АЛГОРИТМ ПОСТРОЕНИЯ ЭНДОМОРФИЗМОВ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Нестеренко А.Ю. (Москва)
nesterenko_a_y@mail.ru

В различных приложениях используются вычисления на эллиптических кривых с известным кольцом эндоморфизмов. При этом, явное задание эндоморфизма позволяет уменьшить трудоемкость операции вычисления кратной точки эллиптической кривой [1].

Пусть $d < 0$ свободное от квадратов целое число, $\tau \in \mathbb{Z}[\sqrt{d}]$ такое, что $\operatorname{Im} \tau > 0$, и $j(z)$ — модулярная функция.

В докладе излагается новый алгоритм, позволяющий по заданному кольцу целых алгебраических чисел $\mathbb{Z}[\sqrt{d}]$ построить эллиптическую кривую

$$\mathcal{E}: \quad y^2 = 4x^3 - g_2 x - g_3,$$

где $g_2, g_3 \in \mathbb{Q}(j(\tau))$ и $g_2^3 - 27g_3^2 \neq 0$. Более того, мы строим эндоморфизм

$$\tau(x, y) \to \left(f(x), \frac{y}{\tau} f'(x)\right), \quad f(x) = \frac{P(x)}{Q(x)},$$

где $P(x), Q(x) \in \mathbb{Q}(\tau, j(\tau))[x]$ и $\deg P(x) = N(\tau)$, $\deg Q(x) = N(\tau) - 1$.

Выбирая подходящее простое число $p > 3$, мы получаем представление $p = \mathfrak{P}_1 \cdots \mathfrak{P}_{2h}$, где $\mathfrak{P}_i$ простой идеал в $\mathbb{Q}(\tau, j(\tau))$. Проводя редукцию построенных коэффициентов кривой g_2, g_3 и многочленов $P(x)$, $Q(x)$ по модулю $\mathfrak{P}_i$ для некоторого $i \in \overline{1, 2h}$, мы получаем кривую и эндоморфизм, определенные над конечным простым полем $\mathbb{F}_p$.

В качестве иллюстрации предложенного метода, приведем пример. Для $d = -5$, $\tau = \sqrt{-5}$ и $p = 3268853741$ мы построили эллиптическую кривую

$$E(\mathbb{F}_p): y^2 = 4x^3 - 1699718456x - 2745808646 \pmod{3268853741}$$

с эндоморфизмом τ, для которого

$$P(x) = 653770748(2887070511 + x) \times$$
$$\times \left(880882706 + 347136513x + x^2\right)\left(3050687895 + 2347406494x + x^2\right),$$
$$Q(x) = (2866433945 + x)^2(3193226555 + x)^2.$$

Список литературы

[1] *Galant R., Lambert R., Vanstone S.* Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms // Proceedings of the 21st

Annual International Cryptology Conference CRYPTO-01. — 2001. — pp. 190-200.

[2] Seminar on Complex Multiplication // A. Borel, S. Chowla, C.S. Herz, K. Iwasawa, J.P.Serre. — Springer. — 1966. — 105 p.