Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.772 DOI 10.17223/2226308X/14/1

О ПОСТРОЕНИИ МАКСИМАЛЬНЫХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДА 3

Ю. Ф. Болтнев, С. А. Новоселов, В. А. Осипов

Описываются два метода построения максимальных гиперэллиптических кривых рода три над конечным полем, т. е. кривых, число точек на которых достигает верхнюю границу Хассе — Вейля — Серра. Рассматриваются кривые с уравнением $y^2 = x^7 + ax^4 + bx$, допускающие декомпозицию на эллиптические кривые. В основе первого метода — построение пары суперсингулярных эллиптических кривых над простым полем, j-инвариант одной из которых равен 1728 или 0, а j-инвариант другой кривой также известен. По построенным эллиптическим кривым строится искомая максимальная гиперэллиптическая кривая над подходящим расширением простого поля. Этот метод не исчерпывает всех максимальных кривых, но даёт весьма эффективный алгоритм построения некоторых их семейств. Второй метод основан на факторизации многочленов Лежандра, которые представляют собой инварианты Хассе соответствующих эллиптических кривых в декомпозиции якобиана. Метод позволяет построить все возможные максимальные кривые для случая $b = 1$ и поля $\mathbb{F}_{p^2}$, и мы применяем его для построения всех максимальных кривых для $p \leqslant 7151$ и $a \neq 0$.

Ключевые слова: *максимальная гиперэллиптическая кривая, суперсингулярная эллиптическая кривая, характеристический многочлен.*

Максимальные кривые, т. е. кривые с максимально возможным числом точек, достигающим верхнюю границу Хассе — Вейля — Серра, находят широкое применение как в криптографии, так и в теории алгебраических кодов. Пусть $C : y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3 над конечным полем $\mathbb{F}_q$, $q = p^n$, $p > 3$. В случае, когда b — кубический вычет, якобиан J_C этой кривой допускает декомпозицию на эллиптические кривые, что описывается следующей теоремой, ранее доказанной авторами в [1].

Теорема 1 [1]. Пусть $C : y^2 = x^7 + ax^4 + bx$ — гиперэллиптическая кривая рода 3, определённая над конечным полем $\mathbb{F}_q$, $q = p^n$, $p > 3$, и b — кубический вычет. Тогда:

1) Если $q \equiv 1 \pmod 6$, то $J_C \sim E_1 \times E_2^2$ 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; t_1, t_2 — их следы Фробениуса.
2) Если $q \equiv 5 \pmod 6$, то $J_C \sim E_1 \times E_2 \times \widetilde{E}_2$ 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 $\widetilde{E}_2$ — скручивание кривой E_2.

Для установления соотношения между j-инвариантами эллиптических кривых E_1 и E_2 нами доказана следующая теорема.

Теорема 2. Пусть заданы две эллиптические кривые над полем K:

$$E_1 : y^2 = x^3 + ax^2 + bx, \quad E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a.$$

Тогда справедливы следующие соотношения для их j-инвариантов:

$$j(E_1) = \frac{256(a^2 - 3b)^3}{b^2(a^2 - 4b)}; \quad j(E_2) = -\frac{4 \cdot 1728b}{a^2 - 4b};$$

$$j(E_1) = \frac{j(E_2)}{27}\left(1728\frac{4}{j(E_2)} - 1\right)^3.$$

1. Максимальные кривые в случае $j(E_1) = 0$ или $j(E_1) = 1728$

Следствие 1. Справедливы следующие утверждения:

1) $j(E_1) = 0 \Leftrightarrow j(E_2) = 4 \cdot 1728$;
2) $j(E_1) = 1728 \Leftrightarrow j(E_2) = 1728$ или $j(E_2) = -8 \cdot 1728$.

Замечание 1. Случай $j(E_1) = j(E_2) = 0$ невозможен, так как тогда дискриминант многочлена $x^7 + ax^4 + bx$ обращается в нуль и кривая C будет не гладкой.

