Constructions Of Elliptic Curves Endomorphisms

Alex Yu. Nesterenko*

June 26, 2013

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

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

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 will describe an algorithm of constructing the endomorphism of the curve $E(\mathbb{F}_p)$, corresponding to the complex number τ. We consider the 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 were known before, see [3]. Our method allows to construct similar endomorphism for arbitrary imaginary quadratic field. Next, we describe the basic steps of the algorithm.

*National Research University Higher School Of Economics.

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 $\mathfrak{p}$ that is lying over p and contains $j(\tau) - j$, 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 $y^2 = 4x^3 - g_2 x - g_3$ 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 series for Weierstrass elliptic function
$$\wp(z) = \wp(z, g_2, g_3) = \frac{1}{z^2} + \sum_{i=1}^{\infty} c_i z^{2(i-1)},$$
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 derive
$$\tau\wp'(\tau z) = \wp'(z) \cdot \frac{f'(\wp(z))g(\wp(z)) - f(\wp(z))g'(\wp(z))}{g(\wp(z))^2}.$$
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

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

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

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 random 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 endomorpisms mentioned below for accelerating a group operation. Let P be a point of order q on elliptic curve $E(\mathbb{F}_p)$. We define G cyclic subgroup generated by P and suppose[1] $\tau(P) \in G$. Then exists an integer t satisfying

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

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

We can find t as a root of characteristic polynomial of τ modulo q, i.e.

$$\begin{cases} x^2 - d \equiv 0 \pmod{q}, & \text{when} \quad d \equiv 2, 3 \pmod{4}, \\ x^2 - x + \frac{1-d}{4} \equiv 0 \pmod{q}, & \text{when} \quad d \equiv 1 \pmod{4}. \end{cases}$$

Let k be an integer, $0 < k < q$. For calculating a sum $[k]P$ we can represent $k = k_0 + k_1 t + \cdots + k_{n-1} t^{n-1}$, where $0 \leq k_0, k_1, \ldots, k_{n-1} < \sqrt[n]{q}$ and n is a minimal integer such $q < t^n$. Now we can calculate $[k]P$ as follows.

1. Let $R = P$ and calculate $Q = k_0 R$.
2. For $i = 1$ to $n - 1$ calculate $R = \tau(R)$ and $Q = Q + k_i R$.

After all we find that $Q = [k]P$.

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.Wiles and Sons. — 1989. — 363 p.

[3] *Galant R., Lambert R., Vanstone S.* Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms // CRYPTO 01 — Proceedings of the 21st Annual International Conference on Advances Of Cryptology. — 2001. — pp. 190-200.

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