_{C/\langle \sigma r^2\rangle}\,.$$

Имеем $C/\left\langle r^2\right\rangle = E$ с фактор-отображением $(x,y) \mapsto (x^g, yx^{\frac{g-1}{2}})$. Хотя автоморфизм r^2 определён над $\mathbb{F}_q[\zeta_g]$, его фактор-отображение определено над $\mathbb{F}_q$ и поэтому якобиан Jac_C в случае нечётного рода g всегда раскладывается над $\mathbb{F}_q$ в произведение E и A.

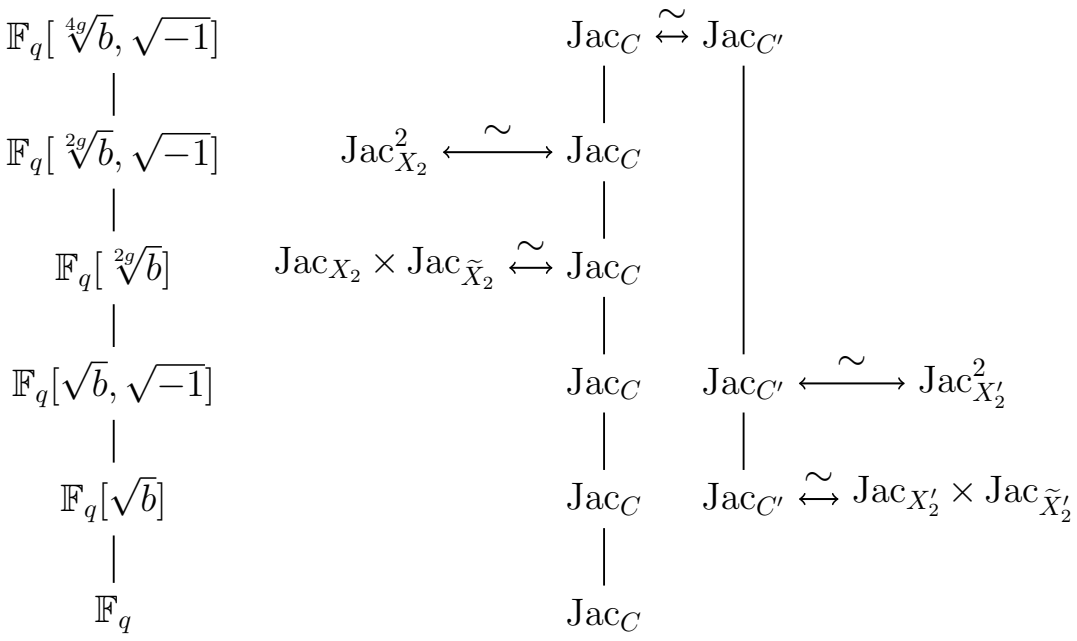
Из Теоремы 2.3.3 имеем $C/\langle\sigma\rangle = X_1$. Также, аналогичным доказательству Теоремы 2.3.3 образом, можно показать, что $C/\left\langle \sigma r^2\right\rangle$ имеет уравнение $y^2 = D_g(x, \zeta_g^2\sqrt[g]{b}) + a$. Используя свойство многочленов Диксона $\beta^g D_g(x,\alpha) = D_g(\beta x, \beta^2\alpha)$ [122, Lemma 2.6, с. 12], получаем, что кривая $C/\left\langle \sigma r^2\right\rangle$ изоморфна кривой X_1 посредством изоморфизма $(x,y) \mapsto (\zeta_g x, y)$. Таким образом, получаем, что $\mathrm{Jac}_C \sim E \times \mathrm{Jac}_{X_1}^2$ над $\mathbb{F}_q[\sqrt[g]{b}, \zeta_g]$. □

Итоговая схема разложения якобиана представлена на Рисунках 2.1 и 2.2.



$X_1 : y^2 = D_g(x, \sqrt[g]{b}) + a$
$X_3 : y^2 = (x^2 - 4\sqrt[g]{b})(D_g(x, \sqrt[g]{b}) + a)$
$E : y^2 = x^3 + ax^2 + bx$
$C' : y^2 = x^{2g+1} + \frac{a}{\sqrt{b}}x^{g+1} + x$
$X_1' : y^2 = D_g(x,1) + \frac{a}{\sqrt{b}}$
$X_3' : y^2 = (x^2-4)(D_g(x,1) + \frac{a}{\sqrt{b}})$

Рисунок 2.1 — Разложение якобиана кривой $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ нечётного рода.



$$X_2 : y^2 = (x + 2\sqrt[2g]{b})(D_g(x, \sqrt[g]{b}) + a) \qquad C' : y^2 = x^{2g+1} + \tfrac{a}{\sqrt{b}}x^{g+1} + x$$
$$\widetilde{X}_2 : y^2 = (x + 2\sqrt[2g]{b})(D_g(x, \sqrt[g]{b}) + a) \qquad X'_2 : y^2 = (x + 2)(D_g(x, 1) + \tfrac{a}{\sqrt{b}})$$
$$\widetilde{X}'_2 : y^2 = (x - 2)(D_g(x, 1) + \tfrac{a}{\sqrt{b}})$$

Рисунок 2.2 — Разложение якобиана кривой $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ чётного рода.

2.3.3 Общий алгоритм подсчёта точек на основе разложения якобиана

Так как нам известно разложение якобиана кривой C на якобианы других кривых над расширением конечного поля (§2.3.2), то задача подсчёта точек в якобиане данной кривой сводится к подсчёту точек на кривых над расширением с последующим восстановлением числа точек над базовым полем по методам из §2.1 и §2.2. В силу того, что кривые в разбиении имеют меньший род, чем кривая C, то подсчёт точек на них имеет меньшую асимптотическую сложность. Соответственно, получаем снижение сложности задачи подсчёта точек на кривой C по сравнению с общим случаем.

Вычисление $\#\operatorname{Jac}_C(\mathbb{F}_q)$ сводится к вычислению характеристического многочлена кривой $\chi_{C,q}(T)$. Из разбиения имеем

$$\chi_{C,q^k}(T) = \chi_{X_1,q^k}(T)\chi_{X_2,q^k}(T), \tag{2.24}$$

где k такое, что $\mathbb{F}_q[\sqrt[g]{b}] \simeq \mathbb{F}_{q^k}$ для нечётного g и $\mathbb{F}_q[\sqrt[2g]{b}] \simeq \mathbb{F}_{q^k}$ для чётного g, а уравнения кривых X_1, X_2 задаются Теоремой 2.3.3. Соответственно, нам нужно вычислить коэффициенты

$$\chi_{C,q}(T) = T^{2g} + a_1T^{2g-1} + a_2T^{2g-1} + \ldots + a_gT^g + a_{g-1}qT^{g-1} + \ldots + a_1q^{g-1}T + q^g$$

по коэффициентам

$$\chi_{C,q^k}(T) = T^{2g} + a_{1,k}T^{2g-1} + \ldots + a_{g,k}T^g + a_{g-1,k}q^kT^{g-1} + \ldots + a_{1,k}q^{k(g-1)}T + q^{kg}.$$

Коэффициенты характеристического многочлена эндоморфизма Фробениуса над базовым полем могут быть получены из коэффициентов над расширением по общему методу из §2.1.2 или формуле [80, с. 195] для L-многочленов (взаимных многочленов к многочленам χ):

$$L_{C,q^k}(T^k) = \prod_{\zeta^k=1} L_{C,q}(\zeta T) \tag{2.25}$$

с использованием дополнительной информации по кривой для сокращения числа возможных вариантов (например, используя информацию по матрицам Картье-Манина из §2.3.4). Для рода 2 вычисление было сделано в [37—39]. Наша работа — это обобщение алгоритмов для рода 2 на любой род. В данном разделе опишем алгоритм для любого рода. Специализации на род 3 и 4 приводим в §3.1 и §3.3.

Сравнением коэффициентов в правой и левой частях формулы (2.25) или с помощью применения рекуррентной формулы (2.3) получаем систему из g уравнений и g неизвестных $a_1, \ldots, a_g$. Система уравнений в общем случае получается довольно большая, поэтому для оптимизации вычислений мы используем обобщение (§2.1.4) метода спуска по расширениям простой степени для рода 2 из работы [39], который заключается в выводе из формулы (2.25) рекуррентных формул для коэффициентов характеристического многочлена над расширениями простой степени и затем рекурсивного их применения. Следующий алгоритм является специализацией на Jac_C обобщённых методов спуска по башне расширений конечного поля из §2.2.

Алгоритм 2: Вычисление характеристического многочлена $\chi_{C,q}(T)$ гиперэллиптической кривой $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ над конечным полем $\mathbb{F}_q$.

Input: $a,b \in \mathbb{F}_q$, $p > 2$.

Output: Коэффициенты $(a_1, \ldots, a_g)$ многочлена $\chi_{C,q}(T)$.

1 Найти k такое, что $\mathbb{F}_q[\sqrt[g]{b}] \simeq \mathbb{F}_{q^k}$, если род g нечётный и $\mathbb{F}_q[\sqrt[2g]{b}] \simeq \mathbb{F}_{q^k}$, если g — чётный;

2 Разложить k на множители: $k = k_1 \cdot \ldots \cdot k_m$, где все k_i простые числа и $k_1 \leqslant \ldots \leqslant k_m$;

3 $n \leftarrow k$;

4 Вычислить $L_{X_1,q^n}(T)$ и $L_{X_2,q^n}(T)$ для $X_1 := X/\langle\sigma\rangle$ и $X_2 := X/\langle\sigma\iota\rangle$ из теоремы 2.3.3;

5 $L_{C,q^n}(T) \leftarrow L_{X_1,q^n}(T)L_{X_2,q^n}(T)$;

6 $list \leftarrow \{(a_{1,n}, \ldots, a_{g,n})\}$;

7 **for** j *from* 1 *to* m **do**

8 $\quad i \leftarrow \frac{n}{k_j}$;

9 $\quad S \leftarrow \{\}$;

10 $\quad$ **foreach** $(a_{1,n}, \ldots, a_{g,n}) \in list$ **do**

11 $\quad\quad$ Составить систему уравнений от неизвестных $a_{1,i}, \ldots, a_{g,i}$ по формуле $L_{C,q^n}(T^{k_j}) = \prod_{\zeta^{k_j}=1} L_{C,q^i}(\zeta T)$;

12 $\quad\quad$ Решить систему, используя неравенства $|a_{m,i}| \leqslant \binom{2g}{m} q^{\frac{im}{2}}$, $m = 1, \ldots, g$ для получения списка S' возможных наборов $(a_{1,i}, \ldots, a_{g,i})$;

13 $\quad\quad$ Исключить лишние решения из S', выбирая случайные элементы $\mathrm{Jac}_C(\mathbb{F}_{q^i})$ и умножая их на $1 + a_{1,i} + \ldots a_{g,i} + a_{1,i}q^i + \ldots + a_{g,i}q^{gi}$;

14 $\quad\quad S \leftarrow S \cup S'$;

$\quad$ **end**

15 $\quad list \leftarrow S$;

16 $\quad n \leftarrow i$;

end

return $list[1]$;

Теорема 2.3.4. *Пусть $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ — гиперэллиптическая кривая рода g, заданная над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена $\chi_{C,q}(T)$ и, соответственно, числа точек на кривой C и в её якобиане имеет эвристическую вероятностную сложность $\widetilde{\mathcal{O}}\left(2^{2g}g^3\log_2 g\delta \log^{\Delta} q\right)$, где $\delta = (2\varepsilon)(3\varepsilon' + \frac{1}{4}) \approx 39.335$. Кроме того, $\Delta = 9$ в случае нечётного рода g, а в случае чётного рода g выбирается такое Δ, что $\widetilde{\mathcal{O}}(\log^{\Delta} q)$ — сложность подсчёта точек на кривой $y^2 = (x+2)(D_g(x)+\frac{a}{\sqrt{b}})$ рода $\frac{g}{2}$.*

Доказательство. Для доказательства теоремы выполним анализ Алгоритма 2. Шаг 1. Пусть $k' = 2g$, если g — чётное, и $k' = g$, если g — нечётное. Число k

может быть найдено с помощью факторизации многочлена $x^i - b$ над $\mathbb{F}_{q^i}$ для i от k' до 1 и $i \nmid k'$. Соответственно, имеем сложность $\widetilde{\mathcal{O}}(k'^2 \log q) = \widetilde{\mathcal{O}}(g^2 \log q)$ операций в $\mathbb{F}_q$.

Шаг 2. Факторизация k может быть выполнена за субэкспоненциальное время $L_k(1/3) = L_g(1/3)$, используя алгоритм решета числового поля.

Для быстрого вычисления $L_{X_1,q^n}(T)$ и $L_{X_2,q^n}(T)$ в Шаге 4 мы вместо вычислений над расширением конечного поля сначала вычисляем характеристические многочлены кручений кривых X_1, X_2, определённых над полем $\mathbb{F}_q[\sqrt{b}]$. После чего определяем коэффициенты $L_{X_1,q^n}(T)$ и $L_{X_2,q^n}(T)$ по рекуррентным формулам (2.3) за время $\widetilde{\mathcal{O}}(g^3k^2 \log q) = \widetilde{\mathcal{O}}(g^5 \log q)$ (Лемма 2.1.1). Уравнения кручений легко вывести как следствие из Теоремы 2.3.3. Они задаются для чётного рода g уравнениями

$$\widetilde{X}_{1,2} : y^2 = (x \pm 2)(D_g(x,1) + a/\sqrt{b}),$$

а для нечётного рода g — уравнениями

$$\widetilde{X}_1 : y^2 = D_g(x,1) + a/\sqrt{b}$$

и

$$\widetilde{X}_2 : y^2 = (x^2 - 4)(D_g(x,1) + a/\sqrt{b}).$$

Общий алгоритм для подсчёта точек на гиперэллиптической кривой при фиксированном роде g имеет сложность $\widetilde{\mathcal{O}}(\log^{cg} q)$ [30] для некоторой константы c. Таким образом, нахождение $L_{\widetilde{X}_1,q^2}(T)$ и $L_{\widetilde{X}_2,q^2}(T)$ в случае чётного g занимает время $\widetilde{\mathcal{O}}(2^{cg/2} \log^{cg/2} q)$. Более того, кривые $\widetilde{X}_1$ и $\widetilde{X}_2$ — квадратичные кручения, поэтому достаточно вычислить $L_{\widetilde{X}_1,q^2}(T)$. В случае если g — нечётное, то из Предложения 4 имеем $\mathrm{Jac}_{X_2} \sim E \times \mathrm{Jac}^2_{X_1}$. Многочлен $L_{E,q}(T)$ может быть вычислен с помощью алгоритма Схоофа-Элкиса-Аткина за время $\widetilde{\mathcal{O}}(\log^4 q)$. Многочлен $L_{\widetilde{X}_1,q^2}(T)$ может быть найден с помощью алгоритма Абелара [65, §2.1] за время $\widetilde{\mathcal{O}}(\log^9 q)$ при $q \to \infty$.

Система уравнений в Шаге 11 может быть составлена за время $\widetilde{\mathcal{O}}(gkB)$, где $B = \binom{g(k+1)}{g}$ (см. Лемму 2.1.2). В общем случае данная система содержит самое большее $2gk_j$ уравнений от g неизвестных степени gk_j. Её решение с помощью результантов или базисов Грёбнера (см. §2.1.4) имеет в общем случае экспоненциальную сложность от $\log q$ и двойную экспоненциальную сложность от k и g.

Шаг 13. Каждый раз, когда мы находим решение $(a_{1,i}, ..., a_{g,i})$ на Шаге 12, мы можем сразу же его проверить, поэтому нет необходимости выполнять проход по списку S'. Для проверки решения мы выполняем $\mathcal{O}(1)$ проверок умножением случайных элементов $\overline{D}$ из $J_C(\mathbb{F}_{q^i})$ на число $N = 1 + a_{1,i} + \ldots + a_{g,i} + a_{1,i}q^i + \ldots + a_{g,i}q^{gi}$ и исключаем решения, для которых $N \cdot \overline{D} \neq 0$. Для целей подсчёта точек достаточно брать элементы $\overline{D}$, представляемые $\mathbb{F}_{q^i}$-рациональными дивизорами $D = P_1 + \ldots + P_g + gP_\infty$, где $P_r \in C(\mathbb{F}_{q^i})$ и $P_r \neq -P_s$ для всех $r \neq s$. Выбор одной точки эквивалентен вычислению квадратного корня в $\mathbb{F}_{q^i}$, что может быть выполнено за время $\widetilde{\mathcal{O}}(\log^2 q^i) = \widetilde{\mathcal{O}}(g^2 \log^2 q)$ битовых операций. Таким образом, выбор одного элемента якобиана занимает время $\widetilde{\mathcal{O}}(g^3 \log^2 q)$. Умножение N на $\overline{D}$ может быть выполнено за время $\widetilde{\mathcal{O}}(g^4 \log^2 q)$ битовых операций с помощью алгоритма Кантора [31] для вычисления группового закона (сложность $\widetilde{\mathcal{O}}(g \log q^i) = \widetilde{\mathcal{O}}(g^2 \log q)$) и быстрых алгоритмов умножения на скаляр (сложность $\widetilde{\mathcal{O}}(\log N) = \widetilde{\mathcal{O}}(g^2 \log q)$ операций в якобиане). Таким образом, время выполнения теста полиномиальное относительно g и $\log q$. Согласно эвристике 2.1.1 и Лемме 2.1.6 при $q \to \infty$, с вероятностью стремящейся к 1, тест отсечёт все лишние решения.

В целом, алгоритм имеет экспоненциальную сложность от $\log q$ из-за того, что требуется решать систему полиномиальных уравнений от нескольких переменных. Однако, используя эвристическое предположение, что данная система уравнений имеет размерность 0, получаем полиномиальную от $\log q$ сложность. Имеем по Теореме 2.1.7 сложность нахождения $L_{C,q}(T)$ по $L_{C,q^k}(T)$ (спуска):

$$\widetilde{\mathcal{O}}\left(2^{2^g g^2 k\varepsilon} \log^2 q + R + 2^{2^g g \log_2 (gk)\varepsilon'} S \log q\right) = \widetilde{\mathcal{O}}\left((2^{2^g g^3 (2\varepsilon)} + g^3 + 2^{2^g g \log_2 (2g^2)\varepsilon'} g^2) \log^2 q\right),$$

учитывая, что $k = 2g$ в худшем случае. Полагая $g \geqslant 2$ и опуская члены малого порядка, получаем эвристическую оценку сложности спуска: $\widetilde{\mathcal{O}}\left(2^{2^g g^3 \log_2(g)\delta} \log^2 q\right)$, где $\delta = (2\varepsilon)(3\varepsilon' + \frac{1}{4})$. Откуда и получается утверждение теоремы, учитывая, что сложность подсчёта точек на кривой $\widetilde{X}_1$ в случае нечётного рода равна $\widetilde{\mathcal{O}}(\log^9 q)$, а для чётного — $\widetilde{\mathcal{O}}(\log^{\frac{cg}{2}} q)$.

В дальнейших разделах мы покажем, что задачу подсчёта точек на C можно решить для рода 3 и 4 на основе общих результатов из §2.2.3 и §2.2.4 за полиномиальное время без использования эвристики о размерности. □

Реализацию общего алгоритма для рода 4 приводим в §3.3. Для рода 3 мы сначала покажем в §3.1, что метод на основе матриц Картье-Манина имеет полиномиальную сложность над простым полем $\mathbb{F}_p$, а затем в §3.2 введём явные формулы для числа точек над полем $\mathbb{F}_q$.

2.3.4 Матрица Картье-Манина и её связь с многочленами Лежандра.

Матрицы Картье-Манина позволяют получить искомый характеристический многочлен $\chi_{C,q}$ по модулю характеристики поля p. В общем случае вычисление данных матриц занимает время $\widetilde{\mathcal{O}}(\sqrt{p})$ [59], что не эффективно, так как размер поля, например, в криптографических приложениях обычно большой.

В данном разделе покажем, что матрицы Картье-Манина кривой C имеют дополнительную структуру и свойства, частично связанные с разложением якобиана, что позволяет эффективно её вычислить в ряде случаев.

А именно, мы покажем что элементы матрицы кривой являются многочленами Лежандра, а сама матрица является обобщённой перестановочной (мономиальной). Эти два свойства позволят нам составить полные списки возможных характеристических многочленов (по модулю p) и использовать их для подсчёта точек.

Как и в случае с разложением якобиана, удобнее сначала вывести свойства матрицы Картье-Манина кривой $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ и затем перейти к общему случаю.

Случай $b = 1$

Покажем, что элементы матрицы Картье-Манина кривых C' представляют собой многочлены Лежандра, а сами матрицы имеют особый вид – они являются центросимметричными и, как следствие, могут быть приведены к блочно-диагональному виду эквивалентным преобразованием. Кроме того, как замечено в работах [114; 115] данные матрицы являются обобщёнными перестановочными (мономиальными) в случае $\gcd(p,g) = 1$.

Следующая лемма позволяет определить, в каких случаях коэффициенты матрицы Картье-Манина кривой являются нулевыми.

Лемма 2.3.5. *Пусть* $X : y^2 = x^t + ax^s + bx^m$ *— гиперэллиптическая кривая рода* g*, заданная над конечным полем* $\mathbb{F}_q$*, где* $q = p^n, p > 2$*,* $t \in \{2g+2, 2g+1\}$*,* $m < s < t$*,* $m \in \{0, 1\}, d = \gcd(t-m, s-m)$*. Тогда если* $W = (w_{i,j})_{1 \leqslant i,j \leqslant g}$ *— матрица Картье-Манина кривой* X*, то* $w_{i,j} = 0$ *для всех* i,j*, таких что* $ip - j \not\equiv m\left(\frac{p-1}{2}\right) \pmod{d}$*.*

Доказательство. Имеем

$$\begin{aligned} w_{i,j} &= [x^{ip-j}](x^t + ax^s + bx^m)^{\frac{p-1}{2}} = \\ &= [x^{ip-j-m\left(\frac{p-1}{2}\right)}](x^{t-m} + ax^{s-m} + b)^{\frac{p-1}{2}} = \\ &= [x^{ip-j-m\left(\frac{p-1}{2}\right)}] \sum_{k_1+k_2+k_3=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k_1,k_2,k_3} a^{k_2} b^{k_3} x^{(t-m)k_1+(s-m)k_2} = \\ &= \sum_{k_1,k_2,k_3} \binom{\frac{p-1}{2}}{k_1,k_2,k_3} a^{k_2} b^{k_3}, \end{aligned}$$

где сумма берётся по всем целым неотрицательным k_1, k_2, k_3, удовлетворяющим системе уравнений:

$$\begin{cases} k_1 + k_2 + k_3 = \frac{p-1}{2}, \\ (t-m)k_1 + (s-m)k_2 = ip - j - m\left(\frac{p-1}{2}\right). \end{cases}$$

Второе уравнение имеет решения в целых числах k_1, k_2 тогда и только тогда, когда $\gcd(t-m, s-m)$ делит $ip - j - m\left(\frac{p-1}{2}\right)$. В противном случае система не имеет решений и $w_{i,j} = 0$. □

Данной леммы уже достаточно для получения условий (анти)диагональности матрицы Картье-Манина кривой.

Теорема 2.3.6. *Пусть* $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ *— гиперэллиптическая кривая рода* g*, определённая над конечным полем* $\mathbb{F}_q$ *характеристики* $p > 2$ *и пусть* W *— её матрица Картье-Манина. Тогда*

1. W *— диагональная матрица, если*
   - *а)* g *— чётное и* $p \equiv 1 \pmod{2g}$*,*
   - *б)* g *— нечётное и* $p \equiv 1 \pmod{g}$*.*
2. W *— антидиагональная матрица, если*
   - *а)* g *— чётное и* $p \equiv -1 \pmod{2g}$*,*
   - *б)* g *— нечётное и* $p \equiv -1 \pmod{g}$*.*

Доказательство. 1. Пусть g — чётное и $p \equiv 1 \pmod{2g}$. Тогда $p = 1 + 2gm$ для некоторого целого m. По лемме 2.3.5 элементы матрицы W могут быть ненулевыми только, если $g|ip - j - \frac{p-1}{2} = i(1 + 2gm) - j - gm$, т. е. $i \equiv j \pmod{g}$. Так как $1 \leqslant i,j \leqslant g$, получаем $i = j$.

Пусть теперь g — нечётное и $p \equiv 1 \pmod{g}$. Так как $\gcd(g,2) = 1$, имеем $ip - j - \frac{p-1}{2} \equiv i - j \pmod{g}$ и $i \equiv j \pmod{g}$.

2. Доказательство аналогично пункту 1. □

Покажем теперь, что коэффициенты матрицы Картье-Манина кривой C' представляют собой многочлены Лежандра.

Теорема 2.3.7. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ — гиперэллиптическая кривая рода g, определённая над конечным полем $\mathbb{F}_q, q = p^n, p > 2$ и $W = (w_{i,j})$ — её матрица Картье-Манина. Тогда*

1. *$w_{i,j} = 0$, если $ip - j \not\equiv \frac{p-1}{2} \pmod{g}$ и*
2. *$w_{i,j} \equiv P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-c/2) \pmod{p}$ в противном случае.*

Доказательство. 1. Следует из леммы 2.3.5.

2. Пусть $ip - j \equiv \frac{p-1}{2} \pmod{g}$ и, следовательно, $g|ip - j - \frac{p-1}{2}$. Имеем

$$w_{i,j} = [x^{ip-j-\frac{p-1}{2}}](x^{2g} + cx^g + 1)^{\frac{p-1}{2}}.$$

Делая подстановку $z = x^g$, получаем

$$w_{i,j} = [z^{\frac{ip-j}{g} - \frac{p-1}{2g}}](z^2 + cz + 1)^{\frac{p-1}{2}} \equiv [z^{\frac{ip-j}{g} - \frac{p-1}{2g}}]\frac{1}{\sqrt{z^2 + cz + 1}} \pmod{p}.$$

Так как производящая функция для многочленов Лежандра имеет вид

$$\sum_{k=0}^{\infty} P_k(x)z^k = \frac{1}{\sqrt{z^2 - 2xz + 1}},$$

то получаем $w_{i,j} \equiv P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-c/2)$. □

Теперь из свойств многочленов Лежандра можно вывести свойства матриц Картье-Манина кривой.

