A. Yu. Nesterenko, Constructions of elliptic curves endomorphisms, *Mat. Vopr. Kriptogr.*, 2014, Volume 5, Issue 2, 99–102

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2014, Т. 5, № 2, С. 99–102

УДК 519.772+512.624

Constructions of elliptic curves endomorphisms

A. Yu. Nesterenko

National Research University Higher School of Economics, Moscow

Received 25.09.2013

Let $\mathbb{K}$ be an imaginary quadratic field. Consider an elliptic curve $E(\mathbb{F}_p)$ defined over prime field $\mathbb{F}_p$ with given ring of endomorphisms $o_{\mathbb{K}}$, where $o_{\mathbb{K}}$ is an order in a ring of integers $\mathbb{Z}_{\mathbb{K}}$.

An algorithm permitting to construct endomorphism of the curve $E(\mathbb{F}_p)$ corresponding to the complex number $\tau \in o_{\mathbb{K}}$ is presented. The endomorphism is represented as a pair of rational functions with coefficients in $\mathbb{F}_p$. To construct these functions we use continued fraction expansion for values of Weierstrass function. After that we reduce the rational functions modulo prime ideal in finite extension of $\mathbb{K}$. One can use such endomorphism for elliptic curve point exponentiation.

Keywords: elliptic curve, continued fraction expansion, reduction modulo prime ideal, point exponentiation.

Построение эндоморфизмов алгебраических кривых

А. Ю. Нестеренко

Национальный исследовательский институт Высшая школа экономики, Москва

Резюме. Пусть $\mathbb{K}$ — мнимое квадратичное поле. Рассмотрим эллиптическую кривую $E(\mathbb{F}_p)$, определенную над простым полем $\mathbb{F}_p$ с заданным кольцом эндоморфизмов $o_{\mathbb{K}}$, где $o_{\mathbb{K}}$ — порядок кольца целых $\mathbb{Z}_{\mathbb{K}}$.

Предложен алгоритм построения эндоморфизма кривой $E(\mathbb{F}_p)$, соответствующего комплексному числу $\tau \in o_{\mathbb{K}}$. Эндоморфизм представляется парой рациональных функций с коэффициентами из $\mathbb{F}_p$. Для построения функций используются разложения значений функции Вейерштрасса в цепные дроби и приведение рациональных функций по модулю простого идеала в конечном расширении $\mathbb{K}$. Такие эндоморфизмы можно использовать для экспоненцирования точек на эллиптической кривой.

Ключевые слова: эллиптические кривые, разложения в цепные дроби, приведение по модулю простого идеала, экспоненцирование точки.

Let $d < 0$ be a square free integer, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. It's well known, see [1, ch.2, §7], that numbers $\{1, \tau\}$, where

$$\tau = \begin{cases} \sqrt{d}, & \text{if} \quad d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{if} \quad d \equiv 1 \pmod 4. \end{cases}$$

form a basis of the ring of integers $\mathbb{Z}_{\mathbb{K}}$.

Let $p > 3$ be a prime and

$$E(\mathbb{F}_p): \quad y^2 \equiv x^3 + Ax + B \pmod p, \quad A, B \in \mathbb{F}_p,$$

be an elliptic curve defined over the field $\mathbb{F}_p$. We assume that the ring of endomorphisms of this curve is isomorphic to the ring of integers $\mathbb{Z}_{\mathbb{K}}$. In this article we describe an algorithm permitting to construct the endomorphism of the curve $E(\mathbb{F}_p)$ corresponding to the complex number τ. We consider an endomorphism corresponding τ, see [2, § 14.B], as a pair of rational functions over $\mathbb{F}_p$, i.e.

$$\tau : E(\mathbb{F}_p) \to E(\mathbb{F}_p), \quad (x, y) \to (\varphi(x), y\psi(x)),$$

where $\varphi(x), \psi(x) \in \mathbb{F}_p(x)$.

Some special cases are known, see [3]. Our method allows to construct similar endomorphism for arbitrary imaginary quadratic field. Next, we describe the basic steps of the algorithm.

1. For given τ we calculate the value of the modular function $j(\tau)$, define the field $\mathbb{L} = \mathbb{Q}(\sqrt{d}, j(\tau))$ and the prime ideal $\mathfrak{p}$ over p containing $j(\tau) - j$, where j is the invariant of the curve $E(\mathbb{F}_p)$.

2. We construct numbers $g_2, g_3 \in \mathbb{L}$ such that the invariant of the curve $y^2 = 4x^3 - g_2x - g_3$ is equal to $j(\tau)$, i.e. $j(\tau) = 1728\dfrac{g_2^3}{g_2^3 - 27g_3^2}$.