Кривая C, заданная над $\mathbb{F}_q$, называется *максимальной кривой*, если число точек на кривой $N = 1 + q + g\lfloor 2\sqrt{q}\rfloor$, то есть достигается верхняя граница Хассе — Вейля — Серра:

$$1 + q - g\lfloor 2\sqrt{q}\rfloor \leqslant N \leqslant 1 + q + g\lfloor 2\sqrt{q}\rfloor.$$

Аналогичная граница известна также для якобианов [2, Theorem 14.15]:

$$(\sqrt{q} - 1)^{2g} \leqslant |J_C| \leqslant (\sqrt{q} + 1)^{2g}.$$

Если C — максимальная кривая, то $|J_C| = (1 + \lfloor 2\sqrt{q}\rfloor + q)^g$. Таким образом, порядок якобиана максимальной гиперэллиптической кривой рода 3 равен

$$|J_C| = (1 + \lfloor 2\sqrt{q}\rfloor + q)^3.$$

Это, в свою очередь, означает, что характеристический многочлен кривой имеет вид

$$\chi_{C,q}(T) = (T^2 + \lfloor 2\sqrt{q}\rfloor T + q)^3.$$

Тогда для гиперэллиптической кривой $C : y^2 = x^7 + ax^4 + bx$ рода 3, определённой над конечным полем $\mathbb{F}_q$, $q = p^n$, $p > 3$, выполняется

$$J_C \sim E_1 \times E_2^2,$$

где $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$ — эллиптические кривые, заданные над $\mathbb{F}_q$. Их характеристические многочлены:

$$\chi_{E_1,q}(T) = \chi_{E_2,q}(T) = T^2 + \lfloor 2\sqrt{q}\rfloor T + q.$$

Заметим, что в случае рассмотрения суперсингулярных эллиптических кривых над простым полем имеем

$$\chi_{E_1,p}(T) = \chi_{E_2,p}(T) = T^2 + p.$$

Согласно методу Вейля [3] для вычисления числа точек эллиптической кривой, число точек кривой E над произвольным расширением $\mathbb{F}_q$, $q = p^r$, равно

$$N_r = p^r + 1 - \alpha^r - \beta^r.$$

Здесь α и β — корни характеристического многочлена, который в случае суперсингулярных над полем $\mathbb{F}_p$ кривых E_1 и E_2 равен $\chi_{E/\,\mathbb{F}_p}(T) = T^2 + p$. Нетрудно видеть, что

$$\alpha^r + \beta^r = (i\sqrt{p})^r + (-i\sqrt{p})^r = \begin{cases} 0, & r \equiv \pm 1 \pmod 4, \\ -2p^{r/2}, & r \equiv 2 \pmod 4, \\ 2p^{r/2}, & r \equiv 0 \pmod 4. \end{cases}$$

Таким образом, имеем

$$N_r = \begin{cases} p^r + 1, & r \equiv \pm 1 \pmod 4, \\ p^r + 1 + 2p^{r/2}, & r \equiv 2 \pmod 4, \\ p^r + 1 - 2p^{r/2}, & r \equiv 0 \pmod 4. \end{cases}$$

Видно, что число точек будет максимально при $r \equiv 2 \pmod 4$, и кривая является максимальной, так как достигается верхняя граница Хассе — Вейля — Серра. Можно заметить, что

$$N_r = p^r + 1 + 2p^{r/2} = 1 + \lfloor 2\sqrt{q} \rfloor + q = \chi_E(1) \;\Rightarrow\; \chi_E(T) = T^2 + \lfloor 2\sqrt{q} \rfloor T + q.$$

Таким образом, для построения максимальной гиперэллиптической кривой нужно построить суперсингулярные эллиптические кривые E_1 и E_2 над простым полем $\mathbb{F}_p$ и рассмотреть их в расширении степени $r \equiv 2 \pmod 4$.