Теорема 2.3.8. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ — гиперэллиптическая кривая рода g, определённая над конечным полем $\mathbb{F}_q, q = p^n, p > 2$ и $W = (w_{i,j})$ — её матрица Картье-Манина. Тогда матрица W:*

1. *центросимметричная;*

2. *мономиальная при* $\gcd(p,g) = 1$;
3. *диагональная, если*
   - *а) род* g *чётный и* $p \equiv 1 \pmod{2g}$,
   - *б) род* g *нечётный и* $p \equiv 1 \pmod{g}$;
4. *антидиагональная, если*
   - *а) род* g *чётный и* $p \equiv -1 \pmod{2g}$,
   - *б) род* g *нечётный и* $p \equiv -1 \pmod{g}$.

Доказательство. 1. По теореме 2.3.7, если $g \mid ip - j - \frac{p-1}{2}$, то имеем

$$w_{i,j} \equiv P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-c/2) \pmod{p}.$$

Многочлены Лежандра имеют свойство [123, (5.9)]:

$$P_{p-1-m}(x) \equiv P_m(x) \pmod{p}, 0 \leqslant m \leqslant p-1.$$

Поэтому получаем

$$\begin{aligned} w_{i,j} &\equiv P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-c/2) \equiv P_{p-1-\frac{ip-j}{g} + \frac{p-1}{2g}}(-c/2) \equiv \\ &\equiv P_{\frac{(g-i+1)p-(g-j+1)}{g} - \frac{p-1}{2g}}(-c/2) \equiv w_{g-i+1,g-j+1} \pmod{p}. \end{aligned}$$

Из чего следует, что матрица Картье-Манина кривой C' является центросимметричной матрицей, по определению центросимметричных матриц.

2. Данное свойство впервые было доказано Миллером [114; 115]. Если зафиксировать j, то при $\gcd(p,g) = 1$ и $ip - j \equiv \frac{p-1}{2} \pmod{g}$ сравнение $ip - j \equiv \frac{p-1}{2} \pmod{g}$ имеет только одно решение для i, т. к. $1 \leqslant i \leqslant g$. Соответственно, в каждой строке может быть не более одного ненулевого элемента. Аналогично можно показать, что каждый столбец содержит не более одного ненулевого элемента. Из чего следует, что W — мономиальная матрица.

3, 4. см. Теорему 2.3.6. □

Известно, что множество центросимметричных (мономиальных) матриц замкнуто относительно операции умножения матриц. Кроме того, возведение всех элементов матриц данных типов в одну и туже степень не меняет вид матрицы. Поэтому, если W — центросимметричная (мономиальная), то матрица $W_p = W^t(W^t)^{(p)} \cdots (W^t)^{(p^{n-1})}$ из формулы Манина (1.1) также будет центросимметричной (мономиальной).

Для центросимметричных матриц известно ортогональное преобразование [124], которое позволяет преобразовать матрицу в блочно-диагональную

форму. Если размер матрицы чётный, то оно определено следующей несингулярной ортогональной матрицей

$$Q = \sqrt{\frac{1}{2}} \begin{pmatrix} I & -J \\ J & I \end{pmatrix}.$$

Для нечётного случая имеем

$$Q = \sqrt{\frac{1}{2}} \begin{pmatrix} I & 0 & -J \\ 0 & \sqrt{2} & 0 \\ J & 0 & I \end{pmatrix}.$$

Здесь J — обменная матрица, т.е. матрица на побочной диагонали которой стоят единицы, а все остальные элементы нулевые.

Данное преобразование определено над $\mathbb{F}_q[\sqrt{2}]$ и, для эквивалентности матриц Картье-Манина необходимо, вместо ортогонального, преобразование следующего вида [55, Proposition 2.2]: $W \mapsto S^{(p)} W S^{-1}$, где S — несингулярная матрица. Поэтому введём немного модифицированное преобразование, которое будет преобразовывать матрицу W в блочно-диагональную форму, но при этом оно определено над базовым полем $\mathbb{F}_q$ и сохраняет эквивалентность матриц Картье-Манина.

Теорема 2.3.9. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ — гиперэллиптическая кривая рода g, заданная над конечным полем $\mathbb{F}_q$, $\operatorname{char} \mathbb{F}_q = p > 2$. Тогда матрица Картье-Манина W кривой C' эквивалентна над $\mathbb{F}_q$ блочно-диагональной матрице относительно преобразования $W \mapsto S^{(p)} W S^{-1}$, где S — несингулярная матрица.*

Доказательство. Разобьём матрицу W на блоки следующим образом. Пусть $W = \begin{pmatrix} W_1 & W_3 \\ W_2 & W_4 \end{pmatrix}$, если g — чётное и

$$W = \begin{pmatrix} W_1 & \vec{a} & W_3 \\ \vec{b} & s & \vec{d} \\ W_2 & \vec{e} & W_4 \end{pmatrix},$$

если g — нечётное. Здесь $\vec{a}, \vec{e}$ — центральные вектор-столбцы матрицы W; $\vec{b}, \vec{d}$ — центральные вектор-строки, а s — элемент матрицы W, лежащий в центре. Так как по теореме 2.3.8 матрица W — центросимметричная над $\mathbb{F}_q$, то она

может быть записана в виде $W = \begin{pmatrix} W_1 & JW_2J \\ W_2 & JW_1J \end{pmatrix}$ для g — чётного и $W = \begin{pmatrix} W_1 & \vec{a} & JW_2J \\ \vec{b} & s & \vec{b}J \\ W_2 & J\vec{a} & JW_1J \end{pmatrix}$ для g — нечётного.

Рассмотрим преобразование вида $S^{(p)}WS^{-1}$.

1. Если $\sqrt{2} \in \mathbb{F}_q$, то возьмём $S = Q$ и тогда $S^{(p)}WS^{-1} = Q^{(p)}WQ^t$. Покажем, что это преобразование приводит матрицу в блочно-диагональную форму. Если g — чётное, то $Q^{(p)} = (\frac{1}{2})^{\frac{p-1}{2}}Q$ и

$$Q^{(p)}WQ^t = \left(\frac{1}{2}\right)^{\frac{p-1}{2}} \begin{pmatrix} W_1 - JW_2 & 0 \\ 0 & J(W_1 + JW_2)J \end{pmatrix}.$$

Если g — нечётное, то

$$Q^{(p)}WQ^t = \left(\frac{1}{2}\right)^{\frac{p-1}{2}} \begin{pmatrix} W_1 - JW_2 & 0 & 0 \\ 0 & 2^{\frac{p-1}{2}}s & \sqrt{2}^p\vec{b} \\ 0 & \sqrt{2}J\vec{a} & J(W_1 + JW_2)J \end{pmatrix}.$$

2. Пусть теперь $\sqrt{2} \notin \mathbb{F}_q$. Возьмём $S = \begin{pmatrix} I & 0 & -J \\ 0 & 1 & 0 \\ J & 0 & I \end{pmatrix}$ для нечётного g и $S = \begin{pmatrix} I & -J \\ J & I \end{pmatrix}$ для чётного g. Тогда $S^{(p)} = S$, т.к. $p > 2$, и

$$S^{-1} = \frac{1}{2}\begin{pmatrix} I & 0 & J \\ 0 & 2 & 0 \\ -J & 0 & I \end{pmatrix} \quad \text{или} \quad S^{-1} = \frac{1}{2}\begin{pmatrix} I & J \\ -J & I \end{pmatrix}.$$

Имеем

$$S^{(p)}WS^{-1} = \begin{pmatrix} W_1 - JW_2 & 0 & 0 \\ 0 & s & \vec{b}J \\ 0 & 2J\vec{a} & J(W_1 + JW_2)J \end{pmatrix}$$

для нечётного случая и

$$S^{(p)}WS^{-1} = \begin{pmatrix} W_1 - JW_2 & 0 \\ 0 & J(W_1 + JW_2)J \end{pmatrix}$$

для чётного. Заметим, что это преобразование уже не является ортогональным. Его также можно использовать и для первого случая ($\sqrt{2} \in \mathbb{F}_q$), если ортогональность не требуется. □

Применяя преобразование из доказательства теоремы к матрице W_p и применяя формулу Манина (1.1), получаем следующую формулу для многочлена Фробениуса кривой $\chi_{C',q}(T)$.

Следствие 2.3.9.1. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ — гиперэллиптическая кривая рода g над конечным полем $\mathbb{F}_q, q = p^n, p > 2$ и пусть матрица Картье-Манина кривой записана как в теореме 2.3.9. Тогда характеристический многочлен эндоморфизма Фробениуса $\chi_{C',q}(T) \pmod p$ имеет следующий вид*

1. *если g — чётное, то*

$$(-1)^g T^g |((W_1 + JW_2)^t)_p - TI| \cdot |((W_1 - JW_2)^t)_p - TI|;$$

2. *если g — нечётное и $p \mid g$, то*

$$(-1)^g T^g \left| \left(\begin{pmatrix} P_{\frac{p-1}{2}}(-c/2) & \vec{b}J \\ 2J\vec{a} & J(W_1 + JW_2)J \end{pmatrix}^t \right)_p - TI \right| |((W_1 - JW_2)^t)_p - TI|;$$

3. *если g — нечётное и $p \nmid g$,*

$$(-1)^g T^g \cdot (N_{F_q/F_p}(P_{\frac{p-1}{2}}(-c/2)) - T) \cdot |((W_1+JW_2)^t)_p - TI| \cdot |((W_1 - JW_2)^t)_p - TI| \pmod p.$$

Заметим, что в следствии мы использовали тот факт, что транспозиция блочно-диагональной матрицы находится транспозицией блоков.

Теперь, если матрица W дополнительно является ещё и мономиальной, то мы можем сопоставить ей некоторую перестановку и представить матрицу W в виде произведения диагональной и перестановочной матриц.

Теорема 2.3.10. *Пусть W — матрица Картье-Манина кривой C' над конечным полем $\mathbb{F}_q, q = p^n$, $\gcd(p,g) = 1$. Тогда матрица W — обобщённая перестановочная с перестановкой σ, задаваемой $\sigma(i) \equiv ip - \frac{p-1}{2} \pmod g$. Пусть матрица P_σ — соответствующая перестановочная матрица, тогда*

1. *если g — чётное, то*

$$\operatorname{diag}(w_{1,\sigma(1)}, \ldots, w_{\frac{g}{2},\sigma(\frac{g}{2})}, w_{\frac{g}{2}+1,\frac{g}{2}+1-\sigma(\frac{g}{2})}, w_{\frac{g}{2}+2,\frac{g}{2}+1-\sigma(\frac{g}{2}-1)}, \ldots, w_{g,g+1-\sigma(1)}) P_\sigma.$$

2. *если g — нечётное, то*

$$\operatorname{diag}(w_{1,\sigma(1)}, \ldots, w_{\frac{g-1}{2},\sigma(\frac{g-1}{2})}, w_{\frac{g+1}{2},\frac{g+1}{2}}, w_{\frac{g+1}{2}+1,g+1-\sigma(\frac{g+1}{2}-1)}, \ldots, w_{g,g+1-\sigma(1)}) P_\sigma.$$

Доказательство. Если $\gcd(p,g) = 1$, то W — мономиальная матрица. Известно, что все мономиальные матрицы могут быть представлены в виде произведения

диагональной матрицы и перестановочной, т.е. $W = \mathrm{diag}(w_{1,\sigma(1)}, \ldots, w_{g,\sigma(g)})P_\sigma$ для некоторой перестановки σ. Из леммы 2.3.5 следует, что индексы (i,j) ненулевых элементов W удовлетворяют сравнению $ip - j \equiv \frac{p-1}{2} \pmod g$, которое и задаёт перестановку σ. Кроме того, так как матрица центросимметричная, получаем дополнительное ограничение: каждый индекс i такой, что $\sigma(i) \equiv ip - \frac{p-1}{2} \pmod g$, единственным образом определяет значение $\sigma(g+1-i)$ как $\sigma(g+1-i) \equiv g+1-\sigma(i) \pmod g$. Откуда и получаем результат теоремы. □

Теперь заметим, что матрице W_p соответствует перестановка σ^n. Кроме того, разбиению перестановки на непересекающиеся циклы соответствует факторизация характеристического многочлена её матрицы. Поэтому из разбиения на циклы перестановки σ^n можно получить факторизацию характеристического многочлена матрицы W_p и, как следствие, из формулы Манина, разложение характеристического многочлена Фробениуса кривой C' по модулю характеристики поля.

Теорема 2.3.11. *Пусть $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ — гиперэллиптическая кривая над конечным полем $\mathbb{F}_q$, $q = p^n, p > 2$, $\gcd(p,g) = 1$ и W — её матрица Картье-Манина. Тогда W — мономиальная матрица с перестановкой σ, задаваемой $\sigma(i) \equiv ip - \frac{p-1}{2} \pmod g$, а W_p — мономиальная матрица с перестановкой задаваемой $\sigma^n(i) \equiv ip^n - \frac{p^n-1}{2} \pmod g$. Если $W_p = (w'_{i,j})$ и $\sigma^n = \sigma_1\sigma_2\ldots\sigma_m$ — разбиение σ^n на непересекающиеся циклы, то*

$$\chi_{C',q}(T) \equiv T^g \prod_{j=1}^{m}(T^{|\sigma_j|} - \prod_{k=1}^{|\sigma_j|} w'_{\sigma_j(k),\sigma_j(k+1)}) \pmod p.$$

Доказательство. Если W — мономиальная матрица с перестановкой σ, то, перемножая матрицы, получаем

$$W_p = (w'_{i,j}) = (w^{p^{n-1}}_{\sigma^{n-1}(i),j} \prod_{k=0}^{n-2} w^{p^k}_{\sigma^k(i),\sigma^{k+1}(i)}), \tag{2.26}$$

где σ^k — перестановки такие, что $\sigma^k(i) \equiv ip^k - \frac{p^k-1}{2} \pmod g$ и $w'_{i,j} = 0$, для всех $j \neq \sigma^n(i)$. Следовательно, W_p — мономиальная матрица с перестановкой $\sigma^n(i) \equiv ip^n - \frac{p^n-1}{2} \pmod g$. Так как разбиение перестановки на циклы влечёт за собой факторизацию характеристического многочлена матрицы [46], получаем результат теоремы. □

В случае диагональной матрицы можно получить ещё более точный результат.

Теорема 2.3.12. *Пусть* $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ *— гиперэллиптическая кривая рода* g *над конечным полем* $\mathbb{F}_q, q = p^n, p > 2$. *Тогда*

1. *если род* g *чётный и* $p \equiv 1 \pmod{2g}$, *то*

$$\chi_{C',q}(T) \equiv T^g \prod_{i=1}^{\frac{g}{2}} (T - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{\frac{(2i-1)(p-1)}{2g}}(-c/2)))^2 \pmod{p}.$$

2. *если род* g *нечётный и* $p \equiv 1 \pmod{g}$, *то* $\chi_{C',q}(T) \pmod{p}$ *имеет вид*

$$T^g (T - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{\frac{p-1}{2}}(-c/2))) \prod_{i=1}^{\frac{g-1}{2}} (T - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{\frac{(2i-1)(p-1)}{2g}}(-c/2)))^2.$$

Теперь, если зафиксировать род g, то с помощью теорем 2.3.11, 2.3.12 и свойства центорсимметричности, мы можем перебрать все возможные многочлены Фробениуса для кривой C' по модулю характеристики для случая $\gcd(p,g) = 1, p > 2$. Полученные таким способом списки характеристических многочленов для кривых родов $g = 1 - 7$ приводим в Приложении A.

Общий случай

Для нахождения матрицы Картье-Манина кривой C мы свяжем её с матрицей кривой C' посредством следующей теоремы.

Теорема 2.3.13. *Пусть* $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ *— гиперэллиптическая кривая рода* g *над конечным полем* $\mathbb{F}_q, q = p^n, p > 2, \gcd(p,g) = 1$, $m = \frac{p-1}{2}$ *и пусть* $W = (w_{i,j}(a,b))$ *— её матрица Картье-Манина. Тогда*

1. $w_{i,j}(a,b) = b^{m+\frac{m-(ip-j)}{2g}} w_{i,j}\left(\frac{a}{\sqrt{b}}, 1\right) = b^{m+\frac{m-(ip-j)}{2g}} P_{\frac{ip-j}{g} - \frac{p-1}{2g}}\left(-\frac{a}{2\sqrt{b}}\right)$ *для* $ip - j \equiv m \pmod{g}$
2. $w_{i,j} = 0$, *в противном случае.*

Доказательство.

$$\begin{aligned} w_{i,j}(a,b) &= [x^{ip-j}](x^{2g+1} + ax^{g+1} + bx)^{\frac{p-1}{2}} = \\ &= [x^{ip-j}] \sum_{k_0+k_1+k_2=m} \binom{n}{k_0,k_1,k_2} x^{(2g+1)k_0+(g+1)k_1+k_2} a^{k_1} b^{k_2} = \\ &= \sum \binom{m}{k_0,k_1,k_2} a^{k_1} b^{k_2}, \end{aligned}$$

где сумма берётся по всем целым неотрицательным k_0,k_1,k_2, удовлетворяющим системе

$$\begin{cases} k_0 + k_1 + k_2 = m, \\ (2g+1)k_0 + (g+1)k_1 + k_2 = ip - j. \end{cases}$$

Система имеет решения только при $ip - j \equiv m \pmod g$. Следовательно,

$$\begin{aligned} w_{i,j}(a,b) &= \sum_{k_0 \geqslant 0} \binom{m}{k_0, \frac{ip-j-m}{g} - 2k_0, m + \frac{m-(ip-j)}{g} + k_0} a^{\frac{ip-j-m}{g} - 2k_0} b^{m + \frac{m-(ip-j)}{g} + k_0} = \\ &= b^{m + \frac{m-(ip-j)}{2g}} \sum_{k_0 \geqslant 0} \binom{m}{k_0, \frac{ip-j-m}{g} - 2k_0, m + \frac{m-(ip-j)}{g} + k_0} \left(\frac{a}{\sqrt{b}}\right)^{\frac{ip-j-m}{g} - 2k_0} = \\ &= b^{m + \frac{m-(ip-j)}{2g}} w_{i,j}\left(\frac{a}{\sqrt{b}}, 1\right). \end{aligned}$$

По Теореме 2.3.7 имеем $w_{i,j}(\frac{a}{\sqrt{b}}, 1) = P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{a}{2\sqrt{b}})$ для $ip - j \equiv \frac{p-1}{2} \pmod g$. □

Теорема позволяет рассчитать матрицу кривой C в случае, когда b — квадратичный вычет в поле. При этом кривые C и C' могут быть неизоморфными над базовым полем.

Заметим, что в отличии от матрицы кривой C', матрица Картье-Манина кривой C уже не является центросимметричной. Однако, как следствие из Теоремы 2.3.13, она также является мономиальной, что позволяет нам применить аналогичный случаю C' метод для нахождения всех возможных характеристических многочленов $\chi_{C,q}(T) \pmod p$.

Из Теоремы 2.3.13 следует, что матрица Картье-Манина W кривой C является мономиальной (обобщенной перестановочной) матрицей, задаваемой перестановкой σ, определенной как

$$\sigma(i) \equiv ip - \frac{p-1}{2} \pmod g.$$

Разбиению перестановки на не пересекающиеся циклы $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_k$ соответствует факторизация характеристического многочлена матрицы W:

$$\chi_W(T) = \prod_{i=1}^{k} \left(T^{|\sigma_i|} - \prod_{j=1}^{|\sigma_i|} w_{\sigma_i(j),\sigma_i(j+1)} \right). \tag{2.27}$$

Аналогичный результат имеет место для матрицы W_p, если взять $\sigma \equiv ip^n - \frac{p^n-1}{2} \pmod{p}$. По формуле Манина имеем

$$\chi_{C,q}(T) \equiv T^g \chi_{W_p}(T) \pmod{p}. \tag{2.28}$$

Сопоставляя формулу (2.28) с Теоремой 2.3.13, можно выразить $\chi_{C,q}(T) \pmod{p}$ через многочлены Лежандра.

Фиксируя род g и целое число s такое, что $p \equiv s \pmod{g}$ для нечетного рода g и $p \equiv s \pmod{2g}$ для четного рода g, мы фиксируем перестановку σ. Таким образом, для каждого рода g (при условии $\gcd(p,g) = 1$) получаем g возможных перестановок и, соответственно, такое же число возможных многочленов $\chi_C(T) \pmod{p}$.

Полученные таким методом списки характеристических многочленов для кривых рода $g = 1 - 7$ приводим в Приложении Б. Заметим, что многочлены приведены в факторизованной форме, которая имеет место над некоторым расширением поля $\mathbb{F}_p$, однако несмотря на это коэффициенты многочлена $\chi_{C,q}(T)$ после раскрытия скобок всегда принадлежат $\mathbb{F}_p$.

2.3.5 Метод подсчёта точек на основе многочленов Лежандра

В разделе §2.3.4 была показана связь матриц Картье-Манина кривой C с многочленами Лежандра и получены списки характеристических многочленов по модулю характеристики поля, выраженных через многочлены Лежандра (Приложение А и Б). Покажем теперь, как использовать эту информацию для подсчёта точек. Для этого нам осталось описать метод для восстановления коэффициентов $\chi_{C,q}(T)$ по $\chi_{C,q}(T) \pmod{p}$ и способ для вычисления многочленов Лежандра.

Первая задача может быть решена стандартным способом — перебором с использованием известных неравенств для коэффициентов характеристического многочлена:

$$|a_i| \leqslant \binom{2g}{i} q^{i/2},$$

либо более точных неравенств для фиксированных родов, например, для рода 2 известны [6; 125] следующие точные границы:

$$\lceil 2\sqrt{q}|a_1| - 2q \rceil \leqslant a_2 \leqslant \lfloor a_1^2/4 + 2q \rfloor.$$

Для решения второй задачи мы сопоставим многочленам Лежандра кривые рода 1 и выше (но меньше, чем род кривой C).

Хорошо известно, что число точек на определённых эллиптических кривых (по модулю характеристики) выражается через многочлены Лежандра. Соответственно, часть характеристических многочленов из таблиц в Приложениях А и Б может быть достаточно эффективно вычислена по алгоритму Схоофа-Элкиса-Аткина (см. [4] и [48, §17.2.2]) за время $\widetilde{\mathcal{O}}(\log^4 p)$.

Известные сопоставления многочленов Лежандра с эллиптическими кривыми приводим в следующей теореме (объединяющей результаты из работ [126—128]). Заметим, что многочлен Лежандра связан (см. преобразование в [129]) с инвариантом Хассе-Витта-Дойринга [40; 130], который широко используется при исследовании суперсингулярных эллиптических кривых.

Теорема 2.3.14. *Пусть $c \in \mathbb{F}_p, p > 3$. Тогда*

1. $P_{\frac{p-1}{2}}(c) \equiv (\frac{-6}{p})t_2 \pmod p$, *где t_2 — след эндоморфизма Фробениуса эллиптической кривой*

$$E_2 : y^2 = x^3 - 3(c^2+3)x + 2c(c^2-9).$$

2. $P_{\lfloor \frac{p}{3} \rfloor}(c) \equiv (\frac{p}{3})t_3 \pmod p$, *где t_3 — след эндоморфизма Фробениуса эллиптической кривой*

$$E_3 : y^2 = x^3 + 3(4c-5)x + 2(2c^2 - 14c + 11).$$

3. $P_{\lfloor \frac{p}{4} \rfloor}(c) \equiv (\frac{6}{p})t_4 \pmod p$, *где t_4 — след эндоморфизма Фробениуса эллиптической кривой*

$$E_4 : y^2 = x^3 - \frac{3}{2}(3c+5)x + 9c + 7.$$

4. $P_{\lfloor \frac{p}{6} \rfloor}(c) \equiv (\frac{3}{p}) t_6 \pmod{p}$, *где* $p > 5$ *и* t_6 *— след эндоморфизма Фробениуса эллиптической кривой*

$$E_6 : y^2 = x^3 - 3x + 2c.$$

С помощью данной теоремы мы можем полностью вычислить матрицу Картье-Манина кривой C в случае рода 3. Соответствующий алгоритм для подсчёта точек приводим в §3.1. Для случая $g > 3$ с помощью Теоремы 2.3.14 может быть получена частичная информация. Например, многочлен $P_{\frac{p-1}{2}}$ присутствует в таблицах Приложения А для $g = 5, 7$.

Помимо представленных в Теореме 2.3.14 многочленов возможно получение новых соотношений сопоставлением многочленов Лежандра кривым в разложении якобиана C' или C. Соответствующий метод с примером нахождения $P_{\frac{p-1}{8}}$ представляем в разделе §4.1. Кроме использования для подсчёта точек полученные сравнения интересны сами по себе, так как представляют собой обобщения известных соотношений для эллиптических кривых на гиперэллиптические кривые.

2.3.6 Выводы

Приведен пример применения общей схемы подсчёта точек из §2.2 к кривой с геометрически приводимым якобианом.

Получено полное разложение якобиана кривой C на якобианы кривых меньшей размерности с точной степенью расширения, над которым это разложение имеет место. Данный результат собирает воедино разрозненную информацию из работ [33; 41—43] и заполняет пробелы.

Спуск к базовому полю известными нам методами может быть выполнен эффективно только для отдельных случаев, которые мы рассматриваем в Главе 3. Кроме того, общие полиномиальные алгоритмы подсчёта точек уже для рода 3 имеют сложность $\widetilde{\mathcal{O}}(\log^{14} q)$ и крайне неэффективны на практике. Поэтому для подсчёта точек в общем случае мы применяем экспоненциальный метод на основе матриц Картье-Манина, который даёт нам также явные формулы.

