

О ЧИСЛЕ ТОЧЕК НА КРИВОЙ $y^2 = x^7 + ax^4 + bx$
НАД КОНЕЧНЫМ ПОЛЕМ

С. А. Новоселов^а, Ю. Ф. Болтнев^б

Балтийский федеральный университет им. И. Канта,
ул. Александра Невского, 14, 236041 Калининград, Россия
E-mail: ^аsnovoselov@kantiana.ru, ^бyuri.boltnev@gmail.com

Аннотация. Представлены явные формулы для числа точек на гиперэллиптической кривой рода 3 вида $y^2 = x^7 + ax^4 + bx$ над конечным полем \mathbb{F}_q характеристики $p > 3$. Как следствие, показано, что задача подсчёта точек на данном классе кривых имеет сложность $O(\log^4 q)$ битовых операций. Табл. 2, библиогр. 27.

Ключевые слова: гиперэллиптическая кривая, число точек, характеристический многочлен.

Введение

Гиперэллиптической кривой C рода g над конечным полем \mathbb{F}_q характеристики $p > 2$ называется кривая, задаваемая уравнением

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

где f — многочлен степени $2g+1$ или $2g+2$, не имеющий кратных корней над замыканием поля.

Гиперэллиптические кривые рода $g = 1$ представляют собой эллиптические кривые, которые в настоящее время на практике широко используются в асимметричной криптографии. В частности, есть стандартизированные [1, 2] цифровые подписи, построенные на их основе. Гиперэллиптические кривые рода $g = 2, 3$ изучаются как альтернатива эллиптическим кривым для построения криптосистем на основе задачи вычисления дискретного логарифма [3]. При этом в вычислениях используется ассоциированная с кривой группа — якобиан кривой $\text{Jac}_C(\mathbb{F}_q)$ и для приложений необходимо знать число элементов в данной группе. За точным определением и свойствами якобиана отсылаем к работе [4, § 14.1].

Работа первого автора выполнена при финансовой поддержке Минобрнауки РФ (соглашение № 075–02–2022–872).

© С. А. Новоселов, Ю. Ф. Болтнев, 2022

Нахождение числа точек на кривой и её якобиане в общем случае является нетривиальной задачей, которую мы будем в дальнейшем называть задачей «подсчёта точек». Для решения данной задачи в случае эллиптических кривых есть достаточно эффективный алгоритм Схоофа — Элкиса — Аткина (SEA) [5] с эвристической сложностью $O(\log^4 q)$ битовых операций. Для гиперэллиптических кривых рода $g > 1$ теоретически доказано [6], что сложность задачи подсчёта точек равна $O(\log^{cg} q)$ для некоторой константы c . Для частных случаев есть более точные оценки: $O(\log^8 q)$ для $g = 2$ [7] и $O(\log^{14} q)$ для $g = 3$ [8]. В случае рода 3 полиномиальные от $\log q$ алгоритмы уже становятся непригодными для практических вычислений и на практике, как правило, используются экспоненциальные алгоритмы. Исходя из этого, в работе [9] предложено использовать кривые рода 3 в криптографических конструкциях на основе групп с «неизвестным порядком», т. е. конечных групп, которые легко построить, но при этом сложно вычислить их порядок. В качестве примеров конструкций на группах с неизвестным порядком можно привести верифицируемые функции задержки [10], механизмы для отправки сообщений «в будущее» (time-lock puzzles) [11] и криптографические аккумуляторы [12]. Таким образом, безопасность таких конструкций строится на сложности вычисления порядка группы, в частности, для гиперэллиптических кривых — порядка якобиана, т. е. подсчёта точек.

В настоящей работе выводятся явные формулы для числа элементов в якобиане кривых рода 3 вида $y^2 = x^7 + ax^4 + bx$, которые позволяют снизить сложность подсчёта точек с $O(\log^{14} q)$ до $O(\log^4 q)$. Тем самым данный класс кривых слабый для криптографических конструкций на группах с неизвестным порядком, основанных на кривых рода 3.

Рассматриваемая кривая рода 3 относится к классу кривых вида $y^2 = x^{2g+1} + ax^{g+1} + bx$. Для случая кривых рода 2 данного класса в [13] представлен алгоритм подсчёта точек на основе сведения задачи к эллиптическим кривым, снижающий сложность подсчёта точек с $O(\log^8 q)$ до $O(\log^4 q)$, а в [14] получены уже явные формулы для порядка якобиана данных кривых. В [15] алгоритм из работы [13] обобщён на кривые вида $y^2 = x^{2g+1} + ax^{g+1} + bx$ произвольного рода сведением задачи к кривым рода $\frac{g-1}{2}$. В нашей работе явные формулы из [14] обобщаются с рода 2 на род 3. По сравнению с общим алгоритмом из [15] найденные формулы позволяют считать число точек более эффективно.

Работа организована следующим образом. Разд. 1 содержит предварительные сведения и определения, разд. 2 — информацию о разложении якобиана кривой на эллиптические кривые над алгебраическим замыканием поля $\overline{\mathbb{F}}_q$. В разд. 3 с помощью разложения якобиана строятся полные списки всех возможных характеристических многочленов эндоморфизма Фробениуса, которые кодируют в себе как информацию

о числе элементов в якобиане, так и о числе точек на кривой. В разд. 4 с использованием списков характеристических многочленов выводятся явные формулы для порядка якобиана, а на их основе выводится сложность задачи подсчёта точек. Разд. 5 содержит практические эксперименты, оценивающие эффективность подсчёта точек на основе явных формул по сравнению с другими алгоритмами. Кроме того, приведены примеры вычисления порядка якобиана для размеров параметров, предложенных в [9] для построения групп с неизвестным порядком с уровнем безопасности в 128 бит.

1. Предварительные сведения

Известно, что число точек на кривой $C: y^2 = f(x)$ над конечным полем \mathbb{F}_q и в её якобиане удовлетворяет границам Хассе — Вейля:

$$q + 1 - 2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q},$$

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

Для нахождения точного числа точек нам потребуется понятие дзета-функции кривой C , которая определяется следующим образом:

$$Z(C/\mathbb{F}_q; T) = \exp \left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n \right) = \frac{L_{C,q}(T)}{(1-T)(1-qT)}.$$

Последнее равенство — частный случай гипотез Вейля [4, теорема 8.3], которые в настоящее время уже доказаны. Отображение $x \mapsto x^q$ индуцирует эндоморфизм в якобиане кривой $\text{Jac}_C(\overline{\mathbb{F}}_q)$, который называется *эндоморфизмом Фробениуса*. Характеристический многочлен эндоморфизма Фробениуса определяется с помощью многочлена $L_{C,q}$ следующим образом [4, утверждение 8.4]:

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

Для характеристического многочлена выполняются свойства

$$\# \text{Jac}_C(\mathbb{F}_q) = \chi_{C,q}(1)$$

и $\#C(\mathbb{F}_q) = q + 1 - a_1$, где a_1 — коэффициент $\chi_{C,q}$ при T^{2g-1} , поэтому задача подсчёта точек сводится к задаче нахождения характеристического многочлена. Значение $-a_1$ называется *следом эндоморфизма Фробениуса*.