С л у ч а й 1 . Будем искать кривую E_2 в виде $y^2 = x^3 + Ax$. Заметим, что j-инвариант такой кривой $j(E_2) = 1728$. Согласно следствию 1, получаем $j(E_1) = 1728$.

Из [3] известно, что эллиптическая кривая данного вида суперсингулярна над простым полем в случае, когда $p \equiv 3 \pmod 4$. Это равносильно $p \equiv 7, 11 \pmod{12}$ при $p > 3$.

Напомним, что $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$, тогда из сравнения коэффициентов получим $a = 0$, $b = -A^3/27$. Имеем искомое уравнение максимальной гиперэллиптической кривой:

$$C : y^2 = x^7 + ax^4 + bx = x^7 - \frac{A^3}{27}x.$$

Таким образом, перебрав все коэффициенты $A \in \mathbb{F}_p$, построим семейство максимальных гиперэллиптических кривых над расширением $\mathbb{F}_q$, соответствующих эллиптической кривой E_2 вида $y^2 = x^3 + Ax$, где $q = p^r$; $p > 3$; $p \equiv 7, 11 \pmod{12}$; $r \equiv 2 \pmod 4$.

С л у ч а й 2 . Будем искать кривую E_1, такую, что $j(E_1) = 1728$. По следствию из теоремы 2, $j(E_2) = 1728$ или $j(E_2) = -8 \cdot 1728$. Но случай $j(E_1) = j(E_2) = 1728$ мы уже рассмотрели, поэтому теперь рассмотрим случай $j(E_1) = 1728$ и $j(E_2) = -8 \cdot 1728$.

По известному методу (например, [4]) находим уравнение кривой E_2 по заданному j-инварианту:

$$E_2 : y^2 = x^3 - \frac{8}{3}x + \frac{16}{9}.$$

Отсюда $a = 16/9$, $b = (8/9)^3$, и получаем уравнение максимальной гиперэллиптической кривой:

$$C : y^2 = x^7 + ax^4 + bx = x^7 + \frac{16}{9}x^4 + \frac{8^3}{9^3}x.$$

Перебором классов изоморфизма кривых E_2 мы получили, что кривая E_2 суперсингулярна при $p = 31, 131, 251, 383, 439, 1459, 1999, 2203, 2999, 3299, 4523, 4759, 5399, 5471, 8719, 9323, \ldots$ При этом все кривые, изоморфные суперсингулярной кривой E_2, будут тоже суперсингулярны. Их можно получить следующим образом:

$$E_2 : y^2 = x^3 - \frac{8}{3}u^4x + \frac{16}{9}u^6,\ u \in \mathbb{F}_p^*.$$

Сравнивая с уравнением $y^2 = x^3 - 3\sqrt[3]{b}x + a$, получаем коэффициенты

$$a = \frac{16}{9}u^6,\ b = \frac{8^3}{9^3}u^{12}.$$

Имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{16}{9}u^6x^4 + \frac{8^3}{9^3}u^{12}x.$$

Кривая $\widetilde{E}_2$, являющаяся скручиванием кривой E_2, будет суперсингулярной в случае, когда E_2 суперсингулярна. Кроме того, весь класс кривых, изоморфных кривой $\widetilde{E}_2$, состоит из суперсингулярных кривых. Уравнение кривых, полученных скручиванием кривой E_2, выглядит следующим образом:

$$\widetilde{E}_2 : y^2 = x^3 - \frac{8}{3}u^2x + \frac{16}{9}u^3.$$

Сравнивая с уравнением $y^2 = x^3 - 3\sqrt[3]{b}x + a$, получаем коэффициенты

$$a = \frac{16}{9}u^3\ b = \frac{8^3}{9^3}u^6.$$

Тогда имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{16}{9}u^3x^4 + \frac{8^3}{9^3}u^6x.$$