С помощью детального исследования и использования структуры матриц Картье-Манина (центросимметричность, мономиальность) получены списки ха-

рактеристических многочленов по модулю характеристики поля. По сравнению с общими формулами для матриц Картье-Манина, которые можно получить по полиномиальной теореме, представленные списки выражены в терминах хорошо известных классических многочленов Лежандра и имеют компактный вид за счёт использования симметрий. В случае эллиптических кривых ($g = 1$) результат совпадает с классическим результатом Хассе-Витта-Дойринга [40; 130] и, таким образом, получено обобщение на кривые больших родов.

2.4 Кривые, задаваемые многочленами Диксона и Чебышева

В данном разделе рассмотрим следующие кривые, которые представляют собой фактор-кривые кривой $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ из Теоремы 2.3.3.

1. $X'_1 : y^2 = D_g(x, 1) + c$;
2. $X'_2 : y^2 = (x + 2)(D_g(x, 1) + c)$;
3. $\widetilde{X}'_2 : y^2 = (x - 2)(D_g(x, 1) + c)$;
4. $X'_3 : y^2 = (x^2 - 4)(D_g(x, 1) + c)$.

За исключением кривой X'_3 и частных случаев данные кривые уже будут иметь абсолютно простые якобианы [41, Cor. 6].

2.4.1 Обзор известных результатов

Известно [42, с. 100], что кривая X'_1 имеет структуру действительного умножения, а именно, кольцо эндоморфизмов якобиана кривой содержит подкольцо $\mathbb{Z}[\zeta_g + \zeta_g^{-1}]$, где ζ_g — примитивный корень из единицы степени g. Более того, эндоморфизм $\zeta_g + \zeta_g^{-1}$ можно построить в явном виде [42, §7.3]. В работе [74] было показано, что ожидаемая сложность подсчёта точек на таких кривых (с явным действительным умножением) равна $\widetilde{\mathcal{O}}(\log^9 q)$ для любого рода. При этом в случае рода 2 сложность ещё меньше — она равна $\widetilde{\mathcal{O}}(\log^5 q)$ [76, §4.2], а для рода 3 имеем $\widetilde{\mathcal{O}}(\log^6 q)$ [64].

Многочлен Диксона связан с многочленом Чебышева первого рода $T_g(x)$ степени g соотношением $D_g(2x, 1) = 2T_g(x)$. Это позволяет записать уравнения

X_1', X_2', $\widetilde{X}_2'$ и X_3' через многочлены Чебышева. Для кривых в таком виде над полем $\mathbb{F}_{q^2}$ работы [131; 132] содержат условия максимальности с параметром $a = 0$, при которых число точек на кривой достигает верхней границы Хассе-Вейля. В нашей работе мы получим в явном виде матрицы Картье-Манина данных кривых и списки характеристических многочленов по аналогии с кривой C'.

2.4.2 Матрица Картье-Манина.

Разбиению якобиана кривой $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ соответствует блочно-диагональная форма матрицы Картье-Манина из §2.3.4. Найдём из данной формы матрицы Картье-Манина интересующих нас кривых. Пусть W — матрица Картье-Манина кривой C'. Тогда из свойства центросимметричности W (см. доказательство Теоремы 2.3.9) следует, что $W = \begin{pmatrix} W_1 & JW_2J \\ W_2 & JW_1J \end{pmatrix}$ для чётного g и $W = \begin{pmatrix} W_1 & \vec{a} & JW_2J \\ \vec{b} & s & \vec{b}J \\ W_2 & J\vec{a} & JW_1J \end{pmatrix}$ для нечётного g.

Теорема 2.4.1. *Пусть g — чётное. Матрицы Картье-Манина гиперэллиптических кривых $X_2' : y^2 = (x+2)(D_g(x,1)+c)$ и $\widetilde{X}_2' : y^2 = (x-2)(D_g(x,1)+c)$ равны $W_1 - JW_2$ и $W_1 + JW_2$, соответственно.*

Доказательство. Для доказательства нам необходимо найти матрицы действия оператора Картье на $\mathbb{F}_q$-векторные пространства голоморфных дифференциалов функциональных полей кривых $X_2', \widetilde{X}_2'$. За определением и свойствами данных пространств отсылаем к [48, §4.4.2.c] и [80, §4]. Так как эти пространства являются подпространствами голоморфных дифференциалов $\Omega^0_{C'}$ кривой C', достаточно найти их базисы, записать их по базису $\Omega^0_{C'}$, применить оператор Картье и выполнить обратное преобразование базиса, чтобы получить матрицу действия оператора Картье на подпространство.

В случае $c = 0$ соответствующие базисы подпространств были найдены в [132, §4]. Можно показать, что они имеют такой же вид и для случая $c \neq 0$. Имеем $X_2' = C'/\langle s \rangle$ и $\widetilde{X}_2' = C'/\langle s\iota \rangle$, где $s : (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$ — инволюция и ι — гиперэллиптическая инволюция (см. Теорему 2.3.2). Поэтому функциональное

поле кривой X_2' представляет собой поле s-инвариантных функций из функционального поля кривой C'. Аналогично, функциональное поле кривой $\widetilde{X}_2'$ — это поле $s\iota$-инвариантных функций из $\mathbb{F}_q(C')$. Известно, что базис пространства голоморфных дифференциалов функционального поля кривой C' (как и любой гиперэллиптической кривой) имеет вид $\left\{\omega_i = \frac{x^{i-1}}{y}dx \mid 1 \leqslant i \leqslant g\right\}$. Напрямую можно проверить (учитывая равенство $d(1/x) = -\frac{dx}{x^2}$), что подпространства s-инвариантных дифференциалов и $s\iota$-инвариантных дифференциалов имеют базисы $\left\{\omega_i - \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g}{2}\right\}$ и $\left\{\omega_i + \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g}{2}\right\}$, соответственно.

Записывая элементы базиса $\{\omega_i \pm \omega_{g-i+1}\}$ по базису $\{\omega_i\}$, получаем матрицу:

$$\left(I_{\frac{g}{2}}; \pm J_{\frac{g}{2}}\right),$$

где элементам базиса $\{\omega_i \pm \omega_{g-i+1}\}$ соответствуют строки матрицы.

Оператор Картье $\mathfrak{C}$ действует на $\Omega^0_{C'}$ следующим образом:

$$\mathfrak{C}\begin{pmatrix}\omega_1\\ \omega_2\\ \dots\\ \omega_g\end{pmatrix} = W^{(1/p)}\begin{pmatrix}\omega_1\\ \omega_2\\ \dots\\ \omega_g\end{pmatrix}.$$

Поэтому действие оператора Картье на пространства $\Omega^0_{X_1'}, \Omega^0_{\widetilde{X}_1'}$ задаётся следующей матрицей.

$$\left(I_{\frac{g}{2}}; \pm J_{\frac{g}{2}}\right) \cdot \begin{pmatrix}W_1 & JW_2J\\ W_2 & JW_1J\end{pmatrix} = \begin{pmatrix}W_1 \pm JW_2\\ W_1J \pm JW_2J\end{pmatrix}.$$

После приведения строк матрицы к базису $\{\omega_i \pm \omega_{g-i+1}\}$ (умножением нижнего блока на матрицу J) получаем, что оператор Картье действует на данный базис умножением на матрицу $W_1 \pm JW_2$. □

Теорема 2.4.2. *Пусть g — нечётное целое. Матрицы Картье-Манина гиперэллиптических кривых $X_1' : y^2 = D_g(x,1) + c$ и $X_3' : y^2 = (x^2-4)(D_g(x,1)+c)$ равны $W_1 - JW_2$ и $\begin{pmatrix}W_1 + JW_2 & \vec{a}\\ \vec{b} & s\end{pmatrix}$, соответственно.*

Доказательство. Доказывается аналогично предыдущей теореме, учитывая, что базис s-инвариантных дифференциалов равен $\left\{\omega_i - \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g-1}{2}\right\}$, а базис $s\iota$-инвариантных дифференциалов равен $\left\{\omega_i + \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g+1}{2}\right\}$.

Записывая $\{\omega_i - \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g-1}{2}\}$ и $\{\omega_i + \omega_{g-i+1} | 1 \leqslant i \leqslant \frac{g+1}{2}\}$ по базису $\{\omega_i\}$, получаем матрицы

$$\begin{pmatrix} I & \vec{0} & -J \\ \vec{0}^t & 0 & \vec{0}^t \end{pmatrix}$$

и

$$\begin{pmatrix} I & \vec{0} & J \\ \vec{0}^t & 2 & \vec{0}^t \end{pmatrix},$$

где I — единичная матрица размера $\frac{g-1}{2} \times \frac{g-1}{2}$, J — обменная матрица размера $\frac{g-1}{2} \times \frac{g-1}{2}$ и $\vec{0}$ — нулевой вектор-столбец размера $\frac{g-1}{2}$.

Имея матричную запись базисов s и $s\iota$-инвариантных подпространств $\Omega^0_{C'}$ относительно базиса $\{\omega_i\}$, мы теперь можем применить оператор Картье и получить матрицы, соответствующие действию оператора Картье на эти подпространства:

$$\begin{pmatrix} I & \vec{0} & -J \\ \vec{0}^t & 0 & \vec{0}^t \end{pmatrix} \cdot W = \begin{pmatrix} W_1 & \vec{0} & JW_2J - W_1J \\ \vec{0}^t & 0 & \vec{0}^t \end{pmatrix}$$

и

$$\begin{pmatrix} I & \vec{0} & J \\ \vec{0}^t & 2 & \vec{0}^t \end{pmatrix} \cdot W = \begin{pmatrix} W_1 + JW_2 & 2\vec{a} & JW_2J + W_1J \\ 2\vec{b} & 2s & 2\vec{b}J \end{pmatrix}.$$

После обратного преобразования базиса получаем искомый результат. □

Так как элементы матрицы W представляют собой многочлены Лежандра, мы можем записать через них и матрицы кривых $X'_1, X'_2, \widetilde{X}'_2$ и X'_3.

Следствие 2.4.2.1. *Пусть g — чётное целое. Для матриц Картье-Манина $W' = (w'_{i,j}), \widetilde{W}' = (\widetilde{w}'_{i,j})$ гиперэллиптических кривых $X'_2 : y^2 = (x+2)(D_g(x,1)+c)$ и $\widetilde{X}'_2 : y^2 = (x-2)(D_g(x,1)+c)$ 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 $1 \leqslant i,j \leqslant \frac{g}{2}$ и P_m — многочлен Лежандра степени m. При этом в случае $m \notin \mathbb{Z}$ полагаем $P_m = 0$.

Доказательство. Из Теоремы 2.3.7 имеем для матрицы Картье-Манина кривой C': $W = (w_{i,j}) = (P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}))$. Поэтому $w'_{i,j} = w_{i,j} - w_{g-i} = P_{\frac{ip-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2}) - P_{\frac{(g-i)p-j}{g} - \frac{p-1}{2g}}(-\frac{c}{2})$ для $i = 1, \ldots, \frac{g-1}{2}$. Аналогично для $\widetilde{w}'_{i,j}$. □

Следствие 2.4.2.2. *Пусть g — нечётное целое. Для матриц Картье-Манина $W' = (w'_{i,j}), \widetilde{W}' = (\widetilde{w}'_{i,j})$ гиперэллиптических кривых $X'_1 : y^2 = D_g(x,1) + c$ и $X'_3 : y^2 = (x^2-4)(D_g(x,1)+c)$ над конечным полем $\mathbb{F}_q$ выполняется:*

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

Здесь P_m — многочлен Лежандра степени m. При этом в случае $m \notin \mathbb{Z}$ полагаем $P_m = 0$.

Доказательство. Аналогично предыдущему следствию. □

2.4.3 Характеристические многочлены (mod p)

Так как нам теперь известны матрицы Картье-Манина кривых $X'_1, X'_2, \widetilde{X}'_2$ и X'_3, то мы можем построить списки характеристических многочленов (mod p), аналогичные Таблице Б для кривой C. Причём в отличии от кривой C данные кривые в общем случае могут иметь абсолютно простой якобиан. В Таблице 5 представлены характеристические многочлены (mod p) кривых $X'_1 : y^2 = D_g(x,1) + c$ рода $\frac{g-1}{2}$ над $\mathbb{F}_p$, выраженные через многочлены Лежандра $P_m := P_m(-\frac{c}{2})$, где $p > 2$, $\gcd(p,g) = 1$, и g — нечётное простое. Аналогично, Таблица 6 содержит характеристические многочлены (mod p) кривых $X'_2 : y^2 = (x+2)(D_g(x,1)+c)$ рода 2 и 4 над $\mathbb{F}_p$.

2.4.4 Выводы

Найдены матрицы Картье-Манина для кривых, задаваемых многочленами Диксона. Для кривых X'_1, X'_2 получены аналогичные кривой C' списки характеристических многочленов по модулю p, выраженные через многочлены Лежандра.

Таблица 5 — Характеристические многочлены кривых $X_1' : y^2 = D_g(x,1) + c$.

Род	Условия	$\chi_{X_1',p}(T) \pmod p$
2	$p \equiv 1 \pmod 5$	$T^2(T - P_{\frac{3p-3}{10}})(T - P_{\frac{p-1}{10}})$
2	$p \equiv 2 \pmod 5$	$T^2(T^2 + P_{\frac{3p-1}{10}} P_{\frac{p-7}{10}})$
2	$p \equiv 3 \pmod 5$	$T^2(T^2 + P_{\frac{3p-9}{10}} P_{\frac{p-3}{10}})$
2	$p \equiv 4 \pmod 5$	$T^2(T + P_{\frac{3p-7}{10}})(T + P_{\frac{p-9}{10}})$
3	$p \equiv 1 \pmod 7$	$T^3(T - P_{\frac{5p-5}{14}})(T - P_{\frac{3p-3}{14}})(T - P_{\frac{p-1}{14}})$
3	$p \equiv 2 \pmod 7$	$T^3(T^3 - P_{\frac{5p-3}{14}} P_{\frac{3p-13}{14}} P_{\frac{p-9}{14}})$
3	$p \equiv 3 \pmod 7$	$T^3(T^3 + P_{\frac{5p-1}{14}} P_{\frac{3p-9}{14}} P_{\frac{p-3}{14}})$
3	$p \equiv 4 \pmod 7$	$T^3(T^3 - P_{\frac{5p-13}{14}} P_{\frac{3p-5}{14}} P_{\frac{p-11}{14}})$
3	$p \equiv 5 \pmod 7$	$T^3(T^3 + P_{\frac{5p-11}{14}} P_{\frac{3p-1}{14}} P_{\frac{p-5}{14}})$
3	$p \equiv 6 \pmod 7$	$T^3(T + P_{\frac{5p-9}{14}})(T + P_{\frac{3p-11}{14}})(T + P_{\frac{p-13}{14}})$
5	$p \equiv 1 \pmod{11}$	$T^5(T - P_{\frac{9p-9}{22}})(T - P_{\frac{7p-7}{22}})(T - P_{\frac{5p-5}{22}})(T - P_{\frac{3p-3}{22}})(T - P_{\frac{p-1}{22}})$
5	$p \equiv 2 \pmod{11}$	$T^5(T^5 + P_{\frac{9p-7}{22}} P_{\frac{7p-3}{22}} P_{\frac{5p-21}{22}} P_{\frac{3p-17}{22}} P_{\frac{p-13}{22}})$
5	$p \equiv 3 \pmod{11}$	$T^5(T^5 - P_{\frac{9p-5}{22}} P_{\frac{7p-21}{22}} P_{\frac{5p-15}{22}} P_{\frac{3p-9}{22}} P_{\frac{p-3}{22}})$
5	$p \equiv 4 \pmod{11}$	$T^5(T^5 - P_{\frac{9p-3}{22}} P_{\frac{7p-17}{22}} P_{\frac{5p-9}{22}} P_{\frac{3p-1}{22}} P_{\frac{p-15}{22}})$
5	$p \equiv 5 \pmod{11}$	$T^5(T^5 - P_{\frac{9p-1}{22}} P_{\frac{7p-13}{22}} P_{\frac{5p-3}{22}} P_{\frac{3p-15}{22}} P_{\frac{p-5}{22}})$
5	$p \equiv 6 \pmod{11}$	$T^5(T^5 + P_{\frac{9p-21}{22}} P_{\frac{7p-9}{22}} P_{\frac{5p-19}{22}} P_{\frac{3p-7}{22}} P_{\frac{p-17}{22}})$
5	$p \equiv 7 \pmod{11}$	$T^5(T^5 + P_{\frac{9p-19}{22}} P_{\frac{7p-5}{22}} P_{\frac{5p-13}{22}} P_{\frac{3p-21}{22}} P_{\frac{p-7}{22}})$
5	$p \equiv 8 \pmod{11}$	$T^5(T^5 + P_{\frac{9p-17}{22}} P_{\frac{7p-1}{22}} P_{\frac{5p-7}{22}} P_{\frac{3p-13}{22}} P_{\frac{p-19}{22}})$
5	$p \equiv 9 \pmod{11}$	$T^5(T^5 - P_{\frac{9p-15}{22}} P_{\frac{7p-19}{22}} P_{\frac{5p-1}{22}} P_{\frac{3p-5}{22}} P_{\frac{p-9}{22}})$
5	$p \equiv 10 \pmod{11}$	$T^5(T + P_{\frac{9p-13}{22}})(T + P_{\frac{7p-15}{22}})(T + P_{\frac{5p-17}{22}})(T + P_{\frac{3p-19}{22}})(T + P_{\frac{p-21}{22}})$

Таблица 6 — Характеристические многочлены кривых $X_2' : y^2 = (x+2)(D_g(x,1)+c)$.

Род	Условия	$\chi_{X_2',p}(T) \pmod p$
2	$p \equiv 1 \pmod 8$	$T^2(T - P_{\frac{p-1}{8}})(T - P_{\frac{3p-3}{8}})$
2	$p \equiv 3 \pmod 8$	$T^2(T^2 - P_{\frac{3p-1}{8}} P_{\frac{p-3}{8}})$
2	$p \equiv 5 \pmod 8$	$T^2(T^2 - P_{\frac{3p-7}{8}} P_{\frac{p-5}{8}})$
2	$p \equiv 7 \pmod 8$	$T^2(T + P_{\frac{3p-5}{8}})(T + P_{\frac{p-7}{8}})$
4	$p \equiv 1 \pmod{16}$	$T^4(T - P_{\frac{7p-7}{16}})(T - P_{\frac{5p-5}{16}})(T - P_{\frac{3p-3}{16}})(T - P_{\frac{p-1}{16}})$
4	$p \equiv 3 \pmod{16}$	$T^4(T^4 - P_{\frac{7p-5}{16}} P_{\frac{5p-15}{16}} P_{\frac{3p-9}{16}} P_{\frac{p-3}{16}})$
4	$p \equiv 5 \pmod{16}$	$T^4(T^4 - P_{\frac{7p-3}{16}} P_{\frac{5p-9}{16}} P_{\frac{3p-15}{16}} P_{\frac{p-5}{16}})$
4	$p \equiv 7 \pmod{16}$	$T^4(T^2 - P_{\frac{5p-3}{16}} P_{\frac{3p-5}{16}})(T^2 - P_{\frac{7p-1}{16}} P_{\frac{p-7}{16}})$
4	$p \equiv 9 \pmod{16}$	$T^4(T^2 - P_{\frac{5p-13}{16}} P_{\frac{3p-11}{16}})(T^2 - P_{\frac{7p-15}{16}} P_{\frac{p-9}{16}})$
4	$p \equiv 11 \pmod{16}$	$T^4(T^4 - P_{\frac{7p-13}{16}} P_{\frac{5p-7}{16}} P_{\frac{3p-1}{16}} P_{\frac{p-11}{16}})$
4	$p \equiv 13 \pmod{16}$	$T^4(T^4 - P_{\frac{7p-11}{16}} P_{\frac{5p-1}{16}} P_{\frac{3p-7}{16}} P_{\frac{p-13}{16}})$
4	$p \equiv 15 \pmod{16}$	$T^4(T + P_{\frac{7p-9}{16}})(T + P_{\frac{5p-11}{16}})(T + P_{\frac{3p-13}{16}})(T + P_{\frac{p-15}{16}})$

Глава 3. Специализированные алгоритмы и формулы

3.1 Алгоритм для рода $g = 3$ на основе многочленов Лежандра

Пусть дана гиперэллиптическая кривая рода 3 вида:

$$C/\mathbb{F}_p : y^2 = x^7 + ax^4 + bx.$$

В данном случае имеем $\mathrm{Jac}_C(\mathbb{F}_q) \sim E \times A$ для некоторой абелевой поверхности A. Для нахождения $\chi_{C,q}(T)$ необходимо найти характеристический многочлен

$$\chi_{A,p}(T) = T^4 - s_1T^3 + s_2T^2 - s_1pT + p^2.$$

Для нахождения коэффициентов s_1, s_2 вычислим $\chi_{A,p}(T) \pmod p$, используя таблицы из Приложения Б, и затем определим s_1, s_2, используя неравенства $|s_1| \leqslant 4\sqrt{p}$ и $|s_2| \leqslant 6p$ по методу из работы [112, Алгоритм 1]. Сначала составим список возможных кандидатов для s_1,s_2 и затем определим правильный умножением случайного элемента $\mathrm{Jac}_C(\mathbb{F}_p)$ на $\#\,\mathrm{Jac}_C(\mathbb{F}_p) = 1 + p^2 + s_1(p+1) + s_2$. Для правильного варианта умножение должно обращать случайный элемент в единичный. Таким образом, вычисление $\chi_{C,p}(T)$ состоит в следующем. Из Таблицы 10 имеем

$$\chi_{C,p}(T) \equiv T^3(T - b_2P_{\frac{p-1}{2}})(T - b_6^5P_{\frac{p-1}{6}})(T - b_6P_{\frac{p-1}{6}}) \pmod p$$

для $p \equiv 1 \pmod 3$ и

$$\chi_{C,p}(T) \equiv T^3(T - b_2P_{\frac{p-1}{2}})(T^2 - b_2^2P_{\frac{p-5}{6}}^2) \pmod p$$

для $p \equiv 2 \pmod 3$. Здесь $b_i = \sqrt{b}^{\frac{p-1}{i}}$.

Вычисление многочленов Лежандра $P_{\frac{p-1}{2}}, P_{\frac{p-1}{6}}, P_{\frac{p-5}{6}}$ в случае $\sqrt{b} \in \mathbb{F}_p$ может быть выполнено по Теореме 2.3.14 с помощью алгоритма Схоофа-Элкиса-Аткина.

В случае $\sqrt{b} \notin \mathbb{F}_p$ значения наших многочленов Лежандра не лежат в поле $\mathbb{F}_p$. В этом случае мы вычисляем $\chi_{C,p^2}(T) = \chi_{E,p^2}(T) \cdot \chi_{A,p^2}(T) \pmod p$ и находим $\chi_{C,p}(T) \pmod p$, решая систему

$$s_{1,2} \equiv s_1^2 - 2s_2,\ s_{2,2} \equiv s_2^2 \pmod p, \tag{3.1}$$

где $s_{1,2}$ и $s_{2,2}$ — коэффициенты многочлена $\chi_{A,p^2}(T)$. Характеристический многочлен $\chi_{C,p^2}(T) \pmod p$ находим по методу из §2.3.5:

$$\chi_{C,p^2}(T) \equiv T^3(T - \sqrt{b}^{\frac{p^2-1}{2}} P^{p+1}_{\frac{p-1}{2}})(T - \sqrt{b}^{\frac{5p^2-5}{6}} P^{p+1}_{\frac{p-1}{6}})(T - \sqrt{b}^{\frac{p^2-1}{6}} P^{p+1}_{\frac{p-1}{6}}) \pmod p$$

для $p \equiv 1 \pmod 3$ и

$$\chi_{C,p^2}(T) \equiv T^3(T - \sqrt{b}^{\frac{p^2-1}{2}} P^{p+1}_{\frac{p-1}{2}})(T - \sqrt{b}^{\frac{5p^2-5}{6}} P^{p+1}_{\frac{p-5}{6}})(T - \sqrt{b}^{\frac{p^2-1}{6}} P^{p+1}_{\frac{p-5}{6}}) \pmod p$$

в случае $p \equiv 2 \pmod 3$. Вычисление $P^{p+1}_{\frac{p-1}{2}}, P^{p+1}_{\frac{p-1}{6}}, P^{p+1}_{\frac{p-5}{6}}$ эквивалентно нахождению следов эндоморфизма Фробениуса $t_{2,2}, t_{6,2}$ для эллиптических кривых E_2, E_6 (из Теоремы 2.3.14) над $\mathbb{F}_{p^2}$. Это может быть выполнено по алгоритму Схоофа-Элкиса-Аткина. После решения (3.1) определение $\chi_{C,p}(T)$ по $\chi_{C,p}(T) \pmod p$ выполняется таким же способом, как и в случае $\sqrt{b} \in \mathbb{F}_p$. Однако в данном случае получается больше кандидатов, так как решений (3.1) два. Описанный метод ведёт к Алгоритму 3.

Алгоритм 3: Вычисление характеристического многочлена $\chi_{C,p}(T)$ для гиперэллиптической кривой рода 3 вида $C : y^2 = x^7 + ax^4 + bx$.

Input: $a, b \in \mathbb{F}_p$, $p > 2$.

Output: $\chi_{C,p}(T)$.