В дальнейшем нам потребуется также понятие абелева многообразия и некоторые его свойства. Опишем их кратко, за более подробным изложением и доказательствами отсылаем к [4, § 4.3]. *Абелевым многообразием* над полем k называется неприводимое проективное алгебраическое многообразие (множество нулей некоторой системы полиномиальных уравнений с коэффициентами из k), обладающее структурой

группы. *Размерностью* абелева многообразия A называется размерность соответствующей системы уравнений, она обозначается через $\dim A$. Абелевы многообразия размерности 2 называются *абелевыми поверхностями*. Известно, что якобианы кривых являются абелевыми многообразиями размерности, равной роду кривой, поэтому вся теория абелевых многообразий может быть применена и к ним.

Изогенией двух абелевых многообразий A и B , заданных над полем \mathbb{F}_q , называется гомоморфизм $\varphi: A \rightarrow B$, который над алгебраическим замыканием $\overline{\mathbb{F}}_q$ сюръективен и имеет конечное ядро. Если существует изогения между абелевыми многообразиями A и B , то они называются *изогенными*, что обозначается через $A \sim B$.

Абелево многообразие A называется *простым*, если не существует изогении из абелева многообразия A в $B \times C$, где B и C — абелевы многообразия. По теореме Пуанкаре о полной приводимости [16, § 19, теорема 1] для любого абелева многообразия A

$$A \sim A_1 \times \cdots \times A_m,$$

где $m \geq 1$ и A_1, \dots, A_m — простые абелевы многообразия такие, что $\dim A = \dim A_1 + \cdots + \dim A_m$. Для абелевых многообразий можно, так же, как и для якобианов кривых, определить эндоморфизм Фробениуса и его характеристический многочлен $\chi_{A,q}$ [16, § 19]. При этом известно, что этот многочлен имеет следующий симметричный вид:

$$\chi_{A,q}(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + a_{g-1} q T^{g-1} + \cdots + a_1 q^{g-1} T + q^g, \quad (1)$$

где $|a_i| \leq \binom{2g}{i} q^{i/2}$. При этом, как и в случае якобианов, выполняется равенство $\#A(\mathbb{F}_q) = \chi_{A,q}(1)$. Кроме того, по теореме Тейта [17, теорема 1] данный многочлен является инвариантом относительно изогении (как следствие, все изогенные абелевы многообразия имеют одинаковое число точек) и выполняется свойство

$$\chi_{A,q} = \chi_{A_1,q} \cdots \chi_{A_m,q}. \quad (2)$$

Таким образом, в случае непростых абелевых многообразий задача подсчёта точек сводится к задаче подсчёта точек на многообразиях меньшей размерности. Заметим, что над базовым полем абелево многообразие может быть простым или содержать в себе нетривиальное абелево подмногообразие, но при этом раскладываться над некоторым расширением поля. Это позволяет упростить задачу подсчёта точек, рассчитав число точек сначала над расширением поля, а затем спустившись к базовому полю. Все кривые вида $y^2 = x^{2g+1} + ax^{g+1} + bx$ обладают таким свойством, и оно использовалось для упрощения задачи подсчёта точек в работах [13–15], которые мы продолжаем в последующих разделах.

2. Разложение якобиана кривой над расширением поля

Пусть $C: y^2 = x^7 + ax^4 + bx$ — это гиперэллиптическая кривая рода 3 над полем \mathbb{F}_q характеристики $p > 3$. Обозначим через $\mathbb{F}_q(\sqrt[3]{b})$ поле, полученное присоединением корня третьей степени из b к полю \mathbb{F}_q . В данном разделе опишем разложение якобиана кривой C на эллиптические кривые над расширением поля, чтобы в дальнейшем получить явные формулы для числа элементов в Jac_C как выражение от следов эндоморфизма Фробениуса данных эллиптических кривых. Всю необходимую информацию о разложении якобиана кривой даёт

Лемма 1. Пусть $C: y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая над конечным полем \mathbb{F}_q характеристики $p > 3$. Тогда

- (1) $\text{Jac}_C \sim E_1 \times A$ над \mathbb{F}_q ;
- (2) $\text{Jac}_C \sim E_1 \times E_2^2$ над $\mathbb{F}_q(\sqrt[3]{b})$, если $q \equiv 1 \pmod{3}$;
- (3) $\text{Jac}_C \sim E_1 \times E_2 \times \widetilde{E}_2$ над $\mathbb{F}_q(\sqrt[3]{b})$, если $q \equiv 2 \pmod{3}$.

Здесь A — некоторая абелева поверхность, E_1 и E_2 — эллиптические кривые, задаваемые уравнениями $y^2 = x^3 + ax^2 + bx$ и $y^2 = x^3 - 3\sqrt[3]{b}x + a$ соответственно. Кроме того, \widetilde{E}_2 — квадратичное кручение кривой E_2 , т. е. $\widetilde{E}_2 \simeq E_2$ над $\mathbb{F}_{q^2}(\sqrt[3]{b})$.

ДОКАЗАТЕЛЬСТВО. Напрямую можно проверить, что отображение

$$\psi_{E_1}: (x, y) \mapsto (x^3, xy)$$

отображает точку кривой C в точку кривой E_1 и тем самым является морфизмом кривых. Если существует нетривиальный морфизм кривых, то из теорем Клаймана — Серра [18, теорема 5] и Тэйта [17, теорема 1(b)] следует, что

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

над \mathbb{F}_q для некоторой абелевой поверхности A . П. (1) доказан.