3. Then we calculate coefficients c_k of the Weierstrass elliptic function expansion

$$\wp(z) = \wp(z, g_2, g_3) = \frac{1}{z^2} + \sum_{i=1}^{\infty} c_i z^{2(i-1)}$$

and evaluate the rational function $\varphi_\tau(x)$ such that

$$\wp(\tau z) = \varphi_\tau(\wp(z)) = \frac{f(\wp(z))}{g(\wp(z))}$$

for some polynomials $f(x), g(x) \in \mathbb{L}[x]$ and $\deg f(x) = N(\tau)$, $\deg g(x) = N(\tau) - 1$.

4. By differentiation of the expression for $\wp(\tau z)$ we find

$$\tau\wp'(\tau z) = \wp'(z) \cdot \frac{f'(\wp(z))g(\wp(z)) - f(\wp(z))g'(\wp(z))}{g(\wp(z))^2}.$$

Next define the second rational function

$$\psi_\tau(x) = \frac{f'(x)g(x) - f(x)g'(x)}{\tau g(x)^2}.$$

Since $\wp(\tau z)$ satisfies the differential equation for Weierstrass function and $\wp(z)$ is transcendental, we derive

$$(y\psi_\tau(x))^2 = 4\varphi_\tau(x)^3 - g_2\varphi_\tau(x) - g_3.$$

5. In conclusion we reduce the rational functions φ_τ, ψ_τ modulo $\mathfrak{p}$, i.e. define

$$\varphi \equiv \varphi_\tau \pmod{\mathfrak{p}}, \quad \psi \equiv \psi_\tau \pmod{\mathfrak{p}}.$$

To demonstrate correctness of our method we present an example. Let $d = -5$ and $p = 3268853741$. Then elliptic curve

$$E(\mathbb{F}_p) : y^2 = x^3 + 2843924127x + 947974709 \pmod{3268853741}$$

has an endomorphism associated with $\tau = \sqrt{-5}$, which is represented as

$$\tau : \quad (x, y) \to \Big(\varphi(x), y\psi(x)\Big),$$

where

$$\varphi(x) \equiv 653770748\,(2887070511 + x)\times \\ \times \frac{(880882706 + 347136513x + x^2)\,(3050687895 + 2347406494x + x^2)}{\zeta^2(x)} \pmod{p},$$

$$\psi(x) \equiv 2492690311\,(319523693 + x)\times \\ \frac{(446480654 + x)(647067904 + x)(2275216235 + x)(2321505934 + x)(2362625857 + x)}{\zeta^3(x)} \\ \pmod{p},$$

and $\zeta(x) = (2866433945 + x)(3193226555 + x)$. It's easy to check that these rational functions represent an endomorphism, see [4]. Let

$$P_1 = (1789807873, 336773927), \quad P_2 = (2701258086, 1160593737)$$

are two randomly chosen points on curve $E(\mathbb{F}_p)$. Then

$$\tau(P_1 + P_2) = \tau(P_1) + \tau(P_2) = (3122761229, 457809648).$$

In cryptography applications we can use above-mentioned endomorpisms to accelerate a group operation. Let P be a point of order q on elliptic curve $E(\mathbb{F}_p)$. We define cyclic subgroup G generated by P and suppose[1] $\tau(P) \in G$. Then there exists an integer t satisfying

$$\tau(P) = [t]P = \underbrace{P + \cdots + P}_{t \text{ times}}$$

and t is a root of minimal polynomial of τ modulo q.

Let k be an integer, $0 < k < q$. Then k may be represented as $k = k_0 + k_1 t$, where $0 \leq k_0, k_1 < \sqrt{q}$. For calculating a sum $[k]P$ we can use the equality

$$[k]P = k_0 P + k_1 \tau(P).$$

More detailed information about elliptic curve point exponentiation may be found in [3].

References

[1] *Borevich Z.I., Shafarevich I.R.* Number Theory. — Academic Press, 1966. — 436 pp.

[2] *Cox D.* Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication. — J.Wiley and Sons, 1989. — 363 pp.

[3] *Galant R., Lambert R., Vanstone S.* Faster point multiplication on elliptic curves with efficient endomorphisms // CRYPTO 01. Lect. Notes Comput. Sci. — 2001. — V. 2139. — P. 190–200.

[4] `http://axelkenzo.ru/downloads/endocheck.nb`

[1] Generally, τ can map a points of elliptic curve $E(\mathbb{F}_p)$ between various subgroups of $E(\mathbb{F}_p)$.