1 Вычислить след Фробениуса t_2 кривой $y^2 = x^3 + ax^2 + bx$ над $\mathbb{F}_p$;
2 **if** $\sqrt{b} \in \mathbb{F}_p$ **then**
3 $\quad c \leftarrow -\frac{a}{2\sqrt{b}} \in \mathbb{F}_p$;
4 $\quad$ Вычислить след Фробениуса t_6 кривой $E_6 : y^2 = x^3 - 3x + 2c$ над $\mathbb{F}_p$;
5 $\quad$ **if** $p \equiv 1 \pmod 3$ **then**
6 $\quad\quad \widetilde{s}_1 \leftarrow -(\frac{3}{p}) t_6 (\sqrt{b}^{\frac{5p-5}{6}} + \sqrt{b}^{\frac{p-1}{6}})$;
7 $\quad\quad \widetilde{s}_2 \leftarrow t_6^2$;
8 $\quad$ **else if** $p \equiv 2 \pmod 3$ **then**
9 $\quad\quad \widetilde{s}_1 \leftarrow 0$;
10 $\quad\quad \widetilde{s}_2 \leftarrow -t_6^2$;
11 $\quad \chi_{A,p}(T) \pmod p \leftarrow T^4 + \widetilde{s}_1 T^3 + \widetilde{s}_2 T^2 + \widetilde{s}_1 pT + p^2$;
12 $\quad$ Восстановить $\chi_{A,p}(T)$ по $\chi_{A,p}(T) \pmod p$;
else
13 $\quad c \leftarrow -\frac{a}{2\sqrt{b}} \in \mathbb{F}_{p^2}$;
14 $\quad$ Вычислить след Фробениуса $t_{6,2}$ кривой $E_6 : y^2 = x^3 - 3x + 2c$ над $\mathbb{F}_{p^2}$;
15 $\quad \widetilde{s}_{1,2} \leftarrow \pm t_{6,2} (\sqrt{b}^{\frac{5p^2-5}{6}} + \sqrt{b}^{\frac{p^2-1}{6}})$;
16 $\quad \tilde{s}_{2,2} \leftarrow t_{6,2}^2$;
17 $\quad \chi_{A,p^2}(T) \pmod p \leftarrow T^4 + \widetilde{s}_{1,2} T^3 + \widetilde{s}_{2,2} T^2 + \widetilde{s}_{1,2} p^2 T + p^4$;
18 $\quad$ Восстановить $\chi_{A,p}(T)$ по $\chi_{A,p^2}(T) \pmod p$;
end
return $(T^2 - t_2 T + p)\chi_{A,p}(T)$

Предложение 5. *Подсчёт числа точек на гиперэллиптических кривых рода* 3 *вида* $C : y^2 = x^7 + ax^4 + bx$ *над конечным полем* $\mathbb{F}_p$ *с помощью Алгоритма 3 имеет вероятностную сложность* $\widetilde{\mathcal{O}}(\log^4 p)$ *битовых операций.*

Доказательство. Следы Фробениуса на шагах 1, 4 и 14 могут быть вычислены с помощью алгоритма Схоофа-Элкиса-Аткина за (вероятностное) время $\widetilde{\mathcal{O}}(\log^4 p)$ битовых операций.

Шаг 2 эквивалентен вычислению символа Лежандра со сложностью $\widetilde{\mathcal{O}}(\log^2 p)$ битовых операций при использовании быстрых алгоритмов возведения в степень. Вычисления квадратных корней на шагах 3, 13 может быть выполнено за время $\widetilde{\mathcal{O}}(\log^2 p)$ битовых операций [69; 133] с помощью алгоритма Чиполы.

Так как p — нечётное простое, $p \equiv 1 \pmod 3$ и для $p = 3$ кривая не гиперэллиптическая, то числа $(5p-5)/6, (p-1)/6, (5p^2-5)/6, (p^2-1)/6$ — целые. Поэтому шаги 6, 15 не требуют извлечения корней и могут быть выполнены за время $\widetilde{\mathcal{O}}(\log^2 p)$ с помощью быстрого возведения в степень.

На шаге 12 для восстановления $\chi_{A,p}(T)$ по $\chi_{A,p}(T) \pmod p$ мы используем неравенства $|s_1| \leqslant 4\sqrt{p}, |s_2| \leqslant 6p$ и значения $s_1, s_2 \pmod p$ для восстановления списка возможных пар (s_1, s_2). После чего мы исключаем лишние пары умножением $N = (1 - t_2 + q)(1 + p^2 + s_1(p+1) + s_2)$ на $\mathcal{O}(1)$ случайных элементов якобиана Jac_C. Из неравенств следует, что список имеет размер $\mathcal{O}(1)$. Генерация случайного элемента якобиана Jac_C занимает три извлечения квадратного корня в $\mathbb{F}_p$. Вычисление умножения элемента якобиана на N может быть выполнено за время $\mathcal{O}(\log N) = O(\log p)$ групповых операций в Jac_C. Одна операция имеет сложность $\widetilde{\mathcal{O}}(\log p)$, используя алгоритм Кантора [31]. Таким образом, общая сложность шага 12 равна $\widetilde{\mathcal{O}}(\log^2 p)$ битовых операций.

На шаге 18 мы сначала решаем систему (3.1), получая до 4 возможных вариантов для $\chi_{C,p}(T) \pmod p$. Это требует два вычисления квадратного корня в $\mathbb{F}_p$. После чего мы выполняем для каждого $\chi_{C,p}(T) \pmod p$ такие же операции, как на шаге 12 с такой же сложностью.

В итоге, наиболее времязатратная операция в алгоритме — вычисление следов Фробениуса $t_2, t_6, t_{6,2}$, поэтому Алгоритм 3 имеет вероятностную сложность $\widetilde{\mathcal{O}}(\log^4 p)$ битовых операций.

Заметим, что на шагах 12, 18 в редких случаях может получится несколько вариантов для $\chi_{A,p}(T)$, так как тест проходят все N, имеющие большой общий множитель с $\#\,\mathrm{Jac}_C(\mathbb{F}_p)$. Более того, в ещё более редком случае может быть два варианта для (s_1, s_2) с $N = \#\,\mathrm{Jac}_C(\mathbb{F}_p)$.

В случае возникновения нескольких (s_1, s_2), мы можем использовать результат Сазерленда [108, Лемма 4], который утверждает, что для достаточно большого значения p коэффициенты $\chi_{C,p}(T)$ единственным образом определяются по значениям $\chi_{C,p}(1)$ и $\chi_{C,p}(-1)$. Значение $\chi_{C,p}(-1)$ — число точек в $\mathrm{Jac}_{\widetilde{C}}(\mathbb{F}_p)$ — якобиане квадратичного кручения $\widetilde{C}$ кривой C и $\chi_{\widetilde{C}}(T) = \chi_C(-T)$.

В качестве $\widetilde{C}$ подходит любое квадратичное кручение, возьмём следующее:

$$\widetilde{C} : y^2 = x^7 + au^3x^4 + bu^6x,$$

где u — квадратичный невычет в поле $\mathbb{F}_p$. Соответствующий изоморфизм $C \simeq \widetilde{C}$ над $\mathbb{F}_{p^2}$ имеет вид $(x, y) \mapsto (u^{-1}x, u^{-\frac{7}{2}}y)$. Таким образом, мы можем запустить алгоритм ещё раз, подав на вход $\widetilde{C}$, получить список возможных вариантов для $\chi_{\widetilde{C},p}$ и сопоставить списки, отсеяв (s_1, s_2), которых нет в обоих списках.

В случае, если при прохождении всех проверок всё равно получается несколько вариантов для $\chi_{C,p}$, то алгоритм возвращает ошибку и список многочленов. Так как в редких случаях возможны ошибки, Алгоритм 3 принадлежит к классу вероятностных алгоритмов. Кроме того, используемый для расчёта следов Фробениуса алгоритм Схоофа-Элкиса-Аткина также является вероятностным. □

Реализация и примеры. Алгоритм был реализован в системе компьютерной алгебры Sage [134]. Исходный код можно найти на личной странице автора[1].

Пример 3.1.1. Пусть $p = fa16da0d09e774b881f9a8836ccc55d1$ (размер 128-бит),

$$a = e565b9386557e274880cd235cd733d8c,$$
$$b = aacc117a8fefc11ca37befa58beb2be9.$$

Применяя алгоритм, получаем

$$t_2 = 4d089c83177cc1f8,$$
$$s_1 = 945309b8f7ad6614,$$
$$s_2 = a426bbdfdd37d53206f17355b5106441.$$

Для краткости значения приведены по основанию шестнадцатеричной системы исчисления. Вычисления заняли 7.01 секунд на ноутбуке с процессором Core i7-4700HQ, 2.40GHz. Многочлены $\chi_{p,A}(T)$ и $\chi_{p^2,A}(T)$ являются неприводимыми над $\mathbb{Q}$ и, соответственно, абелева поверхность A простая над полями $\mathbb{F}_p$ и $\mathbb{F}_{p^2}$. Число точек A равно

$$\#A(\mathbb{F}_p) = f450a3ebab4ff949332678949cc73c566b8ea584ae41c426300701830bde70c9.$$

[1] https://crypto-kantiana.com/semyon.novoselov/src/lp_curves/g3_alg.ipynb

Оно имеет большой делитель:

$$r = e27313cdfeb582ed1111bb6c69c2ac8686d667414686 4b7$$

размера 187-бит.

Пример 3.1.2. Для использования в криптографии якобиан кривой должен содержать подгруппу большого простого порядка r размера минимум 256 бит, т. е. $r > 2^{255}$. Это требуемый стандартами ГОСТ 34.10-2018 и NIST размер группы для стойкости подгруппы точек эллиптических кривых к атаке ρ-методом Полларда. Так как алгоритм работает в любой абелевой группе, данное требование распространяется и на размер подгруппы якобиана.

Покажем на примере, что Алгоритм 3 может быть использован для нахождения кривых с таким свойством. Имеем $\mathrm{Jac_C}(\mathbb{F}_p) \sim E \times A$, поэтому нам нужно найти кривую C якобиан которой содержит абелеву поверхность A с числом точек, близким к простому. Возьмем поле $\mathbb{F}_p$ размера 128 бит:

$$p = b8f1c70570a105ab167718f29ac140b5,$$

где простое число p представлено в шестнадцатеричной системе счисления.

Выбирая случайные коэффициенты $a, b \in \mathbb{F}_p$ и применяя к ним Алгоритм 3, после достаточно большого количества итераций можно найти кривую с простым числом точек $r = \#A(\mathbb{F}_p)$:

$$a = 3a55c031b0e04911dab20f29af712b8e,$$
$$b = 730b82ddda1819bb43014650f43bb5eb$$

и

$$r = 859c727024defc8b8ee1533ed8c992b41e559b27aca96a7485a4914927c0373d.$$

Вычисление заняло 1 ч. 57 мин. на ноутбуке с процессором Core i7-4700HQ, 2.40GHz. Число r имеет размер в 256 бит, соответственно, абелева поверхность A подходит для криптографии на основе задачи вычисления дискретного логарифма. Характеристический многочлен A имеет вид

$$\chi_{A,p}(T) = T^4 + s_1T^3 + s_2T^2 + s_1pT + p^2,$$

где

$$s_1 = 1679f8e9dad36939c,$$
$$s_2 = 1403f1e6b427e83664335d388d82b465b.$$

Применяя рекуррентные формулы из Приложения B, можно также найти и $\chi_{A,p^2}(T)$. Оба многочлена $\chi_{A,p}(T), \chi_{A,p^2}(T)$ неприводимы над $\mathbb{Q}$, и поэтому абелева поверхность A проста над полями $\mathbb{F}_p$ и $\mathbb{F}_{p^2}$.

Другой способ подсчёта точек в данном случае — это получить явные формулы для $\#\operatorname{Jac}_C(\mathbb{F}_q)$ по аналогии с работой [39] для рода 2.

3.2 Явные формулы для рода 3 на основе разложения якобиана

В данном разделе мы получим для кривых рода 3 полное разложение якобиана на эллиптические кривые над расширением поля и выведем явные формулы для коэффициентов характеристического многочлена кривой над базовым полем, выразив их через следы Фробениуса эллиптических кривых. Так как следы Фробениуса могут быть достаточно эффективно вычислены с помощью алгоритма SEA [4], в результате получаем эффективный метод для подсчёта точек на таких кривых.

Пусть $C : y^2 = x^7 + ax^4 + bx$ — это гиперэллиптическая кривая рода 3 над полем $\mathbb{F}_q$ характеристики $p > 2$. Так как существует морфизм

$$(x,y) \mapsto (x^3, xy)$$

из C в эллиптическую кривую $E_1 : y^2 = x^3 + ax^2 + bx$, имеем

$$\operatorname{Jac}_C \sim E_1 \times A$$

над $\mathbb{F}_q$ для абелевой поверхности A. Следовательно,

$$\chi_{C,q}(T) = \chi_{E_1,q}(T)\chi_{A,q}(T).$$

Характеристический многочлен для E_1 может быть достаточно эффективно вычислен с помощью алгоритма SEA. Поэтому нам остаётся только найти коэффициенты $\chi_{A,q}(T) = T^4 - s_1T^3 + s_2T^2 - s_1qT + q^2$. Из разложения якобиана (см. §2.3.2) имеем

$$\operatorname{Jac}_C \sim E_2 \times \operatorname{Jac}_D$$

над $\mathbb{F}_q[\sqrt[3]{b}]$, где E_2 — эллиптическая кривая с уравнением

$$y^2 = x^3 - 3\sqrt[3]{b}x + a$$

и D — гиперэллиптическая кривая

$$y^2 = (x^2 - 4\sqrt[3]{b})(x^3 - 3\sqrt[3]{b}x + a).$$

Заметим, что $E_1 \not\sim E_2$ в общем случае, поэтому Jac_D также раскладывается на эллиптические кривые $\mathrm{Jac}_D \sim E_1 \times E$ для некоторой эллиптической кривой E. Рассмотрим сначала самый простой случай, когда b является кубическим вычетом.

Теорема 3.2.1. *Пусть $C : y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3 над конечным полем $\mathbb{F}_q, q = p^n, p > 3$ и пусть — b кубический вычет. Тогда*

1. *при $q \equiv 1 \pmod 6$ имеем $\mathrm{Jac}_C \sim E_1 \times E_2^2$ над $\mathbb{F}_q$ и*

$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)^2,$$

   где $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$ — эллиптические кривые со следами Фробениуса t_1, t_2.
2. *при $q \equiv 5 \pmod 6$ имеем $\mathrm{Jac}_C \sim E_1 \times E_2 \times \widetilde{E}_2$ над $\mathbb{F}_q$ и*

$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)(T^2 + t_2T + q),$$

   где $\widetilde{E}_2$ — квадратичное кручение E_2.

Доказательство. 1. Так как b — кубический вычет и $q \equiv 1 \pmod 6$, то все три корня 3-ей степени из b лежат в $\mathbb{F}_q$. Если b_1 — один из корней и ζ_3 — примитивный корень третьей степени, то два других корня имеют вид $b_2 = \zeta b_1$ и $b_3 = \zeta^2 b_1$. Для каждого корня b_i можно определить (Теорема 2.3.3) автоморфизм $\sigma_i : (x, y) \mapsto (\frac{b_i}{x}, \frac{yb_i^2}{x^4})$ для которого $C/\langle\sigma_i\rangle = E_2^{(i)} : y^2 = x^3 - 3b_ix + a$.

Так как на кривой есть две негиперэллиптические инволюции, то имеем $\mathcal{D}_4 \times \mathbb{Z}_2 \subseteq \mathrm{Aut}_C$, где $\mathcal{D}_4 = \langle \sigma_1, \sigma_2 \mid \sigma_1^2 = 1, \sigma_2^2 = 1, \sigma_1\sigma_2\sigma_1 = \sigma_1^{-1} \rangle$ и $\mathbb{Z}_2 = \langle\iota\rangle$. Из работы [33, Th. 5] известно, что якобиан кривой рода 3 с такой группой автоморфизмов распадается на три эллиптические кривые. Однако, модели кривых даны только над алгебраическим замыканием поля. Найдём их для нашего случая аналогичным методом.

Применяя теорему Кани-Роузена [45, Th. B], получаем разложение якобиана

$$\mathrm{Jac}_C \times \mathrm{Jac}^2_{C/\langle\sigma_2,\sigma_1\rangle} \sim \mathrm{Jac}_{C/\langle\sigma_2\rangle} \times \mathrm{Jac}_{C/\langle\sigma_1\rangle} \times \mathrm{Jac}_{C/\langle\sigma_2\sigma_1\rangle}.$$

Имеем $\mathrm{Jac}_{C/\langle\sigma_1\rangle} = E_2^{(1)}, \mathrm{Jac}_{C/\langle\sigma_1\rangle} = E_2^{(2)}$ и $\mathrm{Jac}_{C/\langle\sigma_2\sigma_1\rangle} = E_1$, поэтому род кривой $C/\langle\sigma_2,\sigma_1\rangle$ равен 0 и мы убираем её якобиан из разложения.

Кривые $E_2^{(1)}$ и $E_2^{(2)}$ изоморфны, поэтому в итоге получаем разложение:

$$\mathrm{Jac}_C \sim E_1 \times E_2^2.$$

2. Так как в данном случае имеем $q \equiv 2 \pmod 3$, то каждый элемент поля $\mathbb{F}_q$ является кубическим вычетом, и существует только один корень из b третьей степени. Соответственно, существует только одна негиперэллиптическая инволюция $\sigma : (x, y) \mapsto (\frac{\sqrt[3]{b}}{x}, \frac{y\sqrt[3]{b}^2}{x^4})$.

Кроме того, хотя в данном случае автоморфизм $r : (x,y) \mapsto (\zeta_3 x, \zeta_3^2 y)$ не определен над полем $\mathbb{F}_q$, соответствующее фактор-отображение $(x,y) \mapsto (x^3, yx)$, $C \to C/\langle r\rangle = E_1$ определено над полем $\mathbb{F}_q$. Как следствие, имеем разложение якобиана:

$$\mathrm{Jac}_C \sim E_1 \times E_2 \times \widetilde{E}_2,$$

где $\widetilde{E}_2$ — эллиптическая кривая, изоморфная E_2 над квадратичным расширением. Выражения для характеристических многочленов следуют из разложений якобианов. □

В общем случае имеем $\mathrm{Jac}_C \sim E_1 \times A$, где A может быть простым. Так как $A \sim E_2$ над расширением степени 3, то поверхность A не может иметь p-ранг 1, соответственно, она является либо суперсингулярной, либо обычной. Причём определить суперсингулярность/обычность можно по кривой E_2. Для обычных геометрически приводимых абелевых поверхностей в работе [111] есть классификация характеристических многочленов, которая позволяет отсечь лишние варианты. Для суперсингулярных поверхностей полные списки возможных характеристических многочленов представлены в работе [135].

Теорема 3.2.2. *Пусть $C : y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3, определенная над полем $\mathbb{F}_q, q = p^n, p > 3$ и b — кубический невычет. Тогда $p \equiv 1 \pmod 6$ и*

1. *$\chi_{C,q}(T) = (T^2 - t_1 T + q)\chi_A(T)$, где A — некоторая абелева поверхность, а t_1 — след Фробениуса кривой E_1;*
2. *если E_2 — обычная, то $\chi_A(T)$ — один из многочленов:*

- $T^4 - \widetilde{t}_2 T^3 + (\widetilde{t}_2^2 - q)T^2 - \widetilde{t}_2 qT + q^2$, $\sqrt{b} \notin \mathbb{F}_q$;
- $T^4 + \widetilde{t}_2 T^3 + (\widetilde{t}_2^2 - q)T^2 + \widetilde{t}_2 qT + q^2$, $\sqrt{b} \in \mathbb{F}_q$;
- $(T^2 - \widetilde{t}_2 T + q)^2$, $\sqrt{b} \notin \mathbb{F}_q$, $A \sim \widetilde{E}_2^2$;
- $(T^2 + \widetilde{t}_2 T + q)^2$, $\sqrt{b} \in \mathbb{F}_q$, A — *приводима.*

здесь $\widetilde{t}_2$ — *след Фробениуса кривой* $\widetilde{E}_2 : y^2 = x^3 - 3bx + ab$.

3. *если* E_2 — *суперсингулярная, то* $\chi_{A,q}(T)$ — *один из многочленов:*
   - $T^4 - qT^2 + q^2$;
   - $T^4 + 2qT^2 + q^2$;
   - $(T^2 + \sqrt{q}T + q)^2$, n — *чётное,* $p \equiv 2 \pmod 3$, A — *непростое;*
   - $(T^2 + \sqrt{q}T + q)(T^2 - 2\sqrt{q}T + q)$, n – *чётное,* $p \equiv 2 \pmod 3$, A – *непростое;*
   - $(T^2 - \sqrt{q}T + q)^2$, $p \equiv 5 \pmod 6$, n — *чётное,* A — *непростое;*
   - $(T^2 - \sqrt{q}T + q)(T^2 + \sqrt{q}T + q)$, $p \equiv 5 \pmod 6$, n — *чётное,* A — *непростое;*
   - $(T^2 \pm 2\sqrt{q}T + q)^2$, n — *чётное,* A — *непростое;*
   - $(T^2 + \sqrt{q}T + q)^2, p \equiv 1 \pmod 3$, n — *чётное,* A — *простое*
   - $(T^2 - \sqrt{q}T + q)^2, p \equiv 1 \pmod 6$, n — *чётное,* A — *простое*

Доказательство. Из разбиения над $\mathbb{F}_{q^3}$ имеем:

$$L_{C,q^3}(T) = (q^3T^2 - t_{1,3}T + 1)(q^3T - t_{2,3}T + 1)^2.$$

С другой стороны $L_{C,q}(T) = (qT^2 - t_1T + 1)(q^2T^4 + qs_1T^3 + s_2T^2 + s_1T + 1)$.

След Фробениуса эллиптической кривой E над полем $\mathbb{F}_{q^k}$ выражается по известной [48, с. 410] рекуррентной формуле:

$$t_k = tt_{k-1} - qt_{k-2}, t_1 = t, t_2 = t^2 - 2q.$$

Для $k = 3$ и кривой E_2 имеем

$$t_{2,3} = t_2^3 - 3t_2q. \tag{3.2}$$

Соответственно, нам нужно выразить s_1 и s_2 через t_2. Однако, кривая E_2 не определена над базовым полем, и мы не можем посчитать t_2. Поэтому вместо кривой E_2 мы будем использовать её квадратичное кручение.

Известно, что все квадратичные кручения кривой E_2 имеют вид:

$$\widetilde{E}_{2,v} : y^2 = x^3 - 3\sqrt[3]{b}v^2x + av^3,$$

где v — квадратичный невычет в поле $\mathbb{F}_q[\sqrt[3]{b}]$. При этом изоморфизм задаётся отображением $(x,y) \mapsto \left(\frac{x}{v}, \frac{y}{v^{\frac{3}{2}}}\right)$. Для того, чтобы кривая $\widetilde{E}_{2,v}$ была определена над $\mathbb{F}_q$, достаточно взять $v = \sqrt[3]{b}$. Тогда $\widetilde{E}_2 = \widetilde{E}_{2,\sqrt[3]{b}}$ — эллиптическая кривая с уравнением

$$y^2 = x^3 - 3bx + ab.$$

Причём кривые E_2 и $\widetilde{E}_2$ изоморфны тогда и только тогда, когда b является квадратичным вычетом. Соответственно, по b мы можем точно определить знак перед следом Фробениуса $\widetilde{t}_2$.

Найдём теперь выражение s_1, s_2 через t_2, а затем сделаем замену $t_{2,3}, t_2$ на $\widetilde{t}_{2,3}, \widetilde{t}_2$, выбирая знак в зависимости от параметра b.

По формуле $L_{C,q^3}(T^3) = \prod_{\zeta^3=1} L_{C,q}(\zeta T)$ сравнением коэффициентов и взятием редуцированного базиса Грёбнера получаем систему уравнений:

$$\begin{cases} 3s_1^2 s_2 q - 6s_1^2 q^2 - s_2^3 + 3s_2 q^2 + 2q^3 + t_{2,3}^2 = 0, \\ s_1^3 - 3s_1 s_2 + 3s_1 q + 2t_{2,3} = 0. \end{cases} \tag{3.3}$$

В случае $s_1 = 0$ имеем $t_{2,3} = 0$ и $s_2 = -q$ или $s_2 = 2q$. В этом случае A — суперсингулярная абелева поверхность.

Пусть $s_1 \neq 0$. Так как $s_1, s_2 \in \mathbb{Z}$, из теоремы о рациональных корнях и второго уравнения системы следует, что $s_1 \mid 2t_{2,3}$ и $s_1 \equiv t_{2,3} \pmod 3$.

Выражая s_2 во втором уравнении системы и подставляя в первое, получаем:

$$\begin{cases} (t_{2,3} + 3qs_1 - s_1^3)^2 (8t_{2,3} - 12qs_1 + s_1^3) = 0, \\ s_2 = \frac{s_1^2}{3} + q + \frac{2t_{2,3}}{3s_1}, \\ s_1 \neq 0, s_1 \mid 2t_{2,3}, s_1 \equiv t_{2,3} \pmod 3. \end{cases}$$

Таким образом, s_1 — это решение уравнения

$$s_1^3 - 3qs_1 - t_{2,3} = 0 \tag{3.4}$$

или

$$s_1^3 - 12qs_1 + 8t_{2,3} = 0. \tag{3.5}$$

Заметим, что при подстановке $s_1 = t_2$ в (3.4) и $s_1 = -2t_2$ в (3.5) получается формула (3.2). Поэтому $s_1 = t_2$ и $s_1 = -2t_2$ — решения системы уравнений (3.3).

Остальные решения (3.4) и (3.5) следующие:

$$s_1 = \frac{-t_2 \pm \sqrt{d}}{2}$$

и

$$s_1 = t_2 \pm \sqrt{d},$$

где $d = 12q - 3t_2^2$.

В случае, когда E_2 — обычная кривая, то абелева поверхность A будет также обычной, и по результату [111, Prop. 29] возможны только варианты $s_1 = t_2, s_1 = -2t_2$.

Пусть E_2 — суперсинулярная кривая. Тогда A — суперсингулярная. Список суперсингулярных характеристических многочленов для размерности $1-7$ приведён в [135, §12]. Причём для приводимых абелевых поверхностей список получается перебором списка возможных характеристических многочленов эллиптических кривых. Нам осталось только отсеять многочлены, неудовлетворяющие системе уравнений (3.3).

По результатам Дойринга и Ватерхауза [40; 136] для $p > 3$ имеем следующие варианты для $t_{2,3}$:

1. 0, n – нечётное;
2. $-\sqrt{q^3}$, n — чётное, $p \not\equiv 1 \pmod 3$;
3. 0, n — чётное, $p \not\equiv 1 \pmod 4$;
4. $\sqrt{q^3}$, n — чётное, $p \not\equiv 1 \pmod 6$;
5. $\pm 2\sqrt{q^3}$, n — чётное.

В случае $t_{2,3} = 0$ при $p > 3$ возможные варианты для (s_1,s_2) — это $(0, -q)$ и $(0, 2q)$.