Для доказательства второго и третьего пунктов воспользуемся результатами из [15]. Имеет место [15, утверждение 2] следующее разложение якобиана:

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

над $\mathbb{F}_q(\sqrt[3]{b}, \zeta_3)$, где ζ_3 — примитивный корень степени 3 из единицы. П. (2) следует из того, что $\zeta_3 \in \mathbb{F}_q$ тогда и только тогда, когда $q \equiv 1 \pmod{3}$. В случае $q \equiv 2 \pmod{3}$ имеем $\zeta_3 \in \mathbb{F}_{q^2}$, поэтому разложение $\text{Jac}_C \sim E_1 \times E_2^2$ имеет место над $\mathbb{F}_{q^2}(\sqrt[3]{b})$. С другой стороны, согласно теореме 2 из [15] имеем ещё одно разложение якобиана:

$$\text{Jac}_C \sim E_2 \times \text{Jac}_\chi$$

над $\mathbb{F}_q(\sqrt[3]{b})$, где X — гиперэллиптическая кривая

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

при этом присутствие кривой E_2 в разложении следует из существования отображения

$$\psi_{E_2}: (x, y) \mapsto \left(x + \frac{\sqrt[3]{b}}{x}, \frac{y}{x^2} \right)$$

из кривой C в E_2 . Таким образом, над $\mathbb{F}_q(\sqrt[3]{b})$ имеется одновременно два разложения:

$$\text{Jac}_C \sim E_1 \times A \sim E_2 \times \text{Jac}_X.$$

Более того, так как имеется два различных отображения ψ_{E_1} и ψ_{E_2} , заданных над $\mathbb{F}_q(\sqrt[3]{b})$, над данным полем имеем

$$\text{Jac}_C \sim E_1 \times E_2 \times \widetilde{E}_2 \quad (3)$$

для некоторой кривой \widetilde{E}_2 , существование которой следует из теоремы Пуанкаре о полной приводимости. Осталось показать, что \widetilde{E}_2 — квадратичное кручение E_2 . Заметим, что отображения ψ_{E_1} и ψ_{E_2} заданы над полем $\mathbb{F}_q(\sqrt[3]{b})$, а значит, и над его квадратичным расширением $\mathbb{F}_{q^2}(\sqrt[3]{b})$, поэтому разложение (3) имеет место также и над полем $\mathbb{F}_{q^2}(\sqrt[3]{b})$. При этом над $\mathbb{F}_{q^2}(\sqrt[3]{b})$ кривая \widetilde{E}_2 задана явно [15, доказательство утверждения 2] уравнением

$$y^2 = x^3 - 3\zeta_3^2 \sqrt[3]{b}x + a$$

с соответствующим отображением

$$\psi_{\widetilde{E}_2}: (x, y) \mapsto \left(x + \frac{\zeta_3^2 \sqrt[3]{b}}{x}, \frac{y}{x^2} \right)$$

из кривой C в \widetilde{E}_2 . Кроме того, E_2 изоморфна \widetilde{E}_2 над $\mathbb{F}_{q^2}(\sqrt[3]{b})$ посредством изоморфизма $(x, y) \mapsto (\zeta_3 x, y)$, т. е. \widetilde{E}_2 — квадратичное кручение E_2 . Лемма 1 доказана.

3. Характеристические многочлены кривой

Используя разложение якобиана из разд. 2, можем описать характеристические многочлены кривой C , а затем, как следствие, и число элементов якобиана $\# \text{Jac}_C = \chi_{C,q}(1)$. Рассмотрим сначала самый простой случай, когда b является кубическим вычетом.

Теорема 1. Пусть $C: y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3 над конечным полем \mathbb{F}_q характеристики $p > 3$, и пусть b — кубический вычет. Тогда характеристический многочлен $\chi_{C,q}(T)$ равен

- (1) $(T^2 - t_1 T + q)(T^2 - t_2 T + q)^2$, если $q \equiv 1 \pmod{3}$;
- (2) $(T^2 - t_1 T + q)(T^2 - t_2 T + q)(T^2 + t_2 T + q)$, если $q \equiv 2 \pmod{3}$.

Здесь t_1 и t_2 — следы эндоморфизма Фробениуса эллиптических кривых $E_1: y^2 = x^3 + ax^2 + bx$ и $E_2: y^2 = x^3 - 3\sqrt[3]{b}x + a$ соответственно.

ДОКАЗАТЕЛЬСТВО следует из леммы 1 и формулы (2). Если $\sqrt[3]{b} \in \mathbb{F}_q$, то $\text{Jас}_C \sim E_1 \times E_2^2$ для $q \equiv 1 \pmod{3}$ и $\chi_{C,q}(T) = \chi_{E_1,q}(T) \cdot \chi_{E_2,q}^2(T)$, откуда следует п. (1). В случае $q \equiv 2 \pmod{3}$ имеем $\text{Jас}_C \sim E_1 \times E_2 \times \widetilde{E}_2$ и $\chi_{C,q}(T) = \chi_{E_1,q}(T) \cdot \chi_{E_2,q}(T) \cdot \chi_{\widetilde{E}_2,q}(T)$, где \widetilde{E}_2 — квадратичное кручение кривой E_2 . Из [4, утверждение 13.32] известно, что $\chi_{\widetilde{E}_2}(T) = \chi_{E_2}(-T)$, поэтому $\chi_{C,q}(T) = \chi_{E_1}(T) \cdot \chi_{E_2}(T) \cdot \chi_{E_2}(-T)$, из чего следует п. (2). Теорема 1 доказана.

Теперь перейдём к более сложному случаю, когда $\sqrt[3]{b} \notin \mathbb{F}_q$. По лемме 1 над конечным полем \mathbb{F}_q имеет место разложение $\text{Jас}_C \sim E_1 \times A$, где A может быть простой абелевой поверхностью. Следовательно, по формуле (2) получаем

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

Характеристический многочлен для E_1 может быть достаточно эффективно вычислен с помощью алгоритма SEA [5], поэтому остаётся только найти коэффициенты

$$\chi_{A,q}(T) = T^4 - s_1 T^3 + s_2 T^2 - s_1 q T + q^2.$$

Характеристические многочлены абелевых поверхностей можно классифицировать, используя понятие p -ранга кривой, который определяется следующим образом. Группа p -кручения абелевой поверхности A (а в общем случае — абелева многообразия) задаётся как

$$A[p] = \{P \in A(\overline{\mathbb{F}}_q) \mid [p]P = 0\}.$$

Тогда данная группа имеет [16, § 6] следующую структуру:

$$A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^r,$$

где целое число r удовлетворяет неравенствам $0 \leq r \leq \dim A$ и называется p -рангом абелевой поверхности A . Так как p -ранг является инвариантом относительно изогении [16, § 15], для $A \sim A_1 \times A_2$ выполняется $r(A) = r(A_1) + r(A_2)$. В случае $r = \dim A = 2$ абелева поверхность называется *обычной*. Эллиптическая кривая называется *суперсингулярной*, если она имеет p -ранг 0. Абелево многообразие (как частный случай — якобиан кривой) называется *суперсингулярным*, если оно раскладывается на суперсингулярные эллиптические кривые над замыканием поля. Абелевы поверхности p -ранга 0 суперсингулярны [4, замечание 4.75]. Так как в нашем случае $A \sim E_2^2$ над замыканием поля $\overline{\mathbb{F}}_q$, то $r(A) = 2r(E_2) \in \{0, 2\}$ и A не может иметь p -ранг 1.

