УДК: 512.74

Абелевы поверхности над конечным полем с заданным действием Фробениуса на группу l-кручения

Н.С. Колесников, С.А. Новоселов

1) NiKolesnikov@stud.kantiana.ru; Балтийский федеральный университет им. И.Канта

2) snovoselov@kantiana.ru; Балтийский федеральный университет им. И.Канта

Аннотация

В статье рассматриваются абелевы поверхности с действием Фробениуса на группу l-кручения, задаваемым симплектической матрицей. Благодаря исследованию свойств группы симплектических матриц, накладывается ряд ограничений на характеристический многочлен Фробениуса самой поверхности, что позволяет эффективнее производить его вычисление и, как следствие, ускорить алгоритмы для подсчета точек на абелевых поверхностях.

Ключевые слова: Абелевы поверхности, эндоморфизм Фробениуса, подсчёт числа точек, симплектические матрицы.

Одним из актуальных направлений современой криптографии является построение криптосистем с применением абелевых многообразий, главным образом якобианов кривых. Однако сдерживающим фактором практической реализации таких криптосистем является недостаточно ясная картина структуры якобианов и трудности подсчета точек в них. Обе эти проблемы в настоящее время решены для частных случаев (например, для случая малой характеристики p конечного поля $\mathbb{F}_p$).

Наиболее быстрым алгоритмом подсчета точек на эллиптических кривых является алгоритм Шуфа-Элкиса-Аткина [3]. Алгоритм Шуфа был обобщен в [1] до абелевых многообразий. В случае якобианов кривых рода 2 существует специальный алгоритм Годри-Шоста. Алгоритм Шуфа и его обобщения предполагают вычисление характеристического многочлена Фробениуса с помощью китайской теоремы об остатках по известным многочленам действия Фробениуса на подгруппы l-кручения якобиана. Нахождение последних может быть выполнено перебором всевозможных многочленов. В статье будет приведен способ оптимизации такого перебора.

Перечислим основные теоретические результаты, на которые опираются алгоритмы подсчета точек.

Теорема (Тейта-Хонды). *Пусть $\mathcal{A}, \mathcal{B}$ - абелевы многообразия, определенные над полем $\mathbb{F}_q$, их характеристические многочлены Фробениуса равны $\chi_{\mathcal{A}}$ и $\chi_{\mathcal{B}}$ соответственно. Тогда:*

1. $A \sim B \Leftrightarrow \chi_{\mathcal{A}} = \chi_{\mathcal{B}}$;
2. $A \subseteq B \Leftrightarrow \chi_{\mathcal{A}} | \chi_{\mathcal{B}}$.

Пусть $\mathcal{A}$ – абелево многообразие размерности $g = 2$, т.е. абелева поверхность, над конечным полем $k = \mathbb{F}_p$. В этом случае характеристический многочлен Фробениуса $\chi_{\mathcal{A}} \in \mathbb{Z}[T]$ имеет вид [2],[5]:

$$\chi_{\mathcal{A}} = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2, \tag{1}$$

причем согласно теореме Тейта-Хонды, указанный многочлен определяет абелево многообразие с точностью до k-изогении. Обозначим через $Hom_k(\mathcal{A}, \mathcal{B})$, $End_k(\mathcal{A})$ - группу k-гомоморфизмов из $\mathcal{A}$ в $\mathcal{B}$, и кольцо k-эндоморфизмов многообразия $\mathcal{A}$ соответственно. Выберем простое число $l \neq p$ и рассмотрим модуль Тейта [4] $T_l(\mathcal{A})$ многообразия $\mathcal{A}$.

Теорема (Тейта). *Существует изоморфизм $\mathbb{Z}_l$-модулей*

$$Hom_k(\mathcal{A}, \mathcal{B}) \otimes \mathbb{Z}_l \cong Hom_{Gal(\overline{k}/k)}(T_l(\mathcal{A}), T_l(\mathcal{B})). \tag{2}$$

Известно, что $\mathcal{A}[l] \cong (\mathbb{F}_l)^{2g}$. Поэтому эндоморфизм Фробениуса действует как линейный оператор на $\mathbb{F}_l$-векторном пространстве. Сначала рассмотрим матрицы действия Фробениуса $(\chi_{\mathcal{A}})_l$ на модуль Тейта $T_l(\mathcal{A})$. В [2] описана структура таких матриц. Это матрицы $F_l \in GL(4, \mathbb{Z}_l)$, удовлетворяющие следующим свойствам:

1. $F_l^T M_l F_l = p \cdot M_l$;
2. M_l - кососимметричная матрица;
3. $det(M_l)$ - единица в $\mathbb{Z}_l$.

Теперь перейдем от модуля $T_l(\mathcal{A})$ к подгруппе l-кручения $\mathcal{A}[l]$, применяя теорему Тейта. Заметим, что в случае $p \equiv 1 \mod l$ ограничения на матрицу F_l примут вид:

1. $F_l^T M_l F_l = M_l$;
2. M_l - кососимметричная матрица;
3. $det(M_l) = 1$.