При $s_1 \neq 0$ перебором по суперсингулярным эллиптическим следам Фробениуса получаем следующий список возможных вариантов для $\chi_{A,q}(T)$ при $p > 3$:

– $(T^2 + \sqrt{q}T + q)^2$, n – чётное, $p \equiv 2 \pmod 3$, $t_{2,3} = 2q^{3/2}$;
– $(T^2 + \sqrt{q}T + q)(T^2 - 2\sqrt{q}T + q)$, n – чётное, $p \equiv 2 \pmod 3$, $t_{2,3} = 2q^{3/2}$;
– $(T^2 - \sqrt{q}T + q)^2$, n – чётное, $p \equiv 5 \pmod 6$, $t_{2,3} = -2q^{3/2}$;
– $(T^2 - \sqrt{q}T + q)(T^2 + \sqrt{q}T + q)$, n – чётное, $p \equiv 5 \pmod 6$, $t_{2,3} = -2q^{3/2}$;
– $(T^2 - 2\sqrt{q}T + q)^2$, n – чётное, $t_{2,3} = 2q^{3/2}$;
– $(T^2 + 2\sqrt{q}T + q)^2$, n – чётное, $t_{2,3} = -2q^{3/2}$.

В случае, когда A — простое, системе (3.3) удовлетворяют следующие многочлены $\chi_{A,q}(T)$ из списка:

– $(T^2 + \sqrt{q}T + q)^2, p \equiv 1 \pmod 3$, n – чётное
– $(T^2 - \sqrt{q}T + q)^2, p \equiv 1 \pmod 6$, n – чётное
– $(T^2 + q)^2, p \equiv 1 \pmod 4$, n – чётное,
– $T^4 - qT^2 + q^2, p \not\equiv 1 \pmod{12}$, n – чётное.

□

Так как нам теперь известен полный список возможных характеристических многочленов для кривой C, мы можем вычислить $t_1, \widetilde{t_2}$ с помощью алгоритма Схоофа-Элкиса-Аткина, составить список многочленов, и отсечь неверные варианты умножением случайного элемента якобиана на число. Получаем следующее утверждение.

Следствие 3.2.2.1. *Пусть $C : y^2 = x^7+ax^4+bx$ — гиперэллиптическая кривая рода 3 над конечным полем $\mathbb{F}_q$. Тогда задача нахождения характеристического многочлена эндоморфизма Фробениуса и числа точек $\#\operatorname{Jac}_C(\mathbb{F}_q)$ имеет вероятностную сложность $\widetilde{\mathcal{O}}(\log^4 q)$.*

3.3 Алгоритм для рода $g = 4$ на основе разложения якобиана

Пусть C — гиперэллиптическая кривая рода 4 вида

$$y^2 = x^9 + ax^5 + bx,$$

заданная над полем $\mathbb{F}_q$. В данном случае из результатов §2.3.2 имеем

$$\operatorname{Jac}_C(\mathbb{F}_q[\sqrt[8]{b}]) \sim \operatorname{Jac}_{X_1}(\mathbb{F}_q[\sqrt[8]{b}]) \times \operatorname{Jac}_{X_2}(\mathbb{F}_q[\sqrt[8]{b}]),$$

где

$$X_1 : y^2 = (x + 2\sqrt[8]{b})(x^4 - 4\sqrt[4]{b}x^2 + 2\sqrt{b} + a)$$

и

$$X_2 : y^2 = (x - 2\sqrt[8]{b})(x^4 - 4\sqrt[4]{b}x^2 + 2\sqrt{b} + a).$$

Для вычисления порядка якобиана $\#\operatorname{Jac}_C(\mathbb{F}_q)$ мы вычисляем характеристические многочлены кривых рода X_1, X_2 над $\mathbb{F}_q[\sqrt[8]{b}]$ и по ним определяем $\chi_{C,q}(T)$. Так как кривые изоморфны над $\mathbb{F}_q[\sqrt[8]{b}, \sqrt{-1}]$, достаточно вычислить один характеристический многочлен и выбрать знак перед коэффициентами второго многочлена в зависимости от того, является ли -1 квадратом в поле $\mathbb{F}_q$ или нет. Для быстрого вычисления $\chi_{X_1}(T)$ над $\mathbb{F}_q[\sqrt[8]{b}]$ мы используем кручение X_1, определенное над $\mathbb{F}_q[\sqrt{b}]$ уравнением

$$\widetilde{X}_1 : y^2 = (x + 2)(x^4 - 4x^2 + 2 + a/\sqrt{b}).$$

Соответственно, мы вычисляем характеристический многочлен кривой $\widetilde{X}_1$ над $\mathbb{F}_q[\sqrt{b}]$ и определяем характеристический многочлен X_1 над $\mathbb{F}_q[\sqrt[8]{b}]$, используя формулы из [39, с. 5]:

$$a_{1,2} = 2a_2 - a_1^2,$$

$$a_{2,2} = a_2^2 - 4q \cdot a_2 + 2q^2 + 2q \cdot a_{1,2}.$$

После вычисления характеристического многочлена кривой X_1 над $\mathbb{F}_q[\sqrt[8]{b}]$ вычисление многочлена $\chi_{C,q}(T)$ производим, спускаясь раз за разом по квадратичным расширениям. Это можно сделать, решая относительно a_1, a_2, a_3, a_4 следующую систему уравнений, полученную из формулы (2.25):

$$a_{1,2} = -a_1^2 + 2a_2, \tag{3.6}$$

$$a_{2,2} = a_2^2 - 2a_1a_3 + 2a_4, \tag{3.7}$$

$$a_{3,2} = -2q \cdot a_1a_3 + 2q^2a_2 - a_3^2 + 2a_2a_4, \tag{3.8}$$

$$a_{4,2} = 2q^3 \cdot a_{1,2} - 4q \cdot a_3^2 + 4q \cdot a_2a_4 - 4q^2 \cdot a_4 + a_4^2 + 2q^2 \cdot a_{2,2} - 2q \cdot a_{3,2} + 2q^4. \tag{3.9}$$

В случае $a_1 = 0$ имеем:

$$a_2 = a_{1,2}/2,$$

$$a_4 = (a_{2,2} - a_{1,2}^2/4)/2,$$

$$a_3 = \pm\sqrt{2q^2a_2 + 2a_2a_4 - a_{3,2}}.$$

Пусть теперь $a_1 \neq 0$. Из (3.6) и (3.7) получаем

$$a_2 = (a_{1,2} + a_1^2)/2, \tag{3.10}$$

$$a_3 = (a_2^2 + 2a_4 - a_{2,2})/(2a_1). \tag{3.11}$$

Подставляя (3.11) в (3.8) и (3.9), имеем

$$\frac{a_4^2}{a_1^2} + \left(\frac{a_2^2 - a_{2,2}}{a_1^2} - 2a_2 + 2q\right) a_4 - a_{2,2}q + a_2^2q + a_{3,2} + \\ + \frac{a_{2,2}^2 - 2a_2^2a_{2,2} + a_2^4}{4a_1^2} - 2a_2q^2 = 0 \tag{3.12}$$

и

$$\left(1 - \frac{4q}{a_1^2}\right) a_4^2 + 4q\left(\frac{a_{2,2} - a_2^2}{a_1^2} + a_2 - q\right) a_4 + 2q^4 + 2q^3a_{1,2} + \\ + 2q^2a_{2,2} - 2qa_{3,2} - \frac{(a_{2,2}^2 + 2a_2^2a_{2,2} - a_2^4)q}{a_1^2} - a_{4,2} = 0. \tag{3.13}$$

После подстановки (3.10) в уравнения выше, исключения a_4 из системы взятием результанта и деления на a_1^4 получаем следующий многочлен степени 16 от неизвестной a_1

$$a_1^{16} + c_{14}a_1^{14} + c_{12}a_1^{12} + c_{10}a_1^{10} + c_8a_1^8 + c_6a_1^6 + c_4a_1^4 + c_2a_1^2 + c_0 = 0, \qquad (3.14)$$

где коэффициенты c_i приведены в Приложении Г.

Отсюда имеем до 16 возможных значений для a_1. Для их нахождения будем использовать метод из [37, §4]. Разложим данный многочлен на множители над $\mathbb{F}_\ell$ для простого числа $\ell > 16\sqrt{q}$ и исключим решения, которые не удовлетворяют границе $|a_1| \leqslant 8\sqrt{q}$.

Для каждого оставшегося a_1 может быть не более двух возможных наборов (a_2, a_3, a_4) и, таким образом, мы имеем, самое большее, 32 возможных варианта для $\#\operatorname{Jac}_C(\mathbb{F}_q)$. Правильный вариант находим умножением случайных точек якобиана на кандидаты. Описанный метод в строгой форме представляем в виде Алгоритма 4.

Алгоритм 4: Вычисление характеристического многочлена $\chi_{C,q}(T)$ для гиперэллиптической кривой рода 4 вида $C : y^2 = x^9 + ax^5 + bx$.

Input: $a, b \in \mathbb{F}_q$.

Output: (a_1, a_2, a_3, a_4) — коэффициенты $\chi_{C,q}(T)$.

Найти k такое, что $\mathbb{F}_q[\sqrt[8]{b}] \simeq \mathbb{F}_{q^k}$;

Вычислить $\chi_{X_1,q^k}(T) = T^4 + s_{1,k}T^3 + s_{2,k}T^2 + s_{1,k}q^kT + q^{2k}$;

if $\sqrt{-1} \in \mathbb{F}_{q^k}$ **then**

  $a_{1,k} \leftarrow 2s_{1,k}$ и $a_{2,k} \leftarrow 2s_{2,k} + s_{1,k}^2$;

  $a_{3,k} \leftarrow 2s_{1,k}q^k + 2s_{1,k}s_{2,k}$;

  $a_{4,k} \leftarrow 2q^{2k} + 2s_{1,k}^2q^k + s_{2,k}^2$;

else

  $a_{1,k} \leftarrow 0$ и $a_{3,q^k} \leftarrow 0$;

  $a_{2,k} \leftarrow 2s_{2,k} - s_{1,k}^2$;

  $a_{4,k} \leftarrow 2q^{2k} - 2s_{1,k}^2q^k + s_{2,k}^2$;

end

$i \leftarrow k$;

$list \leftarrow \{(a_{1,i}, a_{2,i}, a_{3,i}, a_{4,i})\}$;

while $i \neq 1$ **do**

  $S \leftarrow \{\}$;

  foreach $(a_{1,i}, a_{2,i}, a_{3,i}, a_{4,i}) \in list$ **do**

    Разложить многочлен (3.14) на множители над $\mathbb{F}_\ell$ для простого $\ell > 16\sqrt{q^{i/2}}$ для получения списка возможных $a_{1,i/2}$;

    Создать список S' возможных наборов $(a_{1,i/2}, a_{2,i/2}, a_{3,i/2}, a_{4,i/2})$, удовлетворяющих границе Хассе-Вейля, используя формулы (3.10), (3.11) и (3.12);

    Исключить лишние наборы из списка S' умножением на случайные точки якобиана $\mathrm{Jac}_C(\mathbb{F}_{q^{i/2}})$;

    $S \leftarrow S \cup S'$;

  end

  $list \leftarrow S$;

  $i \leftarrow i/2$;

end

return $list[1]$;

Анализ сложности данного алгоритма ведёт к следующей оценке сложности задачи подсчёта точек.

Теорема 3.3.1. *Пусть* $C : y^2 = x^9 + ax^5 + bx$ — *гиперэллиптическая кривая рода* 4 *над конечным полем* $\mathbb{F}_q$. *Задача нахождения характеристического многочлена эндоморфизма Фробениуса* $\chi_{C,q}$ *и, соответственно, числа элементов в* Jac_C *имеет вероятностную эвристическую сложность* $\widetilde{\mathcal{O}}(\log^8 q)$ *битовых операций.*

Доказательство. Для доказательства выполним анализ сложности Алгоритма 4. Число k на шаге 1 может быть найдено проверкой, является ли b вычетом степени 2^i в $\mathbb{F}_q$ для $i = 1, \ldots, 3$. Каждая проверка занимает время $\widetilde{\mathcal{O}}(\log^2 q)$, так как она эквивалентна возведению в степень. Вычисление характеристического многочлена $\chi_{X_1,q^k}(T)$ для кривой X_1 рода 2 на шаге 2 может быть выполнено за время $\widetilde{\mathcal{O}}(\log^8 q)$ битовых операций с помощью алгоритма Годри-Шоста [75]. Проверка на шаге 3 занимает время $\widetilde{O}(\log^2 q)$ битовых операций. Факторизация многочлена степени 16 на шаге 15 занимает время $\widetilde{\mathcal{O}}(\log^2 \ell) = \widetilde{\mathcal{O}}(\frac{i^2}{4}\log^2 q) = \widetilde{O}(\log^2 q)$ битовых операций (см. таблицу 1). Список S' на шаге 16 содержит до 32 элементов и может быть построен за время $\widetilde{\mathcal{O}}(\log q)$ битовых операций. Исключение наборов из S' на шаге 17 эквивалентно вычислению 4 квадратных корней для генерации случайного элемента из Jac_C и константному количеству скалярных умножений в Jac_C. Скалярное умножение занимает $\mathcal{O}(\log q)$ операций Jac_C, поэтому общая сложность шага равна $\widetilde{\mathcal{O}}(\log^2 q)$ битовых операций. В соответствии с эвристикой 2.1.1 в списке характеристических многочленов в подавляющем большинстве случаев будет только один элемент.

Следовательно, наиболее затратная операция в алгоритме — подсчёт числа точек на кривой рода 2 и общая сложность алгоритма равна $\widetilde{\mathcal{O}}(\log^8 q)$. □

Заметим, что алгоритм менее эффективен, чем алгоритм Схоофа-Элкиса-Аткина со сложностью $\widetilde{\mathcal{O}}(\log^4 p)$, но более эффективен, чем общие алгоритмы для подсчёта точек [5; 30; 137] на кривых рода 4. Наиболее затратной операцией в общих алгоритмах является нахождение элементов из $\mathrm{Jac}_C[\ell]$. При условии, что образующие идеала ℓ-кручения могут быть записаны в виде многочленов степени $\mathcal{O}(\ell^{2g})$, нахождение элементов из $\mathrm{Jac}_C[\ell]$ с помощью методов из [74, §5.2] занимает время, как минимум, $\widetilde{\mathcal{O}}(\ell^{2g}\log^2 q) = \widetilde{\mathcal{O}}(\log^{2g+2} q)$. Для рода 4, соответственно, сложность подсчёта точек будет равна $\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q)$ для некоторого $\varepsilon \geqslant 0$, по сравнению с нашим алгоритмом со сложностью $\widetilde{\mathcal{O}}(\log^8 q)$.

Реализация алгоритма и примеры. Алгоритм был реализован в системе компьютерной алгебры Sage [134]. Исходный код можно найти на личной странице автора[2].

Пример 3.3.1. Возьмем $p = 4398046511233$, $a = 4231746819984$, $b = 141248343157$. Применяя алгоритм, получаем коэффициенты $\chi_C(T)$:

$$a_1 = -2112224,\ a_2 = 2230745113088,\ a_3 = 4306063463022049120,$$

и

$$a_4 = 27453016973128025963440 66.$$

Многочлен $\chi_p(T)$ является $\mathbb{Q}$-неприводимым, поэтому якобиан Jac_C прост. Порядок якобиана

$$\#\,\mathrm{Jac}_C(\mathbb{F}_p) = ffffff7f1c920731feb75b80a59bb590a917dec3284_{16}$$

имеет размер 167 бит. Вычисление заняло 42 мин. 24 сек. на ноутбуке с процессором Core i7-4700HQ CPU, 2.40 GHz.

3.4 Выводы к главе

В данной главе были получены алгоритмы подсчёта точек для кривых рода 3 и 4 вида $y^2 = x^7 + ax^4 + bx$ и $y^2 = x^9 + ax^5 + bx$ со сложностью $\widetilde{\mathcal{O}}(\log^4 q)$ и $\widetilde{\mathcal{O}}(\log^8 q)$ соответственно. Заметим, что мы получили существенное снижение сложности задачи для достаточно больших классов кривых, так как общие алгоритмы имеют сложность $\widetilde{\mathcal{O}}(\log^{14} q)$ и $\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q)$ (см. Таблицу 2) для рода 3 и 4 соответственно.

[2] https://crypto-kantiana.com/semyon.novoselov/src/lp_curves/g4_alg.ipynb

Глава 4. Применение в криптографии и других областях

4.1 Новые сравнения для многочленов Лежандра и метод для их получения

Многочлены Лежандра — классические многочлены, и их свойства над конечными полями исследовались во многих работах [123; 126—128; 138]. Известно, что из факторизации многочленов Лежандра степеней $\frac{p-e}{2}, \frac{p-e}{3}, \frac{p-e}{4}$ над конечным полем $\mathbb{F}_p$ можно получить числа классов мнимых квадратичных числовых полей и j-инварианты суперсингулярных эллиптических кривых (см. [129, Th. 1] и [139; 140]).

Связь кривых $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ и $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ с многочленами Лежандра, исследованная в предыдущих разделах, может быть использована для получения новых свойств многочленов Лежандра над конечным полем. Из §2.3.2 имеем

$$\mathrm{Jac}_{C'}(\mathbb{F}_q) \sim \mathrm{Jac}_{X_1'} \times \mathrm{Jac}_{X_2'}.$$

Соответственно,

$$\chi_{C',q}(T) = \chi_{X_1',q}(T)\chi_{X_2',q}(T).$$

И по формуле Манина (2.28) имеем

$$T^g \chi_{W_p}(T) \equiv \chi_{X_1',q}(T)\chi_{X_2',q}(T) \pmod{p}. \tag{4.1}$$

Так как элементы матрицы W_p представляют собой многочлены Лежандра (по Теореме 2.3.7), мы можем получить новые сравнения (по модулю p) для многочленов Лежандра вида $P_{\frac{ip-j}{g}, \frac{p-1}{2g}}$, сопоставляя коэффициенты многочленов в левой и правой части (4.1). При этом левая часть может быть взята из таблиц в приложениях А и Б.

Якобиан $\mathrm{Jac}_{X_1'}$ является, за исключением небольшого числа частных случаев абсолютно простым [41, Cor. 6]. Кривая X_2' представляет собой либо квадратичное кручение кривой X_1' в случае чётного рода, либо $\mathrm{Jac}_{X_2'} \sim E \times \mathrm{Jac}_{X_1'}$ в случае нечётного рода. Поэтому соотношение (4.1) связывает многочлены Лежандра над конечным полем с характеристическими многочленами

абсолютно простых абелевых многообразий (якобианами гиперэллиптических кривых).

Предыдущие работы [126—129] исследуют связь многочленов Лежандра с эллиптическими кривыми, что позволило получить сравнения по модулю p для многочленов $P_{\frac{p-1}{2}}, P_{\left[\frac{p}{3}\right]}, P_{\left[\frac{p}{4}\right]}$ и $P_{\left[\frac{p}{6}\right]}$ (см. Теорему 2.3.14). Описанный выше метод с использованием гиперэллиптических кривых позволяет получить сравнения для любых многочленов вида $P_{\frac{ip-j}{g}-\frac{p-1}{2g}}$.

Рассмотрим для примера случай $g = 4$. Из разбиения якобиана кривой C', данных из таблицы 8 и формулы (4.1) получаем следующие новые сравнения:

$$P_{\frac{p-1}{8}}\left(-\frac{c}{2}\right) \equiv \frac{-s_1 \pm \sqrt{d}}{2} \pmod p,$$

$$P_{\frac{3p-3}{8}}\left(-\frac{c}{2}\right) \equiv \frac{2s_2}{-s_1 \pm \sqrt{d}} \pmod p,$$

где $c \in \mathbb{F}_p$; s_1, s_2 — коэффициенты характеристического многочлена кривой X_1' : $y^2 = (x+2)(D_g(x)+c)$, т. е. s_1, s_2 такие целые числа, что $\chi_{X_1',p}(T) = T^4 + s_1T^3 + s_2T^2 + s_1pT + p^2$; кроме того, $d = s_1^2 - 4s_2$.

Пример 4.1.1. Достаточно просто найти пример кривой X_1' с абсолютно простым якобианом при небольшой характеристики p. Достаточно взять случайный параметр c и применить результат из работы [111] для проверки абсолютной неприводимости. Возьмём $c = 7$ и $p = 7$, имеем $\chi_{X_1',p}(T) = T^4 - 4T^3 + 16T^2 - 28T + 49$. Данный многочлен является $\mathbb{Q}$-неприводимым, поэтому $\mathrm{Jac}_{X_1'}$ является простым. По результату [111], если простая обычная абелева поверхность является геометрически разложимой (т. е. над замыканием поля), то она раскладывается на эллиптические кривые над расширением степени не больше 6. Таким образом, простой проверкой неприводимости многочленов $\chi_{X_1',p^k}(T)$ для $k \leqslant 6$ можно убедиться, что кривая X_1' имеет абсолютно простой якобиан при $c = 7, p = 7$. Следовательно, мы получили сравнения для многочленов Лежандра $P_{\frac{p-1}{8}}, P_{\frac{3p-3}{8}}$, которые связывают их с кривыми рода 2 с абсолютно простым якобианом. Соответственно, полученные в нашей работе результаты не сводятся к случаю эллиптических кривых, исследованному в предыдущих работах.

4.2 Генерация гиперэллиптических кривых с заданными свойствами

В данном разделе рассмотрим одно из приложений методов подсчёта точек — генерацию кривых. Будем использовать простой «наивный» метод, который состоит из трёх шагов.

1. Выбор случайной кривой X.
2. Вычисление характеристического многочлена $\chi_{C,q}(T)$ эндоморфизма Фробениуса якобиана кривой с помощью одного из алгоритмов подсчёта точек.
3. Проверка требуемого свойства, используя многочлен $\chi_{C,q}(T)$, и переход к шагу 1, если оно не выполняется.

Сложность нахождения кривой зависит при этом от частоты встречаемости кривой с заданным свойством и сложности алгоритма подсчёта точек. Несмотря на простоту, данный метод на практике даёт достаточно хорошие результаты, как мы увидим в дальнейшем.

Рассмотрим теперь проблему нахождения гиперэллиптических кривых X из следующих интересующих нас классов.

1. Кривые с заданным числом точек r в якобиане, т. е. такие, что $\#\operatorname{Jac}_X(\mathbb{F}_q) = r$ для заданного r.
2. Кривые с простым числом точек.
3. Кривые с простым большим делителем порядка якобиана, т. е. $\#\operatorname{Jac}_X(\mathbb{F}_q) = cr$, где c — малое число, а r — большое простое.
4. Кривые с гладким числом точек, т. е. $\#\operatorname{Jac}_X(\mathbb{F}_q) = \ell_1^{e_1} \cdot \ldots \cdot \ell_m^{e_m}$, где $\ell_1, \ldots, \ell_m$ — различные малые простые числа.
5. Кривые с максимальным и минимальным числом точек, т. е. такие, что $\#X(\mathbb{F}_q)$ удовлетворяет левой или правой границе Хассе-Вейля-Серра: $\#X(\mathbb{F}_q) = q + 1 - 2g\lfloor\sqrt{q}\rfloor$ или $\#X(\mathbb{F}_q) = q + 1 + 2g\lfloor\sqrt{q}\rfloor$.
6. Суперсингулярные кривые.

Первые три класса кривых имеют приложения в криптографии на основе задачи вычисления дискретного логарифма, так как кривые, которые не лежат в данных классах, уязвимы к атаке методом Полига-Хеллмана [141]. Также среди классов 1-3 наиболее интересны кривые рода 2 и 3, так как кривые рода $g \geqslant 4$ уязвимы к атакам методом исчисления индексов (см. [142, §7.3, с. 323]). Заме-

тим, что необходимым условием принадлежности заданной кривой к данным трём классам является простота якобиана, так как в случае если якобиан раскладывается в произведение двух или более абелевых многообразий, то число точек на нём будет равно произведению порядков данных абелевых многообразий.

Кривые с гладким порядком из классов 4 и 6, имеют приложения в криптографии на изогениях [1] и в методах факторизации целых чисел на основе гиперэллиптических кривых [143]. Гладкость порядка якобиана означает, что якобиан имеет много подгрупп малого порядка, которые используются при построении изогений малой степени (как ядра изогений) или для поиска малых простых делителей заданного числа в алгоритме факторизации.

Класс 5 кривых имеет приложения в теории кодирования для построения оптимальных кодов.

Для классов 1-4 и 6, как правило, требуются кривые с порядком якобиана размера минимум 256 бит, т. е. $r > 2^{255}$. Это требуемый стандартами ГОСТ 34.10-2018 и NIST размер группы для стойкости подгруппы точек эллиптических кривых к атаке методом Полларда [144]. Так как алгоритм работает в любой абелевой группе порядка r со сложностью $\mathcal{O}(\sqrt{r})$ операций в группе, данное требование распространяется и на размер подгруппы якобиана.

4.2.1 Кривые с заданным числом точек в якобиане

В случае эллиптических кривых «наивный» алгоритм представлен в работе [145, §2.3, с. 18]. Алгоритм 5 представляет собой его обобщение на кривые рода 2 и выше.

Анализ Алгоритма 5. Шаг 1 эквивалентен задаче нахождения простого числа p в интервале от $(\lfloor \sqrt[2g]{N} \rfloor - 1)^2$ до $(\lceil \sqrt[2g]{N} \rceil + 1)^2$. Данную задачу можно решить последовательным перебором чисел от левой границы до правой с применением тестов на простоту. Тесты на простоту имеют полиномиальную сложность (см. обзор в [110]). Однако, в общем случае, существуют интервалы между последовательными простыми числами сколь угодно большой длинны, поэтому простого числа в заданном интервале может не оказаться и в худшем случае алгоритм переберёт все числа в интервале и вернёт FAIL. Соответствен-

Алгоритм 5: Генерация гиперэллиптической кривой с заданным числом точек в якобиане.

Input: целое число $N > 2$.