С л у ч а й 3 . Будем искать кривую E_1, такую, что $j(E_1) = 0$. По следствию из теоремы 2 имеем $j(E_2) = 4 \cdot 1728$. Так как $j(E_1) = 0$, кривая E_1 суперсингулярна в случае, когда $p \equiv 2 \pmod 3$, что равносильно $p \equiv 5 \pmod 6$, когда $p > 3$. Аналогично случаю 2, по заданному j-инварианту $j(E_2)$ находим уравнение кривой E_2:

$$E_2 : y^2 = x^3 - 4x + \frac{8}{3}.$$

Отсюда $a = 8/3$, $b = (4/3)^3$, и уравнение максимальной гиперэллиптической кривой принимает следующий вид:

$$C : y^2 = x^7 + \frac{8}{3}x^4 + \frac{4^3}{3^3}x.$$

Перебор классов изоморфизма кривых E_2 показал, что кривая E_2 суперсингулярна при $p = 359, 647, 719, 971, 4391, 6263, 6983, \ldots$ При этом все кривые, изоморфные суперсингулярной кривой E_2, будут тоже суперсингулярны. Их можно получить следующим образом:

$$E_2 : y^2 = x^3 - 4u^4x + \frac{8}{3}u^6,\ u \in \mathbb{F}_p^*.$$

Имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{8}{3}u^6x^4 + \frac{4^3}{3^3}u^{12}x.$$

Кривая $\widetilde{E}_2$, являющаяся скручиванием кривой E_2, будет суперсингулярной в случае, когда E_2 суперсингулярна. Кроме того, весь класс кривых, изоморфных кривой $\widetilde{E}_2$, состоит из суперсингулярных кривых.

Уравнение кривых, полученных скручиванием кривой E_2, выглядит следующим образом:

$$\widetilde{E}_2 : y^2 = x^3 - 4u^2x + \frac{8}{3}u^3.$$

Тогда получаем уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{8}{3}u^3x^4 + \frac{4^3}{3^3}u^6x.$$

Пример 1. Построим семейство максимальных гиперэллиптических кривых рода 3, заданных над полем $\mathbb{F}_{31}$. Они являются максимальными над его расширением степени 2, то есть над полем $\mathbb{F}_{961}$. Для данного поля якобиан максимальной гиперэллиптической кривой должен иметь порядок

$$(\sqrt{q}+1)^{2g} = (\sqrt{961}+1)^6 = (32)^6 = 2^{30} = 1073741824.$$

При этом характеристические многочлены всех кривых над полем $\mathbb{F}_{961}$ имеют вид $\chi_{C,961}(x) = (x+31)^6$, а для этих же кривых, рассматриваемых над полем $\mathbb{F}_{31}$, — $\chi_{C,31}(x) = (x^2+31)^3$. Далее приведены 20 максимальных гиперэллиптических кривых; кривые в левом столбце построены как в случае 1, в правом — как в случае 2:

$y^2 = x^7 + 4x$	$y^2 = x^7 + 14x^4 + 16x$
$y^2 = x^7 + 2x$	$y^2 = x^7 + 3x^4 + 2x$
$y^2 = x^7 + 30x$	$y^2 = x^7 + 19x^4 + x$
$y^2 = x^7 + 27x$	$y^2 = x^7 + 17x^4 + 16x$
$y^2 = x^7 + 15x$	$y^2 = x^7 + 24x^4 + 4x$
$y^2 = x^7 + 29x$	$y^2 = x^7 + 6x^4 + 8x$
$y^2 = x^7 + 8x$	$y^2 = x^7 + 12x^4 + x$
$y^2 = x^7 + 23x$	$y^2 = x^7 + 25x^4 + 8x$
$y^2 = x^7 + x$	$y^2 = x^7 + 28x^4 + 2x$
$y^2 = x^7 + 16x$	$y^2 = x^7 + 7x^4 + 4x$