Таким образом, абелева поверхность A либо суперсингулярная, либо обычная, причём определить суперсингулярность или обычность можно

по кривой E_2 . Характеристические многочлены суперсингулярных абелевых многообразий размерности 1–7 полностью описываются в [19]. Для обычных геометрически разложимых абелевых поверхностей классификация характеристических многочленов представлена в [20]. Используя классификацию из данных работ для упрощения формул, получаем следующий результат.

Теорема 2. Пусть $C: y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3, определённая над конечным полем \mathbb{F}_q размера $q = p^n$ характеристики $p > 3$, b — кубический невычет. Пусть также $E_1: y^2 = x^3 + ax^2 + bx$ и $\tilde{E}_2: y^2 = x^3 - 3bx + ab$ — эллиптические кривые над \mathbb{F}_q , а t_1 и \tilde{t}_2 — их следы эндоморфизма Фробениуса. Тогда $\chi_{C,q}(T) = (T^2 - t_1T + q)\chi_{A,q}(T)$, где $\chi_{A,q}(T)$ определяется следующим образом.

(1) Если кривая \tilde{E}_2 обычная, то $\chi_{A,q}(T)$ — один из следующих многочленов:

- (a) $T^4 - \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 - \tilde{t}_2qT + q^2$, $\sqrt{b} \notin \mathbb{F}_q$;
- (b) $T^4 + \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 + \tilde{t}_2qT + q^2$, $\sqrt{b} \in \mathbb{F}_q$;
- (c) $(T^2 - \tilde{t}_2T + q)^2$, $\sqrt{b} \notin \mathbb{F}_q$, $A \sim \tilde{E}_2^2$;
- (d) $(T^2 + \tilde{t}_2T + q)^2$, $\sqrt{b} \in \mathbb{F}_q$, A непростая.

(2) Если кривая \tilde{E}_2 суперсингулярная, то $\chi_{A,q}(T)$ — один из следующих многочленов:

- (a) $T^4 - qT^2 + q^2$;
- (b) $T^4 + 2qT^2 + q^2$;
- (c) $(T^2 + \sqrt{q}T + q)^2$, n чётное, $p \equiv 2 \pmod{3}$, A непростая;
- (d) $(T^2 + \sqrt{q}T + q)(T^2 - 2\sqrt{q}T + q)$, n чётное, $p \equiv 2 \pmod{3}$, A непростая;
- (e) $(T^2 - \sqrt{q}T + q)^2$, $p \equiv 5 \pmod{6}$, n чётное, A непростая;
- (f) $(T^2 - \sqrt{q}T + q)(T^2 + 2\sqrt{q}T + q)$, $p \equiv 5 \pmod{6}$, n чётное, A непростая;
- (g) $(T^2 \pm 2\sqrt{q}T + q)^2$, n чётное, A непростая;
- (h) $(T^2 + \sqrt{q}T + q)^2$, $p \equiv 1 \pmod{3}$, n чётное, A простая;
- (i) $(T^2 - \sqrt{q}T + q)^2$, $p \equiv 1 \pmod{6}$, n чётное, A простая.

ДОКАЗАТЕЛЬСТВО. Заметим, что при $q \equiv 2 \pmod{3}$ любое b является кубическим вычетом в \mathbb{F}_q , так как отображение $x \mapsto x^3$ в этом случае является биекцией на мультипликативной группе \mathbb{F}_q^\times поля \mathbb{F}_q . Поэтому считаем далее, что $q \equiv 1 \pmod{3}$ и тем самым примитивный корень третьей степени ζ_3 лежит в \mathbb{F}_q . Тогда по лемме 1 имеем $\text{Jac } C \sim E_1 \times E_2^2$ над \mathbb{F}_{q^3} , где $E_2: y^2 = x^3 - 3\sqrt[3]{b}x + a$. Как следствие,

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

где $t_{1,3}$ и $t_{2,3}$ — следы эндоморфизма Фробениуса эллиптических кривых E_1 и E_2 над \mathbb{F}_{q^3} . При этом для любой эллиптической кривой E след Фробениуса t_k над \mathbb{F}_{q^k} можно выразить через след Фробениуса t над \mathbb{F}_q по известной [4, пример 17.4] рекуррентной формуле:

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

Применяя данную формулу к $t_{2,3}$, получаем

$$t_{2,3} = t_2^3 - 3t_2q. \quad (4)$$

Тогда

$$\chi_{C,q^3}(T) = (T^2 - t_{1,3}T + q^3)(T^2 - (t_2^3 - 3t_2q)T + q^3)^2.$$

С другой стороны, над базовым полем \mathbb{F}_q по той же лемме 1 имеем $\text{Jac}_C \sim E_1 \times A$ и

$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^4 - s_1T^3 + s_2T^2 - s_1qT + q^2)$$

для некоторых целых s_1, s_2 таких, что $|s_1| \leq 4\sqrt{q}$ и $|s_2| \leq 6q$. При этом последние неравенства следуют из общих ограничений для коэффициентов характеристического многочлена в (1). Тем самым необходимо выразить s_1 и s_2 через t_2 . Однако кривая E_2 определена над \mathbb{F}_{q^3} , но не над базовым полем \mathbb{F}_q , поэтому не можем посчитать t_2 напрямую. Значит, вместо кривой E_2 будем использовать её квадратичное кручение $\tilde{E}_2: y^2 = x^3 - 3bx + ab$, изоморфное кривой E_2 над $\mathbb{F}_{q^3}(\sqrt{b})$ посредством изоморфизма $(x, y) \mapsto (\frac{x}{\sqrt[3]{b}}, \frac{y}{\sqrt{b}})$. Из свойств квадратичных кручений имеем $\chi_{\tilde{E}_2,q^3}(T) = \chi_{E_2,q^3}(-T)$ и $t_{2,3} = -\tilde{t}_{2,3}$, если $\sqrt{b} \notin \mathbb{F}_{q^3}$, а при $\sqrt{b} \in \mathbb{F}_{q^3}$ имеем $\chi_{\tilde{E}_2,q}(T) = \chi_{E_2,q}(T)$ и $t_{2,3} = \tilde{t}_{2,3}$.