Output: пара (X, p), где X — гиперэллиптическая кривая, $p > 2$ — простое число и выполняется $\#\operatorname{Jac}_X(\mathbb{F}_p) = N$. Если такой пары не существует, возвращается FAIL.

1 Найти простое число p такое, что $(\sqrt{p}-1)^{2g} \leqslant N \leqslant (\sqrt{p}+1)^{2g}$, если оно существует, иначе вернуть FAIL;

2 Выбрать случайную гиперэллиптическую кривую $X : y^2 = f(x)$;

3 Вычислить число точек $N_0 = \#\operatorname{Jac}_X(\mathbb{F}_p)$;

4 **if** $N \neq N_0$ **then** перейти к Шагу 2;

return (X, p);

но, в худшем случае данный шаг имеет сложность $\widetilde{\mathcal{O}}(\sqrt[2g]{N})$ битовых операций. В среднем и наиболее частом случае время работы полиномиальное — вероятность выбрать случайное простое число в интервале равна $g/\log N$ по теореме о распределении простых чисел, поэтому число попыток до выбора простого числа в среднем будет равно $\log p/g$.

Шаг 2. Здесь выбираются случайные коэффициенты для двух многочленов $h(x)$ (степени не больше $g+1$) и $f(x)$ (степени $2g+1$ или $2g+2$). Так как кривая гиперэллиптическая, то многочлен $f(x)$ должен иметь неравный нулю дискриминант в поле $\mathbb{F}_p$. Вычисление дискриминанта эквивалентно вычислению результанта от многочлена f и его производной f'. Вычисление данного результанта может быть выполнено за время $\widetilde{\mathcal{O}}((2g+1)(2g))$ и $\widetilde{\mathcal{O}}((2g+2)(2g+1))$ битовых операций для многочлена f степени $2g+1$ и $2g+2$, соответственно, с помощью расширенного алгоритма Евклида.

Шаг 3. Подсчёт числа точек на гиперэллиптических кривых может быть выполнен [30] при фиксированном роде g за полиномиальное время в $\mathcal{O}(\log^{cg} p)$, где c — некоторая константа.

Шаг 4. Оценим вероятность успеха на данном шаге в случае $g = 2$. В соответствии с работой [146] всего есть порядка $\mathcal{O}(p^7)$ многочленов f с ненулевым дискриминатом, из них в среднем порядка $\frac{1}{8}p^{11/2}$ (или $\frac{1}{8}p^{9/2}$ если $\deg f = 5$) многочленов f соответствуют кривым с якобианом размера N. Поэтому среднее число попыток до нахождения кривой с порядком якобиана N равно $\mathcal{O}(p^{3/2})$ в

случае, если f — многочлен шестой степени, и $\mathcal{O}(p^{5/2})$, если f — многочлен пятой степени. □

Таким образом, в случае рода 2 алгоритм занимает время в среднем $\widetilde{\mathcal{O}}(p^{3/2})$ или $\widetilde{\mathcal{O}}(p^{5/2})$ битовых операций и, соответственно, имеет экспоненциальную сложность. Поэтому применение данного алгоритма имеет смысл только для небольших размеров характеристики p. Для большой характеристики p лучше подходит более продвинутый метод решения задачи на основе метода комплексного умножения, который представлен в работе [107].

4.2.2 Кривые с (почти) простым числом точек в якобиане

Алгоритм из §4.2.1 имеет экспоненциальную сложность. Однако, если ослабить условия задачи, то можно найти необходимые кривые за полиномиальное время. В данном разделе покажем, что это можно сделать для класса кривых с (почти) простым числом точек, используя для генерации метод из [48, §23.4] с добавлением анализа сложности решения задачи. Вместо того, чтобы фиксировать число точек в якобиане и искать кривую с таким числом точек, мы будем задавать желаемый размер группы якобиана в битах, а затем искать кривую с простым числом точек, либо с простым большим делителем порядка якобиана, т. е. для $\#\operatorname{Jac}(\mathbb{F}_p) = cr$, где r — просто, а $c > 0$ — малое целое число, ограниченное некоторой константой B. Ясно, что в случае $B = 1$ алгоритм будет находить кривые с простым числом точек в якобиане. Соответствующий метод представлен в Алгоритме 6.

Предложение 6. *Пусть $N > 2$, $B \geqslant 1$, $g \geqslant 1$ — целые числа. Тогда нахождение гиперэллиптической кривой X рода g, поля $\mathbb{F}_p$ и простого числа r таких, что $\#\operatorname{Jac}_X(\mathbb{F}_p) = cr$, $c < B$, и $r = 2^{O(N)}$ имеет эвристическую сложность $\widetilde{\mathcal{O}}(g \log^{d+1} p)$ битовых операций в среднем случае при условии, что $g = \mathcal{O}(\log p)$ и сложность подсчёта точек на X равна $\widetilde{\mathcal{O}}(\log^d p)$.*

Доказательство. Для доказательства выполним анализ сложности Алгоритма 6.

Алгоритм 6: Генерация гиперэллиптической кривой с большой подгруппой простого порядка в якобиане.

Input: целое число $N > 2$ — размер якобиана в битах, B — размер сомножителя, g — род кривой.

Output: тройка (X, p, r), где X — гиперэллиптическая кривая, $p > 2$ — простое число и r такое, что $\#\operatorname{Jac}_X(\mathbb{F}_p) = cr = 2^{O(N)}$, $c \leqslant B$. Если такой тройки не существует, возвращается FAIL.

1 Найти простое число $p \in [(2^{\frac{N}{2g}} - 1)^2, (2^{\frac{N}{2g}} + 1)^2]$, если оно существует, иначе вернуть FAIL;

2 Выбрать случайную гиперэллиптическую кривую $X : y^2 = f(x)$ рода g;

3 Вычислить характеристический многочлен $\chi_X(T)$;

4 Если многочлен $\chi_{X,p}(T)$ приводим над $\mathbb{Q}$, то перейти к Шагу 2;

5 Вычислить число точек $n = \#\operatorname{Jac}_X(\mathbb{F}_p) = \chi_{X,p}(1)$;

6 Найти r и c такие, что $n = cr$, где $c < B$ и r — простое. Если таких чисел нет, перейти к Шагу 2;

return (X,p,r);

Шаг 1. В среднем имеет полиномиальное время $\mathcal{O}(\log p/g)$ (см. §4.2.1). В худшем случае, если простого числа на интервале не оказалось, время работы экспоненциальное. Шаг 2. Выбор случайной кривой имеет полиномиальную сложность (см. §4.2.1).

Шаг 3. Характеристический многочлен может быть вычислен за время $\widetilde{\mathcal{O}}(\log^d p)$ по условию предложения 6. В общем случае имеем $d = \mathcal{O}(g)$ [30].

Шаг 4. Проверка приводимости многочлена с рациональными коэффициентами эквивалентна факторизации многочлена, которая может быть выполнена за полилогарифмическое время от степени многочлена: $\widetilde{\mathcal{O}}(\log^{\Delta}(2g))$ битовых операций с помощью LLL-алгоритма [147] ($\Delta = 12$) и его оптимизированных модификаций [148; 149] (в этом случае $\Delta = 6$, см. обзор в [150, с. 396]).

Шаг 5. Вычисление суммы $\chi_{X,p}(1) = 1+a_1+\ldots+a_g+a_{g-1}q+\ldots+a_1q^{g-1}+q^g = 1+q^g+a_1(1+q^{g-1})+\ldots+a_{g-1}(1+q)+a_g$ занимает $2g$ сложений и $2g-2$ умножений в поле, поэтому сложность шага равна $\widetilde{\mathcal{O}}(2g \log p)$ битовых операций.

Шаг 6. Если считать, что B имеет полиномиальный размер $\mathcal{O}(\log^{\Delta} p)$, то на данном шаге для нахождения c можно использовать перебор, либо алгоритм факторизации, допускающий поиск небольших делителей. После нахождения c, используя полиномиальный тест на простоту, можно определить, является ли r

простым. Ясно, что, чем больше c, тем больше вероятность нахождения кривой. Рассмотрим худший случай, когда $B = 1$ и, соответственно, алгоритм возвращает кривые с простым числом точек в якобиане.

Обозначим $P_1(p)$ — вероятность, что целое число в интервале Хассе-Витта $[(\sqrt{p}-1)^{2g}, (\sqrt{p}+1)^{2g}]$ является простым. Пусть также $P_2(p)$ — вероятность, что гиперэллиптическая кривая, задаваемая многочленом f чётной степени, имеет простое число точек в якобиане. Кроме того, пусть $P_3(p)$ — вероятность, что гиперэллиптическая кривая, задаваемая многочленом нечётной степени, имеет простой порядок якобиана. Пусть $\pi(x)$ — функция распределения простых чисел, равная количеству простых чисел, меньше или равных числу x. Тогда

$$P_1(p) = \frac{\pi((\sqrt{p}+1)^{2g}) - \pi((\sqrt{p}-1)^{2g})}{(\sqrt{p}+1)^{2g} - (\sqrt{p}-1)^{2g}}.$$

Применяя теорему о распределении простых чисел ($\pi(x) \sim \frac{x}{\log x}$ при $x \to \infty$), получаем:

$$P_1(p) \sim \frac{1}{g \log p}$$

при $p \to \infty$. В случае рода $g = 2$ известна эвристическая гипотеза [151] для вероятности, что якобиан кривой имеет простое число точек:

$$\lim_{p\to\infty} \left(\frac{P_2(p)}{P_1(p)} - c_p \right) = 0, \tag{4.2}$$

где $c_p \in [0.63987, 0.79890]$ — константа. В случае нечётной степени $f(x)$:

$$\lim_{p\to\infty} \left(\frac{P_3(p)}{P_1(p)} - \frac{9}{19} c_p \right) = 0. \tag{4.3}$$

Аналогичная гипотеза [151, с. 1240, Гипотеза 8] имеет место в случае $g \to \infty$. В этом случае константа $c_p \in [0.63287, 0.79353]$. Таким образом кривая X будет иметь простое число точек в среднем после $\mathcal{O}(g \log p)$ попыток. □

4.3 Генерация кривых рода 3 с большой подгруппой якобиана простого порядка

Для использования в криптографии якобиан кривой должен содержать подгруппу большого простого порядка r размера минимум 256 бит, т. е. $r > 2^{255}$.

Это требуемый стандартами ГОСТ 34.10-2018 и NIST размер группы для стойкости подгруппы точек эллиптических кривых к атаке ρ-методом Полларда [144]. Так как алгоритм работает в любой абелевой группе, данное требование распространяется и на размер подгруппы якобиана.

Покажем на примере, что Алгоритм 3 из §3.1 может быть использован для нахождения кривых с таким свойством. Для кривой $C : y^2 = x^7 + ax^4 + bx$ имеем $\mathrm{Jac_C}(\mathbb{F}_p) \sim E \times A$. Поэтому нам нужно найти кривую C, якобиан которой содержит абелеву поверхность A с числом точек, близким к простому. Возьмем поле $\mathbb{F}_p$ размера 128 бит:

$$p = b8f1c70570a105ab167718f29ac140b5,$$

где простое число p представлено в шестнадцатеричной системе счисления.

Выбирая случайные коэффициенты a, $b \in \mathbb{F}_p$ и применяя к ним Алгоритм 3 после достаточно большого количества итераций, можно найти кривую с простым числом точек $r = \#A(\mathbb{F}_p)$:

$$a = 3a55c031b0e04911dab20f29af712b8e,$$
$$b = 730b82ddda1819bb43014650f43bb5eb$$

и

$$r = 859c727024defc8b8ee1533ed8c992b41e559b27aca96a7485a4914927c0373d.$$

Вычисление заняло 1 ч. 57 мин. на ноутбуке с процессором Core i7-4700HQ, 2.40 GHz. Число r имеет размер в 256 бит, соответственно, абелева поверхность A подходит для криптографии на основе задачи вычисления дискретного логарифма. Характеристический многочлен A имеет вид

$$\chi_{A,p}(T) = T^4 + s_1T^3 + s_2T^2 + s_1pT + p^2,$$

где

$$s_1 = 1679f8e9dad36939c,$$
$$s_2 = 1403f1e6b427e83664335d388d82b465b.$$

Применяя рекуррентные формулы из Приложения B, можно также найти и $\chi_{A,p^2}(T)$. Оба многочлена $\chi_{A,p}(T), \chi_{A,p^2}(T)$ неприводимы над $\mathbb{Q}$ и поэтому абелева поверхность A проста над полями $\mathbb{F}_p$ и $\mathbb{F}_{p^2}$.

4.4 Анализ криптосистем на группах с неизвестным порядком

Для построения криптосистем на группах с неизвестным порядком требуются кривые, на которых трудно вычислить число точек. Для «параноидального» уровня безопасности в 128 бит требуются кривые рода 3 над конечным полем размера 1131 бит [3, Таблица 2], что соответствует якобиану размера 3392 бит. В наших экспериментах (Таблица 7) мы смогли посчитать число элементов в якобиане кривой рода 3 такого размера за сравнительно малое время, которое существенно меньше, чем вычисления даже для рода 2, где известный рекорд подсчёта точек для случайной кривой [75] равен 256 бит в якобиане. Сложность подсчёта точек на кривых рода 3 при этом намного больше — она равна $\widetilde{\mathcal{O}}(\log^{14} q)$ против $\widetilde{\mathcal{O}}(\log^{8} q)$ у кривых рода 2. Поэтому можно заключить, что кривых вида $y^2 = x^7 + ax^4 + bx$ следует избегать при построении криптосистем на группах с неизвестным порядком.

Для кривых рода 4 общего вида задача имеет сложность $\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q)$, поэтому на практике для подсчёта точек используются в основном экспоненциальные от $\log q$ алгоритмы со сложностью $\mathcal{O}(q^2/\sqrt{\log\log q})$ [101]. Для кривых рода 4 вида $y^2 = x^7 + ax^4 + bx$ по Теореме 3.3.1 имеем сложность подсчёта точек $\widetilde{\mathcal{O}}(\log^{8} q)$, так как задача сводится к подсчёту точек на кривых рода 2. Поэтому в теории можно рассчитывать на подсчёт точек на кривых над полем размера 128 бит, что соответствует 512-битному размеру якобиана. В наших вычислениях (Таблица 7) был достигнут размер якобиана 163 бит. Также, как и в случае кривых рода 3, имеем более эффективное вычисление числа точек на кривой по сравнению с общим случаем, поэтому таких кривых также следует избегать при построении криптосистем на группах с неизвестным порядком.

Таблица 7 — Вычисление числа точек кривых рода 3 и 4 над большим полем.

Род	Кривая	Размер якобиана	Метод	Время
3	$y^2 = x^7 + ax^4 + bx$	129 бит	hypellfrob	31 мин.
3	$y^2 = x^7 + ax^4 + bx$	958 бит	Алг. 3	39 мин.
3	$y^2 = x^7 + ax^4 + bx$	2716 бит	явные формулы, §3.2	23 мин.
3	$y^2 = x^7 + ax^4 + bx$	3392 бит	явные формулы, §3.2	3 ч. 10 мин.
4	$y^2 = x^9 + ax^5 + bx$	163 бит	Алг. 4 + hypellfrob	18 мин.

Результаты вычислений, представленные в Таблице 7, были получены на компьютере с процессором Xeon E2146G, 3.50GHz. В качестве кривых выбирались случайные кривые. При этом в случае рода 4 для подсчёта точек на кривых рода 2 использовался экспоненциальный алгоритм (пакет hypellfrob) из-за наличия ошибок в доступной реализации алгоритма Годри-Шоста [75].

4.5 Выводы к главе

В главе представлены приложения полученных алгоритмов и формул для генерации кривых и анализа криптосистем на группах с неизвестным порядком. Получены примеры кривых рода 3, содержащих большую подгруппу простого порядка. Выполнены вычисления для кривых C рода 3 и 4 над большим простым полем — установлено, что такие кривые не рекомендуется использовать в криптосистемах на группах с неизвестным порядком в виду большой эффективности вычислений.

Заключение

Основные результаты работы заключаются в следующем.

1. Предложен общий алгоритм для подсчёта точек на кривой C на основе разложения якобиана над расширением поля.
2. Получен полный список возможных характеристических многочленов (редуцированных по модулю характеристики p) кривой $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ для родов $1 - 7$ и аналогичные списки для кривых $y^2 = (x \pm 2)(D_g(x) + a)$ и $y^2 = D_g(x) + a$.
3. Получено соотношение между многочленами Лежандра и коэффициентами характеристического многочлена $\chi_{C,q}$, расширяющее известное соотношение для эллиптических кривых (через инварианты Хассе-Витта).
4. Для кривых рода $3, 4$ вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ получена эвристическая вероятностная оценка сложности подсчёта точек, равная $\widetilde{\mathcal{O}}(\log^4 q)$ и $\widetilde{\mathcal{O}}(\log^8 q)$ соответственно. Для сравнения — общие алгоритмы имеют сложность $\widetilde{\mathcal{O}}(\log^{14} q)$ для рода 3 и $\widetilde{\mathcal{O}}(\log^{18+\varepsilon} q)$ для рода 4.

Перспективными для дальнейших исследований по теме диссертации выглядят следующие вопросы:

1. Нахождение явных формул для кривых рода 4 и выше.
2. Применение общих алгоритмов из главы 2 к другим классам кривых с геометрически приводимым якобианом.
3. Исследование p-ранга кривой C, который равен рангу матрицы W_p.
4. Обобщение работ Брилхарта и Мортона [129; 139] для эллиптических кривых на кривые больших родов. Использование полученных результатов по связи многочленов Лежандра с кривыми $y^2 = x^{2g+1} + ax^{g+1} + bx$ для нахождения соответствия между числом классов идеалов поля $\mathbb{Q}(\zeta_{2g})$ и количеством множителей в факторизации многочлена Лежандра.

Благодарности. В заключение автор благодарит Киршанову Е. А. за вычитку работы и полезные комментарии к ней, Малыгину Е. С. за поддержку, вычитку работы и обсуждение результатов, Алешникова С. И. за обсуждение результатов, помощь и организацию семинаров по алгебраической

геометрии, которые заложили теоретическую базу для выполнения работы; Болтнева Ю. Ф. за выполнение вычислительных экспериментов для кривых рода 3. Также автор выражает благодарность фонду РФФИ за финансовую поддержку проведённых исследований.

Список сокращений и условных обозначений

$\mathbb{F}_q$	конечное поле размера $q = p^n$, где p — простое число.
$\#C(\mathbb{F}_q)$	число точек на кривой C над конечным полем $\mathbb{F}_q$.
$\mathrm{Jac}_C(k)$	якобиан кривой C над полем k.
$\chi_{C,q}(T)$	характеристический многочлен эндоморфизма Фробениуса якобиана кривой C над конечным полем $\mathbb{F}_q$.
$\chi_{A,q}(T)$	характеристический многочлен эндоморфизма Фробениуса абелева многообразия A над конечным полем $\mathbb{F}_q$.
ι	гиперэллиптическая инволюция.
$\overline{k}$	алгебраическое замыкание поля k.
$\mathcal{C}_m$	циклическая группа порядка m.
$\mathcal{D}_m$	диэдральная группа порядка m.
$D_m(x,a)$	многочлен Диксона степени m.
$D_m(x)$	многочлен Диксона $D_m(x,1)$.
$\dim(A)$	размерность многообразия A.
$P_m(x)$	многочлен Лежандра степени m.
ζ_m	примитивный корень степени m из единицы.
ГЭК	гиперэллиптическая кривая.
ЭК	эллиптическая кривая.

Список литературы

1. *Flynn E.*, *Ti Y.* Genus two isogeny cryptography //. Vol. 11505. — Springer, Cham, 2019. — P. 286—306. — (Lecture Notes in Computer Science).
2. *Costello C.*, *Smith B.* The supersingular isogeny problem in genus 2 and beyond // International Conference on Post-Quantum Cryptography. — Springer. 2020. — 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 // Mathematics of Computation. — 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 // International Algorithmic Number Theory Symposium. — Springer. 2002. — P. 461—474.
7. *Gaudry P.*, *Schost É.* A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm // International Algorithmic Number Theory Symposium. — Springer. 2004. — P. 208—222.
8. *Cheon J. H.*, *Chee S.*, *Park C.* S-boxes with controllable nonlinearity // International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 1999. — P. 286—294.
9. *Cheon J. H.*, *Chee S.* Nonlinearity of Boolean functions and hyperelliptic curves // SIAM Journal on Discrete Mathematics. — 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 // American Journal of Mathematics. — 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. für die reine und angewandte Mathematik. — 1936. — Vol. 175. — P. 55—62.

14. *Hasse H.* Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem. // J. für die reine und angewandte Mathematik. — 1936. — Vol. 175. — P. 69—88.

15. *Hasse H.* Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. // J. für die reine und angewandte Mathematik. — 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 // Publications Mathématiques de l'Institut des Hautes Études Scientifiques. — 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 // Séminaire Bourbaki vol. 1972/73 Exposés 418–435. — Springer, 1974. — 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. of the Mathematical Society of 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 Journal of Computation and Mathematics. — 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 // Mathematics of computation. — 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 // Mathematics of computation. — 1987. — Vol. 48, no. 177. — P. 95—101.

32. *Ekedahl T.*, *Serre J.-P.* Exemples de courbes algébriques à jacobienne complètement décomposable // Comptes rendus de l'Académie des sciences. 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 // Experimental Mathematics. — 2017. — Vol. 26, no. 4. — P. 430—445.

37. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields // Lecture Notes in Computer Science. Vol. 5479. — Springer. 2009. — P. 536—553.

38. *Freeman D. M.*, *Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction // Journal of 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 // Lecture Notes in Computer Science. Vol. 7708. — Springer. 2012. — P. 234—253.

40. *Deuring M.* Die typen der multiplikatorenringe elliptischer funktionenkörper // Abhandlungen aus dem mathematischen Seminar der Universität Hamburg. Vol. 14. — Springer. 1941. — 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 // International Algorithmic Number Theory Symposium. — Springer. 2006. — 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. *Lang S.* Abelian varieties. — Springer Science & Business Media, 1983.

48. Handbook of Elliptic and Hyperelliptic Curve Cryptography / ed. by H. Cohen [et al.]. — Chapman, Hall/CRC, 2005.

49. *Jacobson M. J.*, *Scheidler R.*, *Stein A.* Cryptographic aspects of real hyperelliptic curves // Tatra Mountains Mathematical Publications. — 2010. — Vol. 47, no. 1. — P. 31—65.

50. *Grant D.* Formal groups in genus two // J. reine angew. Math. — 1990. — Vol. 411, no. 96. — P. 121.

51. *Flynn E. V.* The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field // Mathematical Proceedings of the Cambridge Philosophical Society. Vol. 107. — Cambridge University Press. 1990. — P. 425—441.

52. *Flynn E. V.* The group law on the Jacobian of a curve of genus 2 // J. reine angew. Math. — 1993. — Vol. 439. — P. 45—69.

53. *Мамфорд Д.* Лекции о тэта-функциях. — Мир, 1988.

54. *Milio E.* Computing isogenies between Jacobian of curves of genus 2 and 3 // arXiv preprint arXiv:1709.06063. — 2017.

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

56. *Achter J. D.*, *Howe E. W.* Hasse–Witt and Cartier–Manin matrices: A warning and a request // Arithmetic Geometry: Computation and Applications. — 2019. — Vol. 722. — P. 1.

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

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

59. *Bostan A.*, *Gaudry P.*, *Schost É.* Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator // SIAM Journal on Computing. — 2007. — Vol. 36, no. 6. — P. 1777—1806.

60. *Howe E. W.*, *Nart E.*, *Ritzenthaler C.* Jacobians in isogeny classes of abelian surfaces over finite fields // Annales de l'institut Fourier. Vol. 59. — Association des Annales de l'institut Fourier. 2009. — P. 239—289.

61. *Ahmadi O.*, *McGuire G.*, *Rojas-Leon A.* Decomposing Jacobians of curves over finite fields in the absence of algebraic structure // Journal of Number Theory. — 2015. — Vol. 156. — P. 414—431.

62. *Hartshorne R.* Algebraic geometry. — Springer, 1997.

63. *Blankertz R.* A polynomial time algorithm for computing all minimal decompositions of a polynomial // ACM Comm. Computer Algebra. — 2014. — Vol. 48. — P. 13—23.

64. *Abelard S.*, *Gaudry P.*, *Spaenlehauer P.-J.* Counting points on genus-3 hyperelliptic curves with explicit real multiplication // The Open Book Series. — 2019. — Vol. 2, no. 1. — P. 1—19.

65. *Abelard S.* Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus // arXiv preprint arXiv:1810.11068. — 2018.

66. *Brandt R.*, *Stichtenoth H.* Die automorphismengruppen hyperelliptischer Kurven // Manuscripta mathematica. — 1986. — Vol. 55, no. 1. — P. 83—92.

67. *Harvey D.*, *Van Der Hoeven J.* Polynomial multiplication over finite fields in time $O(n \log n)$. — 2019. — URL: https://hal.archives-ouvertes.fr/hal-02070816 ; preprint.

68. *Bernstein D. J.*, *Yang B.-Y.* Fast constant-time gcd computation and modular inversion // IACR Transactions on Cryptographic Hardware and Embedded Systems. — 2019. — P. 340—398.

69. *Müller S.* On the computation of square roots in finite fields // Designs, Codes and Cryptography. — 2004. — Vol. 31, no. 3. — P. 301—312.

70. *Von Zur Gathen J.*, *Gerhard J.* Modern computer algebra. — Cambridge university press, 2013.

71. *Lange H.*, *Ruppert W.* Complete systems of addition laws on abelian varieties // Inventiones mathematicae. — 1985. — Vol. 79, no. 3. — P. 603—610.

72. *Arene C.*, *Kohel D.*, *Ritzenthaler C.* Complete addition laws on abelian varieties // LMS J. Comput. Math. — 2012. — Vol. 15. — P. 308—316.

73. *Van Wamelen P.* Equations for the Jacobian of a hyperelliptic curve // Transactions of the American Mathematical Society. — 1998. — Vol. 350, no. 8. — P. 3083—3106.

74. *Abelard S.* Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus // Journal of Complexity. — 2020. — Vol. 57. — P. 101440.