2. Максимальные кривые вида $y^2 = x^7 + ax^4 + x$ над $\mathbb{F}_{p^2}$

Для группы точек p-кручения якобиана кривой выполняется $J_C[p^s] \simeq \mathbb{Z}/p^{ts}\mathbb{Z}$, где число t, $0 \leqslant t \leqslant 3$, не зависит от s и называется p-рангом кривой [2, с. 61]. Известно, что все максимальные кривые имеют p-ранг 0 [5, Corollary 5]. Поэтому один из способов построить максимальные кривые — найти сначала все кривые p-ранга 0, а затем выбрать среди них максимальные. Проверка на максимальность может быть выполнена за время $\widetilde{\mathcal{O}}(\log^4 q)$ битовых операций с помощью теоремы 1 с использованием алгоритма Схоофа— Элкиса — Аткина для вычисления следов Фробениуса. Для заданной характеристики p все кривые p-ранга 0 вида $y^2 = x^7 + ax^4 + x$ могут быть найдены

с помощью матрицы Картье — Манина кривой, так как её ранг равен p-рангу. Структура матриц Картье — Манина нашей кривой описана в [6]. Для кривой над полем $\mathbb{F}_{p^2}$ матрица Картье — Манина имеет вид

$$\begin{pmatrix} P_{(p-6)/2}(-a/6)^{p+1} & 0 & 0 \\ 0 & P_{(p-1)/2}(-a/2)^{p+1} & 0 \\ 0 & 0 & P_{(p-1)/6}(-a/6)^{p+1} \end{pmatrix}$$

для случая, когда $p \equiv 1 \pmod 3$, и

$$\begin{pmatrix} P_{(p-5)/2}(-a/6)^{p+1} & 0 & 0 \\ 0 & P_{(p-1)/2}(-a/2)^{p+1} & 0 \\ 0 & 0 & P_{(p-5)/6}(-a/6)^{p+1} \end{pmatrix}$$

для случая, когда $p \equiv 2 \pmod 3$. Здесь $P_m(x)$ — многочлен Лежандра степени m. Поэтому p-ранг кривой $y^2 = x^7 + ax^4 + x$ равен 0 тогда и только тогда, когда $-a/2$ является корнем многочлена $L_1(-a/2) = \gcd\left(P_{(p-1)/2}, P_{(p-1)/6}\right)$ для $p \equiv 1 \pmod 3$ или $L_2(-a/2) = \gcd\left(P_{(p-1)/2}, P_{(p-5)/6}\right)$ для $p \equiv 2 \pmod 3$. Таким образом, для фиксированного p мы можем найти все кривые p-ранга 0 с помощью факторизации многочленов L_1, L_2 либо доказать, что таких кривых не существует (L_1 или L_2 в этом случае — константы).

Сложность метода. Построить многочлен Лежандра $P_m(x)$ можно по известным рекуррентным формулам за время $\mathcal{O}\Big(\sum\limits_{i=1}^{m} i\Big) = \mathcal{O}(m(m+1))$ операций в поле. Нахождение наибольшего общего делителя для многочленов степени не больше $(p-1)/2$ занимает время $\widetilde{\mathcal{O}}((p-1)/2)$ операций в поле [7, с. 325]. Факторизация многочленов L_1 и L_2 может быть выполнена [7, с. 390] за время $\widetilde{\mathcal{O}}(\lfloor p/6 \rfloor^2 \log p)$ операций в поле, учитывая, что $\deg L_1 \leqslant (p-1)/6$ и $\deg L_2 \leqslant (p-5)/6$. Проверка на максимальность занимает время $\widetilde{\mathcal{O}}(\log^4 q)$. Предполагая, что количество проверяемых кривых небольшое, получаем в итоге эвристическую сложность в $\widetilde{\mathcal{O}}(p^2 \log^2 p)$ битовых операций. При этом нахождение всех максимальных кривых простым перебором коэффициентов занимает время $\widetilde{\mathcal{O}}(p^2 \log^4 p)$.

Используя полученный метод, мы построили все максимальные кривые над полем $\mathbb{F}_{p^2}$ с параметром $a \neq 0$ (случай $a = 0$ изучен в [8, § 4]) для $p \leqslant 7151$ и определили поля, над которыми таких кривых не существует. Данные по количеству максимальных кривых для $p < 200$ представлены в таблице. Полные данные с явными уравнениями максимальных кривых можно найти на домашней странице второго автора[1].