Найдём выражения s_1, s_2 через t_2 , а затем заменим $t_{2,3}, t_2$ на $\tilde{t}_{2,3}, \tilde{t}_2$, выбирая знак в зависимости от параметра b . Для этого воспользуемся формулой $L_{C,q^3}(T^3) = \prod_{\zeta^3=1} L_{C,q}(\zeta T)$ из [21, доказательство теоремы 5.1.15]. Сравнением коэффициентов в левой и правой частях формулы получаем систему уравнений

$$\begin{cases} 3s_1^2s_2q - 6s_1^2q^2 - s_2^3 + 3s_2q^2 + 2q^3 + t_{2,3}^2 = 0, \\ s_1^3 - 3s_1s_2 + 3s_1q + 2t_{2,3} = 0. \end{cases} \quad (5)$$

При $s_1 = 0$ имеем $t_{2,3} = 0$ и $s_2 = -q$ или $s_2 = 2q$. В этом случае A — суперсингулярная абелева поверхность. Пусть $s_1 \neq 0$. Выражая s_2 во втором уравнении системы и подставляя в первое, получаем

$$\begin{cases} (t_{2,3} + 3qs_1 - s_1^3)^2 (8t_{2,3} - 12qs_1 + s_1^3) = 0, \\ s_2 = \frac{s_1^2}{3} + q + \frac{2t_{2,3}}{3s_1}, \\ s_1 \neq 0. \end{cases} \quad (6)$$

Таким образом, s_1 — это решение одного из уравнений

$$s_1^3 - 3qs_1 - t_{2,3} = 0, \quad (7)$$

$$s_1^3 - 12qs_1 + 8t_{2,3} = 0. \quad (8)$$

Выражая значение $t_{2,3}$ в (7) и (8) и подставляя его в (6), получаем $s_2 = s_1^2 - q$ в первом случае и $s_2 = \frac{s_1^2}{3} + 2q$ во втором.

Заметим, что при подстановке $s_1 = t_2$ в (7) и $s_1 = -2t_2$ в (8) получается формула (4), поэтому $s_1 = t_2$ и $s_1 = -2t_2$ — решения системы уравнений (5). Остальные решения (7) и (8) следующие:

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

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

где $d = 12q - 3t_2^2$. В случае, когда E_2 — обычная кривая, абелева поверхность A также будет обычной, и согласно [20, утверждение 29] в этом случае возможны только варианты $s_1 = t_2$ и $s_1 = -2t_2$.

Пусть E_2 — суперсингулярная кривая. Тогда A — суперсингулярная абелева поверхность. В [19, § 12] приведён список суперсингулярных характеристических многочленов для размерностей 1–7, причём для непротых абелевых поверхностей список получается перебором списка возможных характеристических многочленов суперсингулярных эллиптических кривых. Осталось только отсеять многочлены, не удовлетворяющие системе уравнений (5).

Рассмотрим сначала случай, когда A — непростая суперсингулярная абелева поверхность. По результатам Дойринга и Ватерхауза [19, теоремы 12.1.1, 12.2.1] при $p > 3$ имеем следующие варианты для $t_{2,3}$:

- (1) 0, n нечётное;
- (2) $-\sqrt{q^3}$, n чётное, $p \equiv 2 \pmod{3}$;
- (3) 0, n чётное, $p \equiv 3 \pmod{4}$;
- (4) $\sqrt{q^3}$, n чётное, $p \equiv 5 \pmod{6}$;
- (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 возможных комбинаций суперсингулярных эллиптических следов Фробениуса получаем следующий список возможных вариантов для характеристических многочленов непротых суперсингулярных абелевых поверхностей для $p > 3$ и чётного n :

- (1) $(T^2 + \sqrt{q}T + q)^2$, $p \equiv 2 \pmod{3}$, $s_1 = -2\sqrt{q}$;
- (2) $(T^2 + \sqrt{q}T + q)(T^2 + q)$, $p \equiv 11 \pmod{12}$, $s_1 = -\sqrt{q}$;
- (3) $(T^2 + \sqrt{q}T + q)(T + \sqrt{q})^2$, $p \equiv 2 \pmod{3}$, $s_1 = -3\sqrt{q}$;
- (4) $(T^2 + \sqrt{q}T + q)(T - \sqrt{q})^2$, $p \equiv 2 \pmod{3}$, $s_1 = \sqrt{q}$;
- (5) $(T^2 + q)(T^2 - \sqrt{q}T + q)$, $p \equiv 11 \pmod{12}$, $s_1 = \sqrt{q}$;

- (6) $(T^2 + q)(T \pm \sqrt{q})^2$, $p \equiv 3 \pmod{4}$, $s_1 = \mp 2\sqrt{q}$;
- (7) $(T^2 - \sqrt{q}T + q)^2$, $p \equiv 5 \pmod{6}$, $s_1 = 2\sqrt{q}$;
- (8) $(T^2 - \sqrt{q}T + q)(T + \sqrt{q})^2$, $p \equiv 5 \pmod{6}$, $s_1 = -\sqrt{q}$;
- (9) $(T^2 - \sqrt{q}T + q)(T - \sqrt{q})^2$, $p \equiv 5 \pmod{6}$, $s_1 = 3\sqrt{q}$;
- (10) $(T \pm \sqrt{q})^4$, $s_1 = \mp 4\sqrt{q}$.

Напрямую можно проверить, что системе уравнений (6) удовлетворяют только коэффициенты (s_1, s_2) многочленов из пп. (1), (4), (7), (8) и (10).

Осталось рассмотреть случай, когда A — простая абелева поверхность. В этом случае согласно [19, теоремы 12.1, 12.2] имеем для $s_1 \neq 0$ и $p > 3$ следующий список возможных суперсингулярных характеристических многочленов.

- (1) $T^4 \pm \sqrt{pq}T^3 + 3qT^2 \pm q\sqrt{pq}T + q^2$, n нечётное, $p = 5$;
- (2) $(T^2 + \sqrt{q}T + q)^2$, $p \equiv 1 \pmod{3}$, n чётное;
- (3) $(T^2 - \sqrt{q}T + q)^2$, $p \equiv 1 \pmod{6}$, n чётное;
- (4) $T^4 + \sqrt{q}T^3 + qT^2 + q^{3/2}T + q^2$, $p \not\equiv 1 \pmod{5}$, n чётное;
- (5) $T^4 - \sqrt{q}T^3 + qT^2 - q^{3/2}T + q^2$, $p \not\equiv 1 \pmod{10}$, n чётное.