75. *Gaudry P.*, *Schost É.* Genus 2 point counting over prime fields // Journal of Symbolic Computation. — 2012. — Vol. 47, no. 4. — P. 368—400.

76. *Gaudry P.*, *Kohel D.*, *Smith B.* Counting Points on Genus 2 Curves with Real Multiplication // Advances in Cryptology – ASIACRYPT 2011 / ed. by D. H. Lee, X. Wang. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. — P. 504—519.

77. *Cox D. A.* Galois theory. Vol. 61. — 2nd ed. — John Wiley & Sons, 2012.

78. *Canny J. F.*, *Kaltofen E.*, *Yagati L.* Solving systems of nonlinear polynomial equations faster // Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation. — ACM. 1989. — P. 121—128.

79. *Cantor D. G.*, *Kaltofen E.* On fast multiplication of polynomials over arbitrary algebras // Acta Informatica. — 1991. — Vol. 28, no. 7. — P. 693—701.

80. *Stichtenoth H.* Algebraic function fields and codes. Vol. 254. — Springer, 2009.

81. *Cox D. A.*, *Little J.*, *O'shea D.* Using algebraic geometry. Vol. 185. — Springer Science & Business Media, 2006.

82. *Faugere J.-C.* A new efficient algorithm for computing Gröbner bases (F4) // Journal of pure and applied algebra. — 1999. — Vol. 139, no. 1—3. — P. 61—88.

83. *Faugère J. C.* A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. — 2002. — P. 75—83.

84. *Cox D. A.*, *Little J.*, *O'Shea D.* Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. — 4th. — Springer Publishing Company, Incorporated, 2015.

85. *Makarim R. H.*, *Stevens M.* M4GB: an efficient Gröbner-basis algorithm // Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation. — 2017. — P. 293—300.

86. *Cohen H.* A course in computational algebraic number theory // Graduate texts in Math. — 1993. — Vol. 138. — P. 88.

87. *Lazard D.* Solving zero-dimensional algebraic systems // Journal of symbolic computation. — 1992. — Vol. 13, no. 2. — P. 117—131.

88. *Schost É.* Complexity results for triangular sets // Journal of Symbolic Computation. — 2003. — Vol. 36, no. 3/4. — P. 555—594.

89. *Lazard D.* A new method for solving algebraic systems of positive dimension // Discrete Applied Mathematics. — 1991. — Vol. 33, no. 1—3. — P. 147—160.

90. *Van Der Hoeven J.*, *Lecerf G.* Fast multivariate multi-point evaluation revisited // Journal of Complexity. — 2020. — Vol. 56. — P. 101405.

91. *Kedlaya K. S.*, *Umans C.* Fast modular composition in any characteristic // 2008 49th Annual IEEE Symposium on Foundations of Computer Science. — IEEE. 2008. — P. 146—155.

92. *Kemper G.* A Course in Commutative Algebra. — Springer, Berlin, Heidelberg, 2011.

93. *Bosma W.*, *Cannon J.*, *Playoust C.* The Magma algebra system I: The user language // Journal of Symbolic Computation. — 1997. — Vol. 24, no. 3/4. — P. 235—265.

94. Efficient computation of zero-dimensional Gröbner bases by change of ordering / J.-C. Faugere [et al.] // Journal of Symbolic Computation. — 1993. — Vol. 16, no. 4. — P. 329—344.

95. *Collart S.*, *Kalkbrener M.*, *Mall D.* Converting bases with the Gröbner walk // Journal of Symbolic Computation. — 1997. — Vol. 24, no. 3/4. — P. 465—469.

96. *Tran Q.-N.* A fast algorithm for Gröbner basis conversion and its applications // Journal of Symbolic Computation. — 2000. — Т. 30, № 4. — С. 451—467.

97. *Bardet M.*, *Faugère J.-C.*, *Salvy B.* On the complexity of the F5 Gröbner basis algorithm // Journal of Symbolic Computation. — 2015. — Vol. 70. — P. 49—70.

98. *Alman J.*, *Williams V. V.* A refined laser method and faster matrix multiplication // Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA). — SIAM. 2021. — P. 522—539.

99. *Kalkbrener M.* On the complexity of Gröbner bases conversion // Journal of Symbolic Computation. — 1999. — Vol. 28, no. 1/2. — P. 265—273.

100. *Mayr E. W.*, *Ritscher S.* Dimension-dependent bounds for Gröbner bases of polynomial ideals // Journal of Symbolic Computation. — 2013. — Vol. 49. — P. 78—94. — The International Symposium on Symbolic and Algebraic Computation.

101. *Sutherland A. V.* Order computations in generic groups. — Massachusetts Institute of Technology, 2007.

102. *Nymann J.* On the probability that k positive integers are relatively prime // Journal of number theory. — 1972. — Vol. 4, no. 5. — P. 469—473.

103. *Chidambaraswamy J.*, *Sitaramachandrarao R.* On the probability that the values of m polynomials have a given gcd // Journal of Number Theory. — 1987. — Vol. 26, no. 3. — P. 237—245.

104. *Nemes G.* Error bounds for the asymptotic expansion of the Hurwitz zeta function // Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences. — 2017. — Vol. 473, no. 2203. — P. 20170363.

105. Sato–Tate distributions and Galois endomorphism modules in genus 2 / F. Fité [et al.] // Compositio Mathematica. — 2012. — Vol. 148, no. 5. — P. 1390—1442.

106. *Sutherland A.* Sato-Tate distributions // Contemporary Mathematics. — 2019. — P. 197—248.

107. Genus-2 curves and Jacobians with a given number of points / R. Bröker [et al.] // LMS Journal of Computation and Mathematics. — 2015. — Vol. 18, no. 1. — P. 170—197.

108. *Sutherland A.* A generic approach to searching for Jacobians // Mathematics of Computation. — 2009. — Vol. 78, no. 265. — P. 485—507.

109. Beating Brute Force for Systems of Polynomial Equations over Finite Fields / D. Lokshtanov [et al.] // Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms. — Barcelona, Spain : Society for Industrial, Applied Mathematics, 2017. — P. 2190—2202. — (SODA '17).

110. *Schoof R.* Four primality testing algorithms // Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography. — Cambridge University Press. 2008. — P. 101—126.

111. *Chou K.-M. J.*, *Kani E.* Simple geometrically split abelian surfaces over finite fields // J. Ramanujan Math. Soc. — 2014. — Vol. 29, no. 1. — P. 31—62.

112. *Furukawa E.*, *Kawazoe M.*, *Takahashi T.* Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields // International Workshop on Selected Areas in Cryptography. — Springer. 2003. — P. 26—41.

113. *Haneda M.*, *Kawazoe M.*, *Takahashi T.* Suitable Curves for Genus-4 HCC over Prime Fields: Point Counting Formulae for Hyperelliptic Curves of Type $y^2 = x^{2k+1} + ax$ // International Colloquium on Automata, Languages, and Programming. — Springer. 2005. — P. 539—550.

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

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

116. *Leprévost F.*, *Morain F.* Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères // Journal of Number Theory. — 1997. — Vol. 64, no. 2. — P. 165—182.

117. *Berndt B. C.*, *Williams K. S.*, *Evans R. J.* Gauss and Jacobi sums. — Wiley, 1998.

118. *Bujalance E.*, *Gamboa J.*, *Gromadzki G.* The full automorphism groups of hyperelliptic Riemann surfaces // manuscripta mathematica. — 1993. — Vol. 79, no. 1. — P. 267—282.

119. *Cardona G.* On the number of curves of genus 2 over a finite field // Finite Fields and Their Applications. — 2003. — Vol. 9, no. 4. — P. 505—526.

120. *Lercier R.*, *Ritzenthaler C.* Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects // Journal of Algebra. — 2012. — Vol. 372. — P. 595—636.

121. *Bhargava M.*, *Zieve M. E.* Factoring Dickson polynomials over finite fields // Finite Fields and Their Applications. — 1999. — Vol. 5, no. 2. — P. 103—111.

122. *Lidl R.*, *Mullen G. L.*, *Turnwald G.* Dickson polynomials. Vol. 65. — Chapman & Hall/CRC, 1993.

123. *Carlitz L.* Congruence properties of the polynomials of Hermite, Laguerre and Legendre // Mathematische Zeitschrift. — 1953. — Vol. 59, no. 1. — P. 474—483.

124. *Weaver J. R.* Centrosymmetric (cross-symmetric) matrices, their basic properties, eigenvalues, and eigenvectors // The American Mathematical Monthly. — 1985. — Vol. 92, no. 10. — P. 711—717.

125. *Rück H.-G.* Abelian surfaces and Jacobian varieties over finite fields // Compositio Math. — 1990. — No. 76. — P. 351—366.

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

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

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

129. *Brillhart J.*, *Morton P.* Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial // Journal of Number Theory. — 2004. — Vol. 106, no. 1. — P. 79—111.

130. *Hasse H.*, *Witt E.* Zyklische unverzweigte Erweiterungskörper vom Primzahlgradep über einem algebraischen Funktionenkörper der Charakteristikp // Monatshefte für Mathematik und Physik. — 1936. — Vol. 43, no. 1. — P. 477—492.

131. *Kazemifard A.*, *Tafazolian S.*, *Torres F.* On maximal curves related to Chebyshev polynomials // Finite Fields and Their Applications. — 2018. — Vol. 52. — P. 200—213.

132. *Tafazolian S.*, *Top J.* On certain maximal hyperelliptic curves related to Chebyshev polynomials // Journal of Number Theory. — 2019. — Vol. 203. — P. 276—293.

133. *Lindhurst S.* An analysis of Shanks's algorithm for computing square roots in finite fields // Number theory (Ottawa, 1996), CRM Proc. Lecture Notes. Vol. 19. — 1999. — P. 231—242.

134. *Developers T. S.* SageMath, the Sage Mathematics Software System (Version 8.6). — 2019. — https://www.sagemath.org.

135. *Singh V.*, *Zatysev A.*, *McGuire G.* On the characteristic polynomial of frobenius of supersingular abelian varieties of dimension up to 7 over finite fields // arXiv preprint arXiv:1011.2257. — 2010.

136. *Waterhouse W. C.* Abelian varieties over finite fields // Annales scientifiques de l'École Normale Supérieure. Vol. 2. — 1969. — P. 521—560.

137. *Huang M.-D.*, *Ierardi D.* Counting points on curves over finite fields // Journal of Symbolic Computation. — 1998. — Vol. 25, no. 1. — P. 1—21.

138. *Honda T.* Two congruence properties of Legendre polynomials // Osaka Journal of Mathematics. — 1976. — Vol. 13, no. 1. — P. 131—133.

139. *Morton P.* Legendre polynomials and complex multiplication, I // Journal of Number Theory. — 2010. — Vol. 130, no. 8. — P. 1718—1731.

140. Explicit congruences for class equations / P. Morton [et al.] // Functiones et Approximatio Commentarii Mathematici. — 2014. — Vol. 51, no. 1. — P. 77—110.

141. *Pohlig S.*, *Hellman M.* An improved algorithm for computing logarithms over GF(p) and its cryptographic significance // IEEE Transactions on information Theory. — 1978. — Vol. 24, no. 1. — P. 106—110.

142. *Frey G.*, *Shaska T.* Curves, Jacobians, and cryptography // Contemporary Mathematics. — 2019. — Vol. 724. — P. 279—345.

143. *Cosset R.* Factorization with genus 2 curves // Mathematics of Computation. — 2010. — Vol. 79, no. 270. — P. 1191—1208.

144. *Pollard J. M.* Monte Carlo methods for index computation (mod p) // Mathematics of computation. — 1978. — Vol. 32, no. 143. — P. 918—924.

145. *Bröker R.* Constructing elliptic curves of prescribed order. — Leiden University, 2006.

146. *Lenstra H.*, *Pila J.*, *Pomerance C.* A hyperelliptic smoothness test, II // Proceedings of the London Mathematical Society. — 2002. — Vol. 84, no. 1. — P. 105—146.

147. *Lenstra A. K.*, *Lenstra H. W.*, *Lovász L.* Factoring polynomials with rational coefficients // Mathematische Annalen. — 1982. — Vol. 261, no. 4. — P. 515—534.

148. *Van Hoeij M.* Factoring polynomials and the knapsack problem // Journal of Number theory. — 2002. — Vol. 95, no. 2. — P. 167—189.

149. *Novocin A.*, *Stehlé D.*, *Villard G.* An LLL-reduction algorithm with quasi-linear time complexity // Proceedings of the forty-third annual ACM symposium on Theory of computing. — ACM. 2011. — P. 403—412.

150. Algorithmes Efficaces en Calcul Formel / A. Bostan [et al.]. — Palaiseau : Frédéric Chyzak (auto-édit.), 09/2018. — URL: https://hal.archives-ouvertes.fr/AECF/ ; 686 pages. Imprimé par CreateSpace. Aussi disponible en version électronique.

151. The probability that the number of points on the Jacobian of a genus 2 curve is prime / W. Castryck [et al.] // Proceedings of the London Mathematical Society. — 2012. — Vol. 104, no. 6. — P. 1235—1270.

Публикации автора по теме диссертации

152. *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.

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

154. *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.

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

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

157. *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.

158. *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 рисунков

Список таблиц

Приложение А

Список характеристических многочленов для кривых $C' : y^2 = x^{2g+1} + cx^{g+1} + x$

В Таблицах 8 и 9 представлены характеристические многочлены $\pmod p$ для гиперэллиптической кривой $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ над полем $\mathbb{F}_p$ и $\mathbb{F}_{p^2}$ соответственно. Здесь $p > 2$, $\gcd(p,g) = 1$ и $P_m := P_m(-c/2)$. Многочлены получены по методу из §2.3.4.

Таблица 8 — Характеристические многочлены для кривых $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ над $\mathbb{F}_p$.

g	Условия	$\chi_{C',p}(T) \pmod p$
2	$p \equiv 1 \pmod 4$	$T^2(T - P_{\frac{p-1}{4}})^2$
2	$p \equiv 3 \pmod 4$	$T^2(T^2 - P^2_{\frac{p-3}{4}})$
3	$p \equiv 1 \pmod 3$	$T^3(T - P_{\frac{p-1}{2}})(T - P_{\frac{p-1}{6}})^2$
3	$p \equiv 2 \pmod 3$	$T^3(T - P_{\frac{p-1}{2}})(T^2 - P^2_{\frac{p-5}{6}})$
4	$p \equiv 1 \pmod 8$	$T^4(T - P_{\frac{p-1}{8}})^2(T - P_{\frac{3p-3}{8}})^2$
4	$p \equiv 3 \pmod 8$	$T^4(T^2 - P_{\frac{p-3}{8}} P_{\frac{3p-1}{8}})^2$
4	$p \equiv 5 \pmod 8$	$T^4(T^2 - P_{\frac{p-5}{8}} P_{\frac{3p-7}{8}})^2$
4	$p \equiv 7 \pmod 8$	$T^4(T^2 - P^2_{\frac{p-7}{8}})(T^2 - P^2_{\frac{3p-5}{8}})$
5	$p \equiv 1 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}})(T - P_{\frac{p-1}{10}})^2(T - P_{\frac{3p-3}{10}})^2$
5	$p \equiv 2 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}})(T^4 - P^2_{\frac{p-7}{10}} P^2_{\frac{3p-1}{10}})$
5	$p \equiv 3 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}})(T^4 - P^2_{\frac{p-3}{10}} P^2_{\frac{3p-9}{10}})$
5	$p \equiv 4 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}})(T^2 - P^2_{\frac{p-9}{10}})(T^2 - P^2_{\frac{3p-7}{10}})$
6	$p \equiv 1 \pmod{12}$	$T^6(T - P_{\frac{p-1}{4}})^2(T - P_{\frac{p-1}{12}})^2(T - P_{\frac{5p-5}{12}})^2$
6	$p \equiv 5 \pmod{12}$	$T^6(T - P_{\frac{p-1}{4}})^2(T^2 - P_{\frac{p-5}{12}} P_{\frac{5p-1}{12}})^2$
6	$p \equiv 7 \pmod{12}$	$T^6(T^2 - P^2_{\frac{p-3}{4}})(T^2 - P_{\frac{p-7}{12}} P_{\frac{5p-11}{12}})^2$
6	$p \equiv 11 \pmod{12}$	$T^6(T^2 - P^2_{\frac{p-3}{4}})(T^2 - P^2_{\frac{p-11}{12}})(T^2 - P^2_{\frac{5p-7}{12}})$
7	$p \equiv 1 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T - P_{\frac{p-1}{14}})^2(T - P_{\frac{3p-3}{14}})^2(T - P_{\frac{5p-5}{14}})^2$
7	$p \equiv 2 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T^3 - P_{\frac{p-9}{14}} P_{\frac{3p-13}{14}} P_{\frac{5p-3}{14}})^2$
7	$p \equiv 3 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T^6 - P^2_{\frac{p-3}{14}} P^2_{\frac{3p-9}{14}} P^2_{\frac{5p-1}{14}})$
7	$p \equiv 4 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T^3 - P_{\frac{p-11}{14}} P_{\frac{3p-5}{14}} P_{\frac{5p-13}{14}})^2$
7	$p \equiv 5 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T^6 - P^2_{\frac{5p-11}{14}} P^2_{\frac{3p-1}{14}} P^2_{\frac{p-5}{14}})$
7	$p \equiv 6 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}})(T^2 - P^2_{\frac{p-13}{14}})(T^2 - P^2_{\frac{3p-11}{14}})(T^2 - P^2_{\frac{5p-9}{14}})$

Таблица 9 — Характеристические многочлены для кривых $C' : y^2 = x^{2g+1} + cx^{g+1} + x$ над $\mathbb{F}_{p^2}$.

g	Условия	$\chi_{C',p^2}(T) \pmod p$
2	$p \equiv 1 \pmod 4$	$T^2(T - P_{\frac{p-1}{4}}^{p+1})^2$
2	$p \equiv 3 \pmod 4$	$T^2(T - P_{\frac{p-3}{4}}^{p+1})^2$
3	$p \equiv 1 \pmod 3$	$T^3(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-1}{6}}^{p+1})^2$
3	$p \equiv 2 \pmod 3$	$T^3(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-5}{6}}^{p+1})^2$
4	$p \equiv 1 \pmod 8$	$T^4(T - P_{\frac{p-1}{8}}^{p+1})^2(T - P_{\frac{3p-3}{8}}^{p+1})^2$
4	$p \equiv 3 \pmod 8$	$T^4(T - P_{\frac{p-3}{8}}^{p} P_{\frac{3p-1}{8}})^2(T - P_{\frac{3p-1}{8}}^{p} P_{\frac{p-3}{8}})^2$
4	$p \equiv 5 \pmod 8$	$T^4(T - P_{\frac{p-5}{8}}^{p} P_{\frac{3p-7}{8}})^2(T - P_{\frac{3p-7}{8}}^{p} P_{\frac{p-5}{8}})^2$
4	$p \equiv 7 \pmod 8$	$T^4(T - P_{\frac{p-7}{8}}^{p+1})^2(T - P_{\frac{3p-5}{8}}^{p+1})^2$
5	$p \equiv 1 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-1}{10}}^{p+1})^2(T - P_{\frac{3p-3}{10}}^{p+1})^2$
5	$p \equiv 2 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}}^{p+1})(T^2 - P_{\frac{p-7}{10}}^{2p} P_{\frac{3p-1}{10}}^{2})(T^2 - P_{\frac{3p-1}{10}}^{2p} P_{\frac{p-7}{10}}^{2})$
5	$p \equiv 3 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}}^{p+1})(T^2 - P_{\frac{p-3}{10}}^{2p} P_{\frac{3p-9}{10}}^{2})(T^2 - P_{\frac{3p-9}{10}}^{2p} P_{\frac{p-3}{10}}^{2})$
5	$p \equiv 4 \pmod 5$	$T^5(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-9}{10}}^{p+1})^2(T - P_{\frac{3p-7}{10}}^{p+1})^2$
6	$p \equiv 1 \pmod{12}$	$T^6(T - P_{\frac{p-1}{4}}^{p+1})^2(T - P_{\frac{p-1}{12}}^{p+1})^2(T - P_{\frac{5p-5}{12}}^{p+1})^2$
6	$p \equiv 5 \pmod{12}$	$T^6(T - P_{\frac{p-1}{4}}^{p+1})^2(T - P_{\frac{p-5}{12}}^{p} P_{\frac{5p-1}{12}})^2(T - P_{\frac{5p-1}{12}}^{p} P_{\frac{p-5}{12}})^2$
6	$p \equiv 7 \pmod{12}$	$T^6(T - P_{\frac{p-3}{4}}^{p+1})^2(T - P_{\frac{p-7}{12}}^{p} P_{\frac{5p-11}{12}})^2(T - P_{\frac{5p-11}{12}}^{p} P_{\frac{p-7}{12}})^2$
6	$p \equiv 11 \pmod{12}$	$T^6(T - P_{\frac{p-3}{4}}^{p+1})^2(T - P_{\frac{p-11}{12}}^{p+1})^2(T - P_{\frac{5p-7}{12}}^{p+1})^2$
7	$p \equiv 1 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-1}{14}}^{p+1})^2(T - P_{\frac{5p-5}{14}}^{p+1})^2(T - P_{\frac{3p-3}{14}}^{p+1})^2$
7	$p \equiv 2 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T^3 - P_{\frac{p-9}{14}}^{p+1} P_{\frac{5p-3}{14}}^{p+1} P_{\frac{3p-13}{14}}^{p+1})^2$
7	$p \equiv 3 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T^3 - P_{\frac{p-3}{14}}^{p+1} P_{\frac{3p-9}{14}}^{p+1} P_{\frac{5p-1}{14}}^{p+1})^2$
7	$p \equiv 4 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T^3 - P_{\frac{p-11}{14}}^{p+1} P_{\frac{3p-5}{14}}^{p+1} P_{\frac{5p-13}{14}}^{p+1})^2$
7	$p \equiv 5 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T^3 - P_{\frac{p-5}{14}}^{p+1} P_{\frac{3p-1}{14}}^{p+1} P_{\frac{5p-11}{14}}^{p+1})^2$
7	$p \equiv 6 \pmod 7$	$T^7(T - P_{\frac{p-1}{2}}^{p+1})(T - P_{\frac{p-13}{14}}^{p+1})^2(T - P_{\frac{3p-11}{14}}^{p+1})^2(T - P_{\frac{5p-9}{14}}^{p+1})^2$

Приложение Б

Список характеристических многочленов для кривых $C : y^2 = x^{2g+1} + ax^{g+1} + bx$

В Таблице 10 представлены характеристические многочлены $\pmod p$ гиперэллиптических кривых вида $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ над конечным полем $\mathbb{F}_p$, $p > 2$, $p \nmid g$, $P_m := P_m\left(-\frac{a}{2\sqrt{b}}\right)$, $b_i := \sqrt{b}^{\frac{p-1}{i}}$. Многочлены получены по методу из §2.3.4.