Число максимальных кривых вида $y^2 = x^7 + ax^4 + x$ над $\mathbb{F}_{p^2}$,
$3 < p < 200$, $a \neq 0$

p	Кол-во
5–29, 37–43, 53, 61, 67, 73, 89–101, 107–127, 137–163, 173–181, 193, 197	0
31, 47, 59, 79, 83	2
71, 103, 131, 167	4
191, 199	6

[1] `http://crypto-kantiana.com/semyon.novoselov/genus3/maximal_curves`

ЛИТЕРАТУРА

1. *Novoselov S. A. and Boltnev Y. F.* Characteristic polynomials of the curve $y^2 = x^{2g+1} + ax^{g+1} + bx$ over finite fields // Прикладная дискретная математика. Приложение. 2019. № 12. С. 44–46.
2. *Cohen H. and Frey G.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2006.
3. *Blake I. F., Seroussi G., and Smart N. P.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
4. *Menezes A.* Elliptic curve public key cryptosystem. Kluwer Academic Publ., 1993.
5. *Tafazolian S.* A family of maximal hyperelliptic curves // J. Pure Appl. Algebra. 2012. V. 216. No. 7. P. 1528–1532.
6. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20–31.
7. *Von zur Gathen J. and Gerhard J.* Modern Computer Algebra. Cambridge University Press, 2013.
8. *Kodama T., Top J., and Washio T.* Maximal hyperelliptic curves of genus three // Finite Fields Their Appl. 2009. V. 15. No. 3. P. 392–403.

УДК 519.214 DOI 10.17223/2226308X/14/2

ЦЕНТРАЛЬНАЯ ПРЕДЕЛЬНАЯ ТЕОРЕМА ДЛЯ U-СТАТИСТИК ОТ ЦЕПОЧЕК МЕТОК ВЕРШИН НА ПОЛНОМ ГРАФЕ

Н. М. Меженная, В. Г. Михайлов

В полном графе с вершинами $1, 2, \ldots, n$ вершины $2, 3, \ldots, n$ снабжены независимыми случайными метками, принимающими значения из конечного множества $\mathcal{A}_N$. Рассматривается совокупность всех цепей по s смежных рёбер, каждая из которых выходит из вершины 1 и не проходит через одну и ту же вершину дважды. Каждой цепи соответствует s-цепочка из случайных меток пройденных вершин. Рассматривается U-статистика $U_k(s)$ с ядром, зависящим от k таких s-цепочек. Число $k \geqslant 2$ считается фиксированным, а $s \geqslant 1$ может меняться. Установлено, что достаточным условием асимптотической нормальности $U_k(s)$ (при обычной стандартизации) является условие вида $\mathbf{D}U_k(s) \geqslant Cn^{2(ks-1)+\varkappa}$, где $C, \varkappa > 0$.

Ключевые слова: *U-статистика, центральная предельная теорема, полный граф, цепочка, случайные метки.*

Исследование свойств выборочных характеристик и статистических критериев привело к необходимости изучения распределений функционалов от последовательностей случайных величин $X_1, \ldots, X_n$ вида

$$U_n = U_n(X_1, \ldots, X_n) = \sum_{1 \leqslant j_1 < \ldots < j_r \leqslant n} f(X_{j_1}, \ldots, X_{j_r}), \tag{1}$$

называемых *U-статистиками* [1]. Число r называется *порядком* U-статистики. Функционалы вида (1) широко используются для проверки свойств случайных последовательностей, качества датчиков псевдослучайных чисел, наличия или отсутствия зависимости между членами последовательности, наличия образцов или повторений специального вида и в задачах, связанных с защитой информации.

Основные результаты об асимптотическом поведении распределений U-статистик с непрерывными ядрами можно найти в [2]. Результаты для U-статистик от дискрет-