После подстановки соответствующих данных многочленам коэффициентов (s_1, s_2) в систему (5) видим, что данной системе удовлетворяют только многочлены из пп. (2) и (3). Теорема 2 доказана.

4. Формулы для числа точек и сложность подсчёта точек

Так как теперь известен полный список возможных характеристических многочленов для кривой C , можем найти порядки якобиана, используя свойство $\# \text{Jac}_C(\mathbb{F}_q) = \chi_{C,q}(1)$ и теоремы 1, 2. Для наиболее частого случая, когда кривая E_2 обычная, они представлены в табл. 1.

Таблица 1

Формулы для порядка якобиана
кривой $C: y^2 = x^7 + ax^4 + bx$ над \mathbb{F}_q , $q = p^n$, $p > 3$, $p \nmid \tilde{t}_2$

$\# \text{Jac}_C(\mathbb{F}_q)$	Условия
$(q+1-t_1)(q^2-q+1+\tilde{t}_2^2-(q+1)\tilde{t}_2)$	$\sqrt[6]{b} \notin \mathbb{F}_q$
$(q+1-t_1)(q^2-q+1+\tilde{t}_2^2+(q+1)\tilde{t}_2)$	$\sqrt{b} \in \mathbb{F}_q$, $\sqrt[3]{b} \notin \mathbb{F}_q$
$(q+1-t_1)(q+1-\tilde{t}_2)^2$	$\sqrt[6]{b} \notin \mathbb{F}_q$
$(q+1-t_1)(q+1+\tilde{t}_2)^2$	$\sqrt{b} \in \mathbb{F}_q$, $\sqrt[3]{b} \notin \mathbb{F}_q$
$(q+1-t_1)(q+1-t_2)^2$	$q \equiv 1 \pmod{3}$, $\sqrt[3]{b} \in \mathbb{F}_q$
$(q+1-t_1)(q+1-t_2)(q+1+t_2)$	$q \equiv 2 \pmod{3}$

Следы эндоморфизма Фробениуса t_1, t_2, \tilde{t}_2 эллиптических кривых E_1, E_2, \tilde{E}_2 можно вычислить с помощью алгоритма Схоофа — Элкиса — Аткина [5] за эвристическое время $O(\log^4 q)$.

Следствие 1. Пусть $C: y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3 над конечным полем \mathbb{F}_q характеристики $p > 3$. Тогда задача нахождения характеристического многочлена эндоморфизма Фробениуса и числа точек $\# \text{Jас}_C(\mathbb{F}_q)$ имеет эвристическую сложность $O(\log^4 q)$.

ДОКАЗАТЕЛЬСТВО. Заметим, что следы t_2 и \tilde{t}_2 отличаются только знаком, поэтому достаточно вычислить \tilde{t}_2 для кривой \tilde{E}_2 , которая определена над \mathbb{F}_q . Вычисление \tilde{t}_2 имеет эвристическую сложность $O(\log^4 q)$ битовых операций [5]. После вычисления \tilde{t}_2 становится известно, является кривая \tilde{E}_2 суперсингулярной ($p \mid \tilde{t}_2$) или обычной ($p \nmid \tilde{t}_2$). Применяя теоремы 1 и 2, получаем список из одного или нескольких возможных характеристических многочленов $\chi_{C,q}(T)$ и соответствующих им кандидатов на групповой порядок $N = \chi_{C,q}(1)$. Для определения истинного значения можно воспользоваться тем свойством, что для любого $D \in \text{Jас}_C(\mathbb{F}_q)$ выполняется $\# \text{Jас}_C(\mathbb{F}_q) \cdot D = 0$. Таким образом, отсекаем кандидаты N на порядок якобиана, для которых не выполняется условие $N \cdot D = 0$ для нескольких случайных элементов $D \in \text{Jас}_C(\mathbb{F}_q)$. Выбор случайного элемента D якобиана кривой рода 3 эквивалентен [4, § 14.1.2] нахождению трёх точек кривой C , а нахождение одной точки кривой эквивалентно вычислению квадратного корня в \mathbb{F}_q . Вычисление квадратного корня по алгоритму Тонелли — Шэнкса занимает время $O(\log^4 q)$ [22, § 1.5]. Как следствие, выбор случайного элемента D и весь процесс подсчёта точек занимают такое же время. Следствие 1 доказано.

5. Экспериментальные результаты

Для оценки эффективности вычислений на основе полученных формул наш метод нахождения порядка якобиана был реализован в системе компьютерной алгебры SageMath [23]. Исходный код реализации вместе с примерами вычислений доступен на домашней странице первого автора¹⁾. Результаты вычислений на компьютере с процессором Xeon E-2146G, 3,50 ГГц представлены в табл. 2 в сравнении с другими алгоритмами.

Для сравнения взято время вычисления в `hypellfrob` для максимального размера поля, на котором работает алгоритм при ограничении в 16 ГБ памяти. Заметим, что библиотека `hypellfrob` реализует экспоненциальный от $\log p$ алгоритм из [24]. Хотя в настоящее время доказано [6], что для любой гиперэллиптической кривой задача подсчёта точек имеет полиномиальную сложность, для кривых рода 3 эта оценка теоретическая. На практике для кривых рода 3 общего вида такой полиномиальный

¹⁾<https://crypto-kantiana.com/semyon.novoselov>

Таблица 2

**Вычисления для случайных
кривых $y^2 = x^7 + ax^4 + bx$ над простым полем \mathbb{F}_p**

$\log_2 p$	$\log_2 (\# \text{Jac}_C)$	Метод	Время
43	129	hyrellfrob [24, 25]	31 мин
322	958	[15, алгоритм 2]	39 мин
906	2716	(данная работа)	23 мин
1131	3392	(данная работа)	3 ч 10 мин

алгоритм ещё никем не реализован, поэтому мы сравниваем эффективность с доступным алгоритмом из hyrellfrob с экспоненциальной сложностью для кривых общего вида и специализированным алгоритмом из [15].

Последняя строка табл. 2 — время вычисления порядка якобиана на размерах параметров, предложенных в [9, табл. 2] для построения групп с неизвестным порядком на кривых рода 3 с «параноидальным» уровнем безопасности в 128 бит. Возможность считать порядок якобиана для размера поля $p \approx 2^{1131}$ за столь малое время делает кривые класса $y^2 = x^7 + ax^4 + bx$ слабыми для использования в конструкциях на группах с неизвестным порядком. Таким образом, мы описали успешную атаку на представленный класс гиперэллиптических кривых.