Таблица 10 — Характеристические многочлены для кривых $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ над $\mathbb{F}_p$.

g	Условия	$\chi_{C,p}(T) \pmod p$
2	$p \equiv 1 \pmod 4$	$T^2(T - b_4^3 P_{\frac{p-1}{4}})(T - b_4 P_{\frac{p-1}{4}})$
2	$p \equiv 3 \pmod 4$	$T^2(T^2 - b_2^2 P^2_{\frac{p-3}{4}})$
3	$p \equiv 1 \pmod 3$	$T^3(T - b_2 P_{\frac{p-1}{2}})(T - b_6^5 P_{\frac{p-1}{6}})(T - b_6 P_{\frac{p-1}{6}})$
3	$p \equiv 2 \pmod 3$	$T^3(T - b_2 P_{\frac{p-1}{2}})(T^2 - b_2^2 P^2_{\frac{p-5}{6}})$
4	$p \equiv 1 \pmod 8$	$T^4(T - b_8^5 P_{\frac{3p-3}{8}})(T - b_8^3 P_{\frac{3p-3}{8}})(T - b_8^7 P_{\frac{p-1}{8}})(T - b_8 P_{\frac{p-1}{8}})$
4	$p \equiv 3 \pmod 8$	$T^4(T^2 - b_2^3 P_{\frac{3p-1}{8}} P_{\frac{p-3}{8}})(T^2 - b_2 P_{\frac{3p-1}{8}} P_{\frac{p-3}{8}})$
4	$p \equiv 5 \pmod 8$	$T^4(T^2 - b_4^5 P_{\frac{3p-7}{8}} P_{\frac{p-5}{8}})(T^2 - b_4^3 P_{\frac{3p-7}{8}} P_{\frac{p-5}{8}})$
4	$p \equiv 7 \pmod 8$	$T^4(T^2 - b_2^2 P^2_{\frac{3p-5}{8}})(T^2 - b_2^2 P^2_{\frac{p-7}{8}})$
5	$p \equiv 1 \pmod 5$	$T^5(T - b_2 P_{\frac{p-1}{2}})(T - b_{10}^7 P_{\frac{3p-3}{10}})(T - b_{10}^3 P_{\frac{3p-3}{10}})(T - b_{10}^9 P_{\frac{p-1}{10}})(T - b_{10} P_{\frac{p-1}{10}})$
5	$p \equiv 2 \pmod 5$	$T^5(T - b_2 P_{\frac{p-1}{2}})(T^4 - b_2^4 P^2_{\frac{3p-1}{10}} P^2_{\frac{p-7}{10}})$
5	$p \equiv 3 \pmod 5$	$T^5(T - b_2 P_{\frac{p-1}{2}})(T^4 - b_2^4 P^2_{\frac{3p-9}{10}} P^2_{\frac{p-3}{10}})$
5	$p \equiv 4 \pmod 5$	$T^5(T - b_2 P_{\frac{p-1}{2}})(T^2 - b_2^2 P^2_{\frac{3p-7}{10}})(T^2 - b_2^2 P^2_{\frac{p-9}{10}})$
6	$p \equiv 1 \pmod{12}$	$T^6(T - b_{12}^7 P_{\frac{5p-5}{12}})(T - b_{12}^5 P_{\frac{5p-5}{12}})(T - b_{12}^9 P_{\frac{p-1}{4}})(T - b_{12}^3 P_{\frac{p-1}{4}})(T - b_{12}^{11} P_{\frac{p-1}{12}})\times$ $\times(T - b_{12} P_{\frac{p-1}{12}})$
6	$p \equiv 5 \pmod{12}$	$T^6(T - b_4^3 P_{\frac{p-1}{4}})(T - b_4 P_{\frac{p-1}{4}})(T^2 - b_2^3 P_{\frac{5p-1}{12}} P_{\frac{p-5}{12}})(T^2 - b_2 P_{\frac{5p-1}{12}} P_{\frac{p-5}{12}})$
6	$p \equiv 7 \pmod{12}$	$T^6(T^2 - b_2^2 P^2_{\frac{p-3}{4}})(T^2 - b_3^4 P_{\frac{5p-11}{12}} P_{\frac{p-7}{12}})(T^2 - b_3^2 P_{\frac{5p-11}{12}} P_{\frac{p-7}{12}})$
6	$p \equiv 11 \pmod{12}$	$T^6(T^2 - b_2^2 P^2_{\frac{p-3}{4}})(T^2 - b_2^2 P^2_{\frac{5p-7}{12}})(T^2 - b_2^2 P^2_{\frac{p-11}{12}})$
7	$p \equiv 1 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T - b_{14}^9 P_{\frac{5p-5}{14}})(T - b_{14}^5 P_{\frac{5p-5}{14}})(T - b_{14}^{11} P_{\frac{3p-3}{14}})(T - b_{14}^3 P_{\frac{3p-3}{14}})\times$ $\times(T - b_{14}^{13} P_{\frac{p-1}{14}})(T - b_{14} P_{\frac{p-1}{14}})$
7	$p \equiv 2 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T^3 - b_2^3 P_{\frac{5p-3}{14}} P_{\frac{3p-13}{14}} P_{\frac{p-9}{14}})^2$
7	$p \equiv 3 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T^6 - b_2^6 P^2_{\frac{5p-1}{14}} P^2_{\frac{3p-9}{14}} P^2_{\frac{p-3}{14}})$
7	$p \equiv 4 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T^3 - b_2^3 P_{\frac{5p-13}{14}} P_{\frac{3p-5}{14}} P_{\frac{p-11}{14}})^2$
7	$p \equiv 5 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T^6 - b_2^6 P^2_{\frac{5p-11}{14}} P^2_{\frac{3p-1}{14}} P^2_{\frac{p-5}{14}})$
7	$p \equiv 6 \pmod 7$	$T^7(T - b_2 P_{\frac{p-1}{2}})(T^2 - b_2^2 P^2_{\frac{5p-9}{14}})(T^2 - b_2^2 P^2_{\frac{3p-11}{14}})(T^2 - b_2^2 P^2_{\frac{p-13}{14}})$

Приложение B

Рекуррентные формулы для вычисления коэффициентов характеристических многочленов над расширениями

Пусть A — абелево многообразие размерности g над конечным полем $\mathbb{F}_q$. Обозначим его характеристический многочлен эндоморфизма Фробениуса над $\mathbb{F}_q$ как

$$\chi_{A,q}(T) = T^{2g} + a_1 T^{2g-1} + \ldots + a_g T^g + a_{g-1} q T^{g-1} + \ldots + a_1 q^{g-1} T + q^g,$$

а над $\mathbb{F}_{q^k}$ следующим образом:

$$\chi_{A,q^k}(T) = T^{2g} + a_{1,k} T^{2g-1} + \ldots + a_{g,k} T^g + a_{g-1,k} q^k T^{g-1} + \ldots + a_{1,k} q^{k(g-1)} T + q^{kg}.$$

В последующих подразделах приводим формулы, выражающие $a_{1,k}, \ldots, a_{g,k}$ через $a_1, \ldots, a_g$.

B.1 Размерность $g = 2$

$$a_{1,2} = -a_1^2 + 2a_2,$$
$$a_{2,2} = a_2^2 - 4a_2 q + 2a_{1,2} q + 2q^2.$$

B.2 Размерность $g = 3$

$$a_{1,3} = a_1^3 - 3a_1 a_2 + 3a_3,$$
$$a_{2,3} = 3a_1^2 a_2 q - 3a_1^2 q^2 - 3a_1 a_2 a_3 + a_2^3 - 3a_2^2 q + 3a_3^2 + 3q^3,$$
$$a_{3,3} = 6a_3 q^3 - 6a_1 a_2 q^3 - 3a_1^2 a_3 q^2 + 6a_1 a_2^2 q^2 - 3a_2^2 a_3 q + a_3^3.$$

B.3 Размерность $g = 4$

$$a_{1,2} = -a_1^2 + 2a_2,$$
$$a_{2,2} = -2a_1a_3 + a_2^2 + 2a_4,$$
$$a_{3,2} = -a_2^2q + 2a_2a_4 + 2a_2q^2 - a_3^2 - 2a_4q + a_{2,2}q,$$
$$a_{4,2} = 4a_2a_4q - 4a_3^2q + a_4^2 - 4a_4q^2 + 2a_{1,2}q^3 + 2a_{2,2}q^2 - 2a_{3,2}q + 2q^4.$$

B.4 Размерность $g = 5$

$$\begin{aligned}
a_{1,5} &= 5a_5 - 5a_1a_4 + (5a_1^2 - 5a_2)a_3 + 5a_1a_2^2 - 5a_1^3a_2 + a_1^5,\\
a_{2,5} &= 5q^5 - 5a_1^2q^4 - 5a_2^2q^3 + 5a_1^2a_2q^3 - 5a_3^2q^2 + 10a_1a_2a_3q^2 - 5a_1^3a_3q^2 - 5a_4^2q +\\
&\quad + 10a_1a_3a_4q + 5a_2^2a_4q - 15a_1^2a_2a_4q + 5a_1^4a_4q + 10a_5^2 - 15a_1a_4a_5 - 15a_2a_3a_5 +\\
&\quad + 10a_1^2a_3a_5 + 10a_1a_2^2a_5 - 5a_1^3a_2a_5 + 5a_2a_4^2 + 5a_1^2a_4^2 + 5a_3^2a_4 - 5a_1a_2a_3a_4 +\\
&\quad - 5a_1^3a_3a_4 - 5a_2^3a_4 + 5a_1^2a_2^2a_4 - 5a_1a_3^3 + 5a_2^2a_3^2 + 5a_1^2a_2a_3^2 - 5a_1a_2^3a_3 + a_2^5,\\
a_{3,5} &= 20a_5q^5 - 20a_1a_4q^5 - 20a_2a_3q^5 + 10a_1^2a_3q^5 + 10a_1a_2^2q^5 - 5a_1^3a_2q^5 +\\
&\quad - 15a_1^2a_5q^4 + 20a_1a_2a_4q^4 + 10a_1^3a_4q^4 + 10a_1a_3^2q^4 - 5a_1^2a_2a_3q^4 - 5a_1^4a_3q^4 +\\
&\quad - 5a_1a_2^3q^4 + 5a_1^3a_2^2q^4 - 15a_2^2a_5q^3 + 10a_1^2a_2a_5q^3 + 20a_2a_3a_4q^3 - 15a_1^2a_3a_4q^3 +\\
&\quad - 5a_1a_2^2a_4q^3 - 5a_1^3a_2a_4q^3 - 15a_1a_2a_3^2q^3 + 10a_2^3a_3q^3 + 10a_1^2a_2^2a_3q^3 - 5a_1a_2^4q^3 +\\
&\quad - 15a_3^2a_5q^2 + 20a_1a_2a_3a_5q^2 - 5a_1^3a_3a_5q^2 + 10a_3a_4^2q^2 - 15a_1a_2a_4^2q^2 + 10a_1^3a_4^2q^2 +\\
&\quad - 5a_1a_3^2a_4q^2 - 15a_2^2a_3a_4q^2 + 10a_1^2a_2a_3a_4q^2 + 10a_2a_3^3q^2 + 5a_1^2a_3^3q^2 - 15a_1a_2^2a_3^2q^2 +\\
&\quad + 5a_2^4a_3q^2 - 15a_4^2a_5q + 20a_1a_3a_4a_5q + 10a_2^2a_4a_5q - 15a_1^2a_2a_4a_5q + 10a_1a_4^3q +\\
&\quad - 5a_2a_3a_4^2q - 15a_1^2a_3a_4^2q + 10a_1a_2^2a_4^2q - 5a_3^3a_4q + 10a_1a_2a_3^2a_4q - 5a_2^3a_3a_4q +\\
&\quad + 10a_5^3 - 15a_1a_4a_5^2 - 15a_2a_3a_5^2 + 5a_1^2a_3a_5^2 + 5a_1a_2^2a_5^2 + 10a_2a_4^2a_5 + 5a_1^2a_4^2a_5 +\\
&\quad + 10a_3^2a_4a_5 - 5a_1a_2a_3a_4a_5 - 5a_2^3a_4a_5 - 5a_1a_3^3a_5 + 5a_2^2a_3^2a_5 - 5a_3a_4^3 - 5a_1a_2a_4^3 +\\
&\quad + 5a_1a_3^2a_4^2 + 5a_2^2a_3a_4^2 - 5a_2a_3^3a_4 + a_3^5,
\end{aligned}$$

$$
\begin{aligned}
a_{4,5} = {} & 10q^{10} - 15a_1^2q^9 - 15a_2^2q^8 + 15a_1^2a_2q^8 + 5a_1^4q^8 - 15a_3^2q^7 + 30a_1a_2a_3q^7 + \\
& - 5a_1^3a_3q^7 - 5a_1^2a_2^2q^7 - 5a_1^4a_2q^7 - 15a_4^2q^6 + 30a_1a_3a_4q^6 + 15a_2^2a_4q^6 + \\
& - 15a_1^2a_2a_4q^6 - 5a_1^2a_3^2q^6 - 30a_1a_2^2a_3q^6 + 10a_1^3a_2a_3q^6 + 5a_2^4q^6 + 5a_1^2a_2^3q^6 + \\
& + 30a_5^2q^5 - 45a_1a_4a_5q^5 - 45a_2a_3a_5q^5 + 10a_1^2a_3a_5q^5 + 10a_1a_2^2a_5q^5 + 15a_2a_4^2q^5 + \\
& + 25a_1^2a_4^2q^5 + 15a_3^2a_4q^5 - 15a_1a_2a_3a_4q^5 - 15a_1^3a_3a_4q^5 - 5a_2^3a_4q^5 + 10a_1^2a_2^2a_4q^5 + \\
& - 5a_1a_3^3q^5 + 25a_2^2a_3^2q^5 + 10a_1^2a_2a_3^2q^5 - 15a_1a_2^2a_3q^5 - 15a_1^2a_5^2q^4 + 40a_1a_2a_4a_5q^4 + \\
& + 10a_1^3a_4a_5q^4 + 20a_1a_3^2a_5q^4 - 5a_1^2a_2a_3a_5q^4 - 5a_1a_2^3a_5q^4 - 30a_1a_3a_4^2q^4 + \\
& - 5a_2^2a_4^2q^4 - 30a_1^2a_2a_4^2q^4 - 30a_2a_3^2a_4q^4 + 15a_1^2a_3^2a_4q^4 + 30a_1a_2^2a_3a_4q^4 - 5a_2^4a_4q^4 + \\
& + 5a_3^4q^4 - 20a_1a_2a_3^3q^4 + 10a_2^3a_3^2q^4 - 15a_2^2a_5^2q^3 + 5a_1^2a_2a_5^2q^3 + 40a_2a_3a_4a_5q^3 + \\
& - 15a_1^2a_3a_4a_5q^3 - 5a_1a_2^2a_4a_5q^3 - 15a_1a_2a_3^2a_5q^3 + 10a_2^3a_3a_5q^3 - 10a_2a_4^3q^3 + \\
& + 10a_1^2a_4^3q^3 - 5a_3^2a_4^2q^3 + 30a_1a_2a_3a_4^2q^3 + 5a_2^3a_4^2q^3 + 10a_1a_3^3a_4q^3 - 30a_2^2a_3^2a_4q^3 + \\
& + 5a_2a_3^4q^3 - 15a_3^2a_5^2q^2 + 10a_1a_2a_3a_5^2q^2 + 20a_3a_4^2a_5q^2 - 15a_1a_2a_4^2a_5q^2 + \\
& - 5a_1a_3^2a_4a_5q^2 - 15a_2^2a_3a_4a_5q^2 + 10a_2a_3^3a_5q^2 + 5a_4^4q^2 - 20a_1a_3a_4^3q^2 + 5a_2^2a_4^3q^2 + \\
& + 15a_2a_3^2a_4^2q^2 - 5a_3^4a_4q^2 - 15a_4^2a_5^2q + 10a_1a_3a_4a_5^2q + 5a_2^2a_4a_5^2q + 10a_1a_4^3a_5q + \\
& - 5a_2a_3a_4^2a_5q - 5a_3^3a_4a_5q - 5a_2a_4^4q + 5a_3^2a_4^3q + 5a_5^4 - 5a_1a_4a_5^3 + \\
& - 5a_2a_3a_5^3 + 5a_2a_4^2a_5^2 + 5a_3^2a_4a_5^2 - 5a_3a_4^3a_5 + a_4^5, \\
a_{5,5} = {} & 30a_5q^{10} - 30a_1a_4q^{10} - 30a_2a_3q^{10} + 10a_1^2a_3q^{10} + 10a_1a_2^2q^{10} - 30a_1^2a_5q^9 + \\
& + 40a_1a_2a_4q^9 + 20a_1^3a_4q^9 + 20a_1a_3^2q^9 - 10a_1^2a_2a_3q^9 - 10a_1a_2^3q^9 - 30a_2^2a_5q^8 + \\
& + 20a_1^2a_2a_5q^8 + 5a_1^4a_5q^8 + 40a_2a_3a_4q^8 - 30a_1^2a_3a_4q^8 - 10a_1a_2^2a_4q^8 + \\
& - 30a_1^3a_2a_4q^8 - 30a_1a_2a_3^2q^8 + 10a_1^3a_3^2q^8 + 20a_2^3a_3q^8 + 10a_1^2a_2^2a_3q^8 - 30a_3^2a_5q^7 + \\
& + 40a_1a_2a_3a_5q^7 - 5a_1^2a_2^2a_5q^7 + 20a_3a_4^2q^7 - 30a_1a_2a_4^2q^7 - 10a_1a_3^2a_4q^7 + \\
& - 30a_2^2a_3a_4q^7 + 40a_1^2a_2a_3a_4q^7 + 20a_1a_2^3a_4q^7 + 20a_2a_3^3q^7 - 30a_1a_2^2a_3^2q^7 + \\
& - 30a_4^2a_5q^6 + 40a_1a_3a_4a_5q^6 + 20a_2^2a_4a_5q^6 - 5a_1^2a_3^2a_5q^6 - 30a_1a_2^2a_3a_5q^6 + \\
& + 5a_2^4a_5q^6 + 20a_1a_4^3q^6 - 10a_2a_3a_4^2q^6 - 30a_1^2a_3a_4^2q^6 + 10a_1a_2^2a_4^2q^6 - 10a_3^3a_4q^6 + \\
& + 40a_1a_2a_3^2a_4q^6 - 30a_2^3a_3a_4q^6 - 10a_1a_3^4q^6 + 20a_2^2a_3^3q^6 + 20a_5^3q^5 - 30a_1a_4a_5^2q^5 + \\
& - 30a_2a_3a_5^2q^5 + 20a_2a_4^2a_5q^5 + 20a_1^2a_4^2a_5q^5 + 20a_3^2a_4a_5q^5 - 10a_1a_2a_3a_4a_5q^5 + \\
& + 20a_2^2a_3^2a_5q^5 - 10a_3a_4^3q^5 - 30a_1a_2a_4^3q^5 + 20a_1a_3^2a_4^2q^5 + 20a_2^2a_3a_4^2q^5 + \\
& - 30a_2a_3^3a_4q^5 - 5a_1^2a_5^3q^4 + 20a_1a_2a_4a_5^2q^4 + 10a_1a_3^2a_5^2q^4 - 30a_1a_3a_4^2a_5q^4 + \\
& - 5a_2^2a_4^2a_5q^4 - 30a_2a_3^2a_4a_5q^4 + 5a_3^4a_5q^4 + 10a_1a_4^4q^4 + 20a_2a_3a_4^3q^4 + 10a_3^3a_4^2q^4 + \\
& - 5a_2^2a_5^3q^3 + 20a_2a_3a_4a_5^2q^3 - 10a_2a_4^3a_5q^3 - 5a_3^2a_4^2a_5q^3 - 10a_3a_4^4q^3 - 5a_3^2a_5^3q^2 + \\
& + 10a_3a_4^2a_5^2q^2 + 5a_4^4a_5q^2 - 5a_4^2a_5^3q + a_5^5.
\end{aligned}
$$

B.5 Размерность $g = 6$

$$
\begin{aligned}
a_{1,2} &= 2a_2 - a_1^2,\\
a_{2,2} &= 2a_4 - 2a_1a_3 + a_2^2,\\
a_{3,2} &= 2a_6 - 2a_1a_5 + 2a_2a_4 - a_3^2,\\
a_{4,2} &= 2a_4q^2 - 2a_6q - 2a_2a_4q + a_{3,2}q + a_3^2q + 2a_2a_6 - 2a_3a_5 + a_4^2,\\
a_{5,2} &= 2a_2q^4 + a_{2,2}q^3 - a_2^2q^3 - 2a_6q^2 + a_{3,2}q^2 + a_3^2q^2 + 2a_2a_6q - 4a_3a_5q - a_{4,2}q +\\
&\quad + a_4^2q + 2a_4a_6 - a_5^2,\\
a_{6,2} &= 2q^6 + 2a_{1,2}q^5 + 2a_{2,2}q^4 - 4a_6q^3 + 2a_{3,2}q^3 + 4a_2a_6q^2 - 8a_3a_5q^2 - 2a_{4,2}q^2 +\\
&\quad + 4a_4^2q^2 + 4a_4a_6q - 2a_{5,2}q - 4a_5^2q + a_6^2,\\
a_{1,3} &= 3a_3 - 3a_1a_2 + a_1^3,\\
a_{2,3} &= 3a_6 - 3a_1a_5 - 3a_2a_4 + 3a_1^2a_4 + 3a_3^2 - 3a_1a_2a_3 + a_2^3,\\
a_{3,3} &= 3a_3q^3 - 3a_1a_4q^2 - 3a_2a_5q + 3a_1^2a_5q + 6a_3a_6 - 3a_1a_2a_6 - 3a_4a_5 +\\
&\quad - 3a_1a_3a_5 + 3a_2^2a_5 + 3a_1a_4^2 - 3a_2a_3a_4 + a_3^3,\\
a_{4,3} &= 3q^6 - 3a_1^2q^5 - 3a_2^2q^4 + 3a_1^2a_2q^4 + 6a_3^2q^3 - 3a_1a_2a_3q^3 +\\
&\quad - 3a_4^2q^2 - 3a_1a_3a_4q^2 + 3a_2^2a_4q^2 - 3a_5^2q + 6a_1a_4a_5q +\\
&\quad - 3a_2a_3a_5q + 3a_6^2 - 3a_1a_5a_6 - 3a_2a_4a_6 + 3a_3^2a_6 + 3a_2a_5^2 - 3a_3a_4a_5 + a_4^3,\\
a_{5,3} &= 6a_3q^6 - 3a_1a_2q^6 - 3a_1a_4q^5 - 3a_1^2a_3q^5 + 3a_1a_2^2q^5 - 3a_2a_5q^4 +\\
&\quad + 6a_1a_2a_4q^4 - 3a_2^2a_3q^4 + 6a_3a_6q^3 - 3a_4a_5q^3 - 3a_1a_3a_5q^3 - 3a_2a_3a_4q^3 +\\
&\quad + 3a_3^3q^3 - 3a_1a_4a_6q^2 + 3a_1a_5^2q^2 + 6a_2a_4a_5q^2 - 3a_3a_4^2q^2 - 3a_2a_5a_6q - 3a_3a_5^2q +\\
&\quad + 3a_4^2a_5q + 3a_3a_6^2 - 3a_4a_5a_6 + a_5^3,\\
a_{6,3} &= 6a_6q^6 - 6a_1a_5q^6 - 6a_2a_4q^6 + 6a_3^2q^6 - 3a_1^2a_6q^5 +\\
&\quad + 12a_1a_2a_5q^5 - 6a_1a_3a_4q^5 - 3a_2^2a_6q^4 - 6a_2a_3a_5q^4 +\\
&\quad + 6a_2a_4^2q^4 + 6a_3^2a_6q^3 - 6a_3a_4a_5q^3 - 3a_4^2a_6q^2 + 6a_4a_5^2q^2 - 3a_5^2a_6q + a_6^3.
\end{aligned}
$$

Приложение Г

Данные для специализированного алгоритма для кривых рода 4

$$a_1^{16} + c_{14}a_1^{14} + c_{12}a_1^{12} + c_{10}a_1^{10} + c_8a_1^8 + c_6a_1^6 + c_4a_1^4 + c_2a_1^2 + c_0 = 0.$$

$$\begin{aligned}
c_0 =&(128q^4 - 128a_{1,2}q^3 + 32a_{1,2}^2q^2 + 128a_{3,2}q - 64a_{1,2}a_{2,2}q+\\
&+ 16a_{1,2}^3q - 64a_{4,2} + 16a_{2,2}^2 - 8a_{1,2}^2a_{2,2} + a_{1,2}^4)^2,\\
c_2 =&-131072q^7 + 163840a_{1,2}q^6 - 32768a_{2,2}q^5 - 65536a_{1,2}^2q^5 - 81920a_{3,2}q^4+\\
&+ 45056a_{1,2}a_{2,2}q^4 + 5120a_{1,2}^3q^4 + 65536a_{4,2}q^3 + 49152a_{1,2}a_{3,2}q^3+\\
&- 16384a_{2,2}^2q^3 - 12288a_{1,2}^2a_{2,2}q^3 + 2048a_{1,2}^4q^3 - 49152a_{1,2}a_{4,2}q^2+\\
&+ 4096a_{1,2}^2a_{3,2}q^2 + 8192a_{1,2}a_{2,2}^2q^2 - 5120a_{1,2}^3a_{2,2}q^2 + 768a_{1,2}^5q^2+\\
&+ 16384a_{2,2}a_{4,2}q - 16384a_{3,2}^2q + 4096a_{1,2}a_{2,2}a_{3,2}q - 1024a_{1,2}^3a_{3,2}q+\\
&- 4096a_{2,2}^3q + 4096a_{1,2}^2a_{2,2}^2q - 1280a_{1,2}^4a_{2,2}q + 128a_{1,2}^6q+\\
&+ 8192a_{3,2}a_{4,2} - 6144a_{1,2}a_{2,2}a_{4,2} + 1536a_{1,2}^3a_{4,2} + 2048a_{2,2}^2a_{3,2}+\\
&- 1024a_{1,2}^2a_{2,2}a_{3,2} + 128a_{1,2}^4a_{3,2} - 512a_{1,2}a_{2,2}^3 + 384a_{1,2}^3a_{2,2}^2+\\
&- 96a_{1,2}^5a_{2,2} + 8a_{1,2}^7,\\
c_4 =&253952q^6 - 233472a_{1,2}q^5 + 47104a_{2,2}q^4 + 65024a_{1,2}^2q^4 + 57344a_{3,2}q^3+\\
&- 26624a_{1,2}a_{2,2}q^3 - 5632a_{1,2}^3q^3 - 61440a_{4,2}q^2 - 12288a_{1,2}a_{3,2}q^2+\\
&+ 7168a_{2,2}^2q^2 - 2048a_{1,2}^2a_{2,2}q^2 + 1344a_{1,2}^4q^2 + 22528a_{1,2}a_{4,2}q+\\
&- 2048a_{2,2}a_{3,2}q - 2560a_{1,2}^2a_{3,2}q + 3584a_{1,2}a_{2,2}^2q - 1280a_{1,2}^3a_{2,2}q+\\
&+ 96a_{1,2}^5q - 7168a_{2,2}a_{4,2} + 1280a_{1,2}^2a_{4,2} + 4096a_{3,2}^2+\\
&- 2048a_{1,2}a_{2,2}a_{3,2} + 512a_{1,2}^3a_{3,2} - 256a_{2,2}^3 + 576a_{1,2}^2a_{2,2}^2+\\
&- 240a_{1,2}^4a_{2,2} + 28a_{1,2}^6,\\
c_6 =&-204800q^5 + 136192a_{1,2}q^4 - 16384a_{2,2}q^3 - 29696a_{1,2}^2q^3+\\
&- 12288a_{3,2}q^2 + 1024a_{1,2}a_{2,2}q^2 + 4096a_{1,2}^3q^2 + 20480a_{4,2}q+\\
&- 1024a_{1,2}a_{3,2}q + 1024a_{2,2}^2q - 320a_{1,2}^4q - 2560a_{1,2}a_{4,2}+\\
&- 1024a_{2,2}a_{3,2} + 768a_{1,2}^2a_{3,2} + 384a_{1,2}a_{2,2}^2 - 320a_{1,2}^3a_{2,2} + 56a_{1,2}^5,
\end{aligned}$$

$$
\begin{aligned}
c_8 =& 79104q^4 - 38144a_{1,2}q^3 + 512a_{2,2}q^2 + 7104a_{1,2}^2q^2 + 256a_{3,2}q + \\
&+ 640a_{1,2}a_{2,2}q - 800a_{1,2}^3q - 2176a_{4,2} + 512a_{1,2}a_{3,2} + 96a_{2,2}^2 + \\
&- 240a_{1,2}^2a_{2,2} + 70a_{1,2}^4, \\
c_{10} =& -15360q^3 + 5376a_{1,2}q^2 + 256a_{2,2}q - 768a_{1,2}^2q + 128a_{3,2} + \\
&- 96a_{1,2}a_{2,2} + 56a_{1,2}^3, \\
c_{12} =& 1472q^2 - 352a_{1,2}q - 16a_{2,2} + 28a_{1,2}^2, \\
c_{14} =& 8a_{1,2} - 64q.
\end{aligned}
$$