Указанные условия означают, что матрица $F_l \in Sp(4, \mathbb{F}_l)$ – симплектическая матрица. При этом действие Фробениуса на подгруппу l-кручения задается тем же многочленом $(\chi_{\mathcal{A}})_l$. Следовательно, он равен характеристическому многочлену матрицы F_l. Таким образом, последовательный перебор коэффициентов в (1) можно свести к перебору характеристических многочленов симплектических матриц $Sp(4, \mathbb{F}_l)$ при малых $l = 2, 3, 5, \ldots$, таких, что $p \equiv 1 \mod l$.

Следует отметить, что для обобщения методов Элкиеса и Аткина для эллиптических кривых на кривые больших родов нам необходимо находить порядки действия Фробениуса ϕ на группу l-кручения. Причем порядок действия r определяется как порядок F_l в $PSp(4, \mathbb{F}_l)$, т.к. в этом случае ϕ^r действует как скалярная матрица. Поэтому мы строим и далее рассматриваем группу проективных симплектических матриц $PSp(4, \mathbb{F}_l)$.

Свойство 1. *Характеристический многочлен матрицы $F_l \in PSp(4, \mathbb{F}_l)$ реверсивен, т.е. имеет вид*

$$\chi(F_l) = T^4 + a_1 T^3 + a_2 T^2 + a_1 T + 1. \tag{3}$$

Свойство 2. *Порядок проективной симплектической группы:*

$$\#PSp(2g, \mathbb{F}_l) = l^{g^2} \cdot \frac{\prod_{i=1}^{g} (l^{2i} - 1)}{НОД(2, l-1)}. \tag{4}$$

Исходя из свойства 1, всего возможно l^2 вариантов характеристических многочленов. Далее мы рассмотрим порядки матриц F_l как элементов группы $PSp(4, \mathbb{F}_l)$. Несмотря

на большое количество делителей порядка (4), возможных порядков в симплектической группе значительно меньше и количество элементов, имеющих тот или иной порядок, распределено неравномерно. Это распределение можно предварительно вычислить. Приведем его для $l = 2, 3, 5, \ldots$.

Табл. 1. Характеристические многочлены матриц $Sp(4, \mathbb{F}_2)$.

Хар. многочлен	Порядки матриц	Количество матриц	Общее количество
$x^4 + 1$	1 2 4	1 75 180	256
$x^4 + x^2 + 1$	3 6	40 120	160
$x^4 + x^3 + x + 1$	3 6	40 120	160
$x^4 + x^3 + x^2 + x + 1$	5	144	144

Табл. 2. Характеристические многочлены матриц $Sp(4, \mathbb{F}_3)$.

Хар. многочлен	Порядки матриц	Количество матриц	Общее количество
$x^4 + 1$	4	6480	6480
$x^4 + x^2 + 1$	2 6	90 7200	7290
$x^4 + 2x^2 + 1$	2 6	540 4320	4860
$x^4 + x^3 + x + 1$	1 3 9	1 800 5760	6561
$x^4 + 2x^3 + 2x + 1$	1 3 9	1 800 5760	6561
$x^4 + x^3 + 2x^2 + x + 1$	4 12	540 4320	4860
$x^4 + 2x^3 + 2x^2 + 2x + 1$	4 12	540 4320	4860
$x^4 + 2x^3 + x^2 + 2x + 1$	5	5184	5184
$x^4 + x^3 + x^2 + x + 1$	5	5184	5184

Заключение. Приведенные в таблицах многочлены соответствуют многочленам действия Фробениуса на подгруппу l-кручения при $p \equiv 1 \bmod l$. Для ускорения работы алгоритма Годри-Шоста необходимо предварительно подобрать такие l, затем осуществлять перебор возможных многочленов $(\chi_A)_l$ в порядке увеличения вероятности их отыскания.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №18-31-00244.

Список литературы

[1] Pila J. *Frobenius maps of abelian varieties and finding roots of unity in finite fields.* // Mathematics of Computation. –1990. –Vol. 55. –№. 192. – P. 745-763.

[2] Rück H.-G., *Abelian surfaces and jacobian varieties over finite fields.* // Compositio Mathematica –1990. – Vol. 76.3. – P. 351–366.

[3] Schoof R. *Counting points on elliptic curves over finite fields.* // J. Theor. Nombres Bordeaux. –1995. –Vol. 7. –№. 1. – P. 219-254.

[4] Tate J., *Endomorphisms of abelian varieties over finite fields.* // Invent. Math. Vol.2 – 1966. – P. 134–144.

[5] Waterhouse W., *Abelian varieties over finite fields.* // Ann. Sci. Ecole Norm. Sup. (4)2 – 1969. – P. 521–560.

Abelian surfaces over a finite field with prescribed Frobenius action on l-torsion subgroup.

N.S. Kolesnikov, S.A. Novoselov

Abstract

In this paper we study abelian surfaces over finite fields with symplectic action of Frobenius on its l-torsion. We obtain some restrictions on the Frobenius polynomial of a general abelian surface by observing specific properties of symplectic matrices. It makes a computation of a Frobenius polynomial faster.

Keywords: Abelian surfaces, Frobenius endomorphism, symplectic matrices, point counting.