Кафедра компьютерной безопасности

07 июня 2023 г.

Вычисление кратной точки с использованием комплексных ~~обедов~~ эндоморфизмов

CTCRYPT 2023 (#trumpsession)

Алексей Нестеренко

anesterenko@hse.ru
https://www.hse.ru/org/persons/47634770

Представление натуральных чисел

в комплексной системе счисления

$$
\begin{aligned}
\alpha &= \tfrac{1}{2}(1+\sqrt{-7}),\\
N(\alpha) &= 2,\\
\\
1 &= 1,\\
2 &= -\alpha^2+\alpha,\\
3 &= -\alpha^2+\alpha+1,\\
4 &= \alpha^5+\alpha^2,\\
5 &= \alpha^5+\alpha^2+1,\\
6 &= \alpha^5+\alpha,\\
7 &= \alpha^5+\alpha+1,\\
8 &= \alpha^5-\alpha^3,\\
9 &= \alpha^5-\alpha^3+1,\\
10 &= \alpha^5-\alpha^3-\alpha^2+\alpha,\\
11 &= \alpha^5-\alpha^3-\alpha^2+\alpha+1,\\
12 &= -\alpha^7+\alpha^6+\alpha^5-\alpha^4+\alpha^3+\alpha^2,
\end{aligned}
$$

Теорема. Пусть $d > 1$ – свободное от квадратов, целое число и задан элемент $\alpha \in \Lambda_\tau \subseteq \mathbb{Z}_{\mathbb{K}} \subset \mathbb{Q}(\sqrt{-d})$ такой, что $N(\alpha) \geq 2$. Определим натуральное число $n_\alpha = \frac{N(\alpha)-\delta_\alpha}{2}$, где $\delta_\alpha \equiv N(\alpha) \pmod 2$, и множество $\mathcal{N} = [-n_\alpha, -n_\alpha+1, \ldots, n_\alpha-1, n_\alpha]$. Тогда, если α удовлетворяет неравенству $|\mathtt{tr}(\alpha)-1| \leq n_\alpha$, то для любого натурального k найдется многочлен $g(z) \in \mathcal{N}[z]$ такой, что

$$k = g(\alpha) = \sum_{i=0}^{w+c_1} x_i\alpha^i, \quad x_i \in \mathcal{N},$$

где $\deg g(z) \leq w + c_1$, где $w = \left\lceil 2\log_{N(\alpha)} k \right\rceil$ и

$$c_1 = \begin{cases} 4, & \text{если} \quad \alpha = 1 \pm \sqrt{-2},\\ 3, & \text{иначе.} \end{cases}$$

Вычисление кратной точки

Эллиптическая кривая:

$$v^2 = u^3 - \frac{3}{32}(\alpha - 6)u^2 - \frac{1}{64}(3\alpha - 2)u,$$

и эндоморфизм

$$\phi_\alpha : (u, v) \to \left(-\frac{(\alpha+1)u^2 + u - \mu}{4u},\ -\frac{(\alpha+1)u^2 + \mu}{4\alpha u^2} v, \right),$$

где $\alpha = \frac{1}{2}(1 + \sqrt{-7})$ и $\mu = \frac{\alpha - 2}{16} = \left(\frac{\alpha}{4}\right)^2 = \frac{1}{4(\alpha+1)}$.
Пример:

$$[10]P = \phi_\alpha(\phi_\alpha(\phi_\alpha(\phi_\alpha(\phi_\alpha(P)) - P) - P) + P)$$

Сложение + комплексное умножение