Заключение

В данной работе получены явные формулы для характеристических многочленов и порядка якобиана кривой $y^2 = x^7 + ax^4 + bx$. Это позволило снизить сложность подсчёта точек на данной кривой с $O(\log^{14} q)$ до $O(\log^4 q)$ битовых операций. Кроме того, данные формулы позволяют на практике вычислять порядок якобиана для размеров параметров, предложенных в [9] для криптографических конструкций на группах с неизвестным порядком с уровнем безопасности в 128 бит. Как следствие, кривые вида $y^2 = x^7 + ax^4 + bx$ не подходят для таких криптографических конструкций. Предварительные результаты данной работы докладывались на конференциях SibeCrypt'19 [26] и ANTS-XIV [27].

ЛИТЕРАТУРА

1. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введ. 01.06.2019. М.: Стандартинформ, 2018. 21 с.
2. FIPS 186-4. Digital signature standard (DSS). Gaithersburg, MD: NIST, 2013. Available at <https://doi.org/10.6028/NIST.FIPS.186-4> (accessed Mar. 9, 2022).

3. **Koblitz N.** Hyperelliptic cryptosystems // J. Cryptol. 1989. V. 1, No. 3. P. 139–150.
4. Handbook of elliptic and hyperelliptic curve cryptography. Boca Raton, FL: Chapman Hall/CRC, 2006. 808 p.
5. **Schoof R.** Counting points on elliptic curves over finite fields // J. Théor. Nombres Bordx. 1995. V. 7, No. 1. P. 219–254.
6. **Abelard S., Gaudry P., Spaenlehauer P. J.** Improved complexity bounds for counting points on hyperelliptic curves // Found. Comput. Math. 2019. V. 19, No. 3. P. 591–621.
7. **Gaudry P., Schost É.** Genus 2 point counting over prime fields // J. Symb. Comput. 2012. V. 47, No. 4. P. 368–400.
8. **Abelard S.** Counting points on hyperelliptic curves in large characteristic: Algorithms and complexity : PhD thes. Nancy: Univ. Lorraine, 2018.
9. **Dobson S., Galbraith S. D., Smith B.** Trustless unknown-order groups // J. Math. Cryptol. [in print].
10. **Boneh D., Bonneau J., Bünz B., Fisch B.** Verifiable delay functions // Advances in cryptology – CRYPTO 2018. Proc. 38th Annu. Int. Cryptol. Conf. (Santa Barbara, CA, USA, Aug. 19–23, 2018). Pt. I. Cham: Springer, 2018. P. 757–788. (Lect. Notes Comput. Sci.; V. 10991).
11. **Rivest R. L., Shamir A., Wagner D. A.** Time-lock puzzles and timed-release Crypto. Tech. rep. MIT-LCS-TR-684. Cambridge, MA: MIT, 1996. 9 p.
12. **Benaloh J., de Mare M.** One-way accumulators: A decentralized alternative to digital signatures // Advances in cryptology – EUROCRYPT'93. Proc. Workshop Theory Appl. Cryptogr. Tech. (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 274–285. (Lect. Notes Comput. Sci.; V. 765).
13. **Satoh T.** Generating genus two hyperelliptic curves over large characteristic finite fields // Advances in cryptology – EUROCRYPT 2009. Proc. 28th Annu. Int. Conf. Theory Appl. Cryptogr. Tech. (Cologne, Germany, Apr. 26–30, 2009). Heidelberg: Springer, 2009. P. 536–553. (Lect. Notes Comput. Sci.; V. 5479).
14. **Guillevic A., Vergnaud D.** Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions // Pairing-based cryptography – Pairing 2012. Rev. Sel. Pap. 5th Int. Conf. (Cologne, Germany, May 16–18, 2012). Heidelberg: Springer, 2013. P. 234–253. (Lect. Notes Comput. Sci.; V. 7708).
15. **Novoselov S. A.** Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$ // Finite Fields Appl. 2020. V. 68, ID 101757. 27 p.
16. **Mumford D.** Abelian varieties. Oxford: Oxford Univ. Press, 1974.
17. **Tate J.** Endomorphisms of Abelian varieties over finite fields // Invent. Math. 1966. V. 2, No. 2. P. 134–144.
18. **Blanco-Chacón I., Chapman R., Fordham S., McGuire G.** Divisibility of L-polynomials for a family of curves // Contemporary Developments in Finite Fields and Applications. Singapore: World Sci., 2016. P. 1–10.
19. **Singh V., McGuire G., Zaytsev A.** Classification of characteristic polynomials of simple supersingular Abelian varieties over finite fields // Funct. Approximatio, Comment. Math. 2014. V. 51, No. 2. P. 415–436.

- 20. **Chou K. M. J., Kani E.** Simple geometrically split Abelian surfaces over finite fields // J. Ramanujan Math. Soc. 2014. V. 29, No. 1. P. 31-62.
- 21. **Stichtenoth H.** Algebraic function fields and codes. Heidelberg: Springer, 2009. (Grad. Texts Math.; V. 254).
- 22. **Cohen H.** A course in computational algebraic number theory. Heidelberg: Springer, 1993. (Grad. Texts Math.; V. 138).
- 23. **Stein W.** SageMath. 2021. Available at <https://www.sagemath.org> (accessed Mar. 11, 2022).
- 24. **Harvey D.** Kedlaya's algorithm in larger characteristic // Int. Math. Res. Not. 2007. V. 2007, No. 22, ID rnm095. 29 p.
- 25. **Harvey D.** Hypellfrob. 2008. Available at <https://web.maths.unsw.edu.au/~davidharvey/code/hypellfrob> (accessed Mar. 11, 2022).
- 26. **Novoselov S. A., Boltnev Yu. F.** Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields // Прикл. дискрет. математика. Прил. 2019. № 12. С. 44–46.
- 27. **Novoselov S. A.** Counting points on hyperelliptic curves with geometrically split Jacobians [poster] // 14th Algorithmic Number Theory Symp. (Auckland, New Zealand, June 29–July 4, 2020). Auckland: Univ. Auckland, 2020. Available at <https://www.math.auckland.ac.nz/~sgal018/ANTS/posters/Novoselov.pdf> (accessed Mar. 11, 2022).

Новоселов Семён Александрович
Болтнев Юрий Фёдорович

Статья поступила
31 октября 2021 г.
После доработки —
31 января 2022 г.
Принята к публикации
7 февраля 2022 г.

