

Секция 1

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ
ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ**

УДК 511

**ОПТИМАЛЬНЫЕ КРИВЫЕ РОДА 3 НАД КОНЕЧНЫМ ПОЛЕМ
С ДИСКРИМИНАНТОМ -19**

Е. С. Алексеенко, С. И. Алешников, А. И. Зайцев

Пусть E — эллиптическая кривая, определенная над конечным полем $\mathbb{F}_q$ с дискриминантом $d(\mathbb{F}_q) = [2\sqrt{q}]^2 - 4q = -19$.

Если число рациональных точек кривой равно $q + 1 \pm g[2\sqrt{q}]$, то кривая называется максимальной (соответственно минимальной) кривой. Будем называть такие кривые оптимальными над $\mathbb{F}_q$.

Теория Хонда — Тэйта [1] показывает, что для максимальной (минимальной) кривой C имеет место изогения $\text{Jas}(C) \sim E^g$, где E — максимальная (минимальная) эллиптическая кривая над конечным полем $\mathbb{F}_q$. Класс изогении эллиптической кривой E определяется с помощью характеристического многочлена эндоморфизма Фробениуса кривой E .

Пусть $\text{Jas}(C)$ — главное поляризованное якобиево многообразие кривой C с тэта-дивизором θ . По теореме Торелли [2] кривая C полностью определена посредством $(\text{Jas}(C), \theta)$ с точностью до изоморфизма над алгебраическим замыканием поля $\mathbb{F}_q$. Рассмотрим эрмитов модуль $(\mathcal{O}_K^g; h)$, где $\mathcal{O}_K^g$ является $\mathcal{O}_K$ -модулем, и $h : \mathcal{O}_K^g \times \mathcal{O}_K^g \rightarrow \mathcal{O}_K$ — эрмитова форма. Эквивалентность категорий определяется посредством функтора $F : \text{Jas}(C) \rightarrow \text{Hom}(E, \text{Jas}(C))$ и обратного к нему $V : \mathcal{O}_K^g \rightarrow \mathcal{O}_K^g \otimes_{\mathcal{O}_K} E$. Относительно этой эквивалентности главная поляризация якобиана $\text{Jas}(C)$ соответствует неприводимой эрмитовой $\mathcal{O}_K$ -форме h . Таким образом, мы можем использовать классификацию унимодулярных неприводимых эрмитовых форм для изучения изоморфных классов $\text{Jas}(C)$.

Получение оптимальных (максимальных) алгебраических кривых над конечным полем является важной проблемой в дискретной математике, решение которой имеет многочисленные приложения в криптографии и теории кодирования. На таких кривых можно строить алгебро-геометрические коды большой длины, и трудность разрешения проблемы дискретного логарифма в якобиане такой кривой гарантирует криптостойкость соответствующей криптосистемы. В работе представлены максимальные и минимальные оптимальные кривые рода 3 над конечным полем с дискриминантом -19 мощности до 997.

Теорема 1.

1. Над полем $\mathbb{F}_q$ не может одновременно существовать максимальной и минимальной оптимальной кривых.
2. Если C — оптимальная кривая рода 3 над конечным полем $\mathbb{F}_q$ с дискриминантом -19 , то C не является гиперэллиптической.

Теорема 2. Оптимальная кривая C задается следующими уравнениями:

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + (\beta_0 + \beta_1 x)y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + (\beta_0 + \beta_1 x)y, \\ y^2 = x^3 + ax + b, \end{cases}$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, a, b$ — коэффициенты из $\mathbb{F}_q$. Эллиптическая кривая E задана уравнением $y^2 = x^3 + ax + b$.

ЛИТЕРАТУРА

1. *Waterhouse W. C.* Abelian varieties over finite fields // Ann. Sci. Ecole Norm. Sup. 1969. No. 2. P. 521–560.
2. *Andreotti A.* On a Theorem of Torelli // American J. of Math. V. 80. 1958. No. 4. P. 801–828.

УДК 512.6

НЕКОТОРЫЕ СВОЙСТВА ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ В ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ И ПОЛЯХ КОНЕЧНОЙ ХАРАКТЕРИСТИКИ

А. М. Гришин

Дискретное преобразование Фурье — это один из видов ортонормированного преобразования векторов [1, 2]. Для конечной последовательности элементов $\{s_0, s_1, \dots, s_{N-1}\}$ дискретное преобразование Фурье (ДПФ) заключается в поиске другой последовательности $\{S_0, S_1, \dots, S_{N-1}\}$, элементы которой вычисляются по формуле (прямое преобразование)

$$S_k = \sum_{n=0}^{N-1} s_n \cdot W_N^{kn}; \quad k = \overline{0, N-1}, \quad (1)$$

где W_N — примитивный корень степени N из единицы [1, 3]. В предположении, что элемент $N^{-1} = 1/N$ существует, для обратного преобразования можно записать выражение

$$s_n = \frac{1}{N} \sum_{k=0}^{N-1} S_k \cdot W_N^{-kn}; \quad n = \overline{0, N-1}. \quad (2)$$

Считается, что вектор $s = (s_0, s_1, \dots, s_{N-1})$ является представлением данных во временной области, а вектор $S = (S_0, S_1, \dots, S_{N-1})$ — в частотной (спектральной).

Векторы s и S можно задать с помощью соответствующих многочленов $s(X)$ и $S(X)$

$$s(X) = s_0 + s_1 X + \dots + s_{N-1} X^{N-1}; \quad (3)$$

$$S(X) = S_0 + S_1 X + \dots + S_{N-1} X^{N-1}. \quad (4)$$

Если конечная последовательность

$$\{s_n = s[nT] = s(t), \quad n = \overline{0, N-1}; \quad t = nT\} \quad (5)$$