ON THE NUMBER OF POINTS ON THE CURVE
 $y^2 = x^7 + ax^4 + bx$ OVER A FINITE FIELD

S. A. Novoselov^a and Yu. F. Boltnev^b

Immanuel Kant Baltic Federal University,
14 Aleksandr Nevskii Street, 236041 Kaliningrad, Russia
E-mail: ^asnovoselov@kantiana.ru, ^byuri.boltnev@gmail.com

Abstract. We provide explicit formulae for the number of points on a genus 3 hyperelliptic curve of type $y^2 = x^7 + ax^3 + bx$ over a finite field \mathbb{F}_q of characteristic $p > 3$. As an application of these formulae, we prove that point-counting problem on this type of curves has heuristic time complexity of order $O(\log^4 q)$ bit operations. Tab. 2, bibliogr. 27.

Keywords: hyperelliptic curve, point-counting, characteristic polynomial.

REFERENCES

1. Information technology. Cryptographic data security. Signature and verification processes of electronic digital signature, *GOST 34.10-2018* (Standartinform, Moscow, 2018) [Russian].
2. Digital signature standard (DSS), *FIPS 186-4* (NIST, Gaithersburg, MD, 2013). Available at <https://doi.org/10.6028/NIST.FIPS.186-4> (accessed Mar. 9, 2022).
3. N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptol.* **1** (3), 139–150 (1989).
4. *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (Chapman Hall/CRC, Boca Raton, FL, 2006).
5. R. Schoof, Counting points on elliptic curves over finite fields, *J. Théor. Nombres Bordx.* **7** (1), 219–254 (1995).
6. S. Abelard, P. Gaudry, and P. J. Spaenlehauer, Improved complexity bounds for counting points on hyperelliptic curves, *Found. Comput. Math.* **19** (3), 591–621 (2019).
7. P. Gaudry and É. Schost, Genus 2 point counting over prime fields, *J. Symb. Comput.* **47** (4), 368–400 (2012).

The work of the first author is supported by the Ministry of Science and Higher Education of the Russian Federation (Agreement 075–02–2022–872).

English version: Journal of Applied and Industrial Mathematics **16** (2) (2022).

8. **S. Abelard**, Counting points on hyperelliptic curves in large characteristic: Algorithms and complexity, *PhD Thesis* (Univ. Lorraine, Nancy, 2018).
9. **S. Dobson**, **S. Galbraith**, and **S. Benjamin**, Trustless unknown-order groups, *J. Math. Cryptol.* [in print].
10. **D. Boneh**, **J. Bonneau**, **B. Bünz**, and **B. Fisch**, Verifiable delay functions, in *Advances in Cryptology – CRYPTO 2018* (Proc. 38th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 19–23, 2018), Pt. I (Springer, Cham, 2018), pp. 757–788 (Lect. Notes Comput. Sci., Vol. 10991).
11. **R. L. Rivest**, **A. Shamir**, and **D. A. Wagner**, Time-lock puzzles and timed-release crypto. *Tech. Rep. MIT-LCS-TR-684* (MIT, Cambridge, MA, 1996).
12. **J. Benaloh** and **M. de Mare**, One-way accumulators: A decentralized alternative to digital signatures, in *Advances in Cryptology – EUROCRYPT’93* (Proc. Workshop Theory Appl. Cryptogr. Tech., Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 274–285 (Lect. Notes Comput. Sci., Vol. 765).
13. **T. Satoh**, Generating genus two hyperelliptic curves over large characteristic finite fields, in *Advances in Cryptology – EUROCRYPT 2009* (Proc. 28th Annu. Int. Conf. Theory Appl. Cryptogr. Tech., Cologne, Germany, Apr. 26–30, 2009) (Springer, Heidelberg, 2009), pp. 536–553 (Lect. Notes Comput. Sci., Vol. 5479).
14. **A. Guillevic** and **D. Vergnaud**, Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions, in *Pairing-Based Cryptography – Pairing 2012* (Rev. Sel. Pap. 5th Int. Conf., Cologne, Germany, May 16–18, 2012) (Springer, Heidelberg, 2013), pp. 234–253 (Lect. Notes Comput. Sci., Vol. 7708).
15. **S. A. Novoselov**, Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$, *Finite Fields Appl.* **68**, ID 101757, 27 p. (2020).
16. **D. Mumford**, *Abelian Varieties* (Oxford Univ. Press, Oxford, 1974).
17. **J. Tate**, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (2), 134–144 (1966).
18. **I. B. Chacon**, **R. Chapman**, **S. Fordham**, and **G. McGuire**, Divisibility of L-polynomials for a family of curves, in *Contemporary Developments in Finite Fields and Applications* (World Sci., Singapore, 2016), pp. 1–10.
19. **V. Singh**, **G. McGuire**, and **A. Zaytsev**, Classification of characteristic polynomials of simple supersingular abelian varieties over finite fields, *Funct. Approximatio, Comment. Math.* **51** (2), 415–436 (2014).
20. **K. M. J. Chou** and **E. Kani**, Simple geometrically split abelian surfaces over finite fields, *J. Ramanujan Math. Soc.* **29** (1), 31–62 (2014).
21. **H. Stichtenoth**, *Algebraic Function Fields and Codes* (Springer, Heidelberg, 2009) (Grad. Texts Math., Vol. 254).
22. **H. Cohen**, *A Course in Computational Algebraic Number Theory* (Springer, Heidelberg, 1993) (Grad. Texts Math., Vol. 138).
23. **W. Stein**, SageMath (2021). Available at <https://www.sagemath.org> (accessed Mar. 11, 2022).
24. **D. Harvey**, Kedlaya’s algorithm in larger characteristic, *Int. Math. Res. Not.* **2007** (22), ID rnm095, 29 p. (2007).

- 25. **D. Harvey**, Hypellfrob (2008). Available at <https://web.maths.unsw.edu.au/~davidharvey/code/hypellfrob> (accessed Mar. 11, 2022).
- 26. **S. A. Novoselov** and **Yu. F. Boltnev**, Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields, *Prikl. Diskretn. Mat., Prilozh.*, No. 12, 44–46 (2019).
- 27. **S. A. Novoselov**, Counting points on hyperelliptic curves with geometrically split Jacobians [poster], in *14th Algorithmic Number Theory Symp., Auckland, New Zealand, June 29–July 4, 2020* (Univ. Auckland, Auckland, 2020). Available at <https://www.math.auckland.ac.nz/~sgal018/ANTS/posters/Novoselov.pdf> (accessed Mar. 11, 2022).

Semyon A. Novoselov
Yurii F. Boltnev

Received October 31, 2021
Revised January 31, 2022
Accepted February 7, 2022