The discrete logarithm problem on elliptic curves defined over $\mathbb{Q}$

Masaya Yasuda *

Extended Abstract

The discrete logarithm problem on elliptic curves defined over a field K is: given an E be an elliptic curve over K, a point $S \in E(K)$, and a point $T \in \langle S \rangle$, find the integer $d \in \mathbb{Z}$ such that $T = [d]S$. In the case where $K = \mathbb{F}_q$ is a finite field with q elements, there are a number of ways of approaching the solution to this problem (see [1]). On the other hand, the solution to this problem in the case where $K = \mathbb{Q}$ is the field of rational numbers is not well known. The purpose of this study is to give an algorithm for the discrete logarithm problem on elliptic curves defined over $\mathbb{Q}$. Let E be an elliptic curve over $\mathbb{Q}$. Fix a point $S \in E(\mathbb{Q})$. Assume that the order of S is of infinite. The subset $\{[d]S \mid d \in \mathbb{Z}_{\geq 0}\}$ of the group $\langle S \rangle$ is denoted by $\langle S \rangle_+$. Given a point $T \in \langle S \rangle_+$. Our main idea to find the positive integer d such that $T = [d]S$ is based on the method solving the discrete logarithm problem for an anomalous elliptic curve over a prime field (see [2]).

Let p be a prime number where E has good reduction. Denote $\widetilde{E}$ the reduction of E modulo p and let $\pi : E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$ be the reduction map (see [3]). For $n \geq 1$, define a subgroup of $E(\mathbb{Q}_p)$ by

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid v(x(P)) \leq -2n\} \cup \{O\},$$

where v is the normalized p-adic valuation. We have the exact sequence of abelian groups

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \xrightarrow{\pi} \widetilde{E}(\mathbb{F}_p) \to 0$$

(see [3]). The group $E_1(\mathbb{Q}_p)$ is isomorphic to the group of $p\mathbb{Z}_p$-valued points of the one-parameter formal group $\mathcal{E}$ associated to E (see [3]). For $n \geq 1$, the subgroup $E_n(\mathbb{Q}_p)$ of $E_1(\mathbb{Q}_p)$ corresponds to the subgroup $\mathcal{E}(p^n\mathbb{Z}_p)$ of $\mathcal{E}(p\mathbb{Z}_p)$ under the isomorphism $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$. Moreover, for $n \geq 1$ there is the isomorphisms of groups

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \simeq \mathcal{E}(p^n\mathbb{Z}_p)/\mathcal{E}(p^{n+1}\mathbb{Z}_p) \simeq p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \tag{1}$$

(see [3]). Let N be the order of the group $\widetilde{E}(\mathbb{F}_p)$. Let h_p be a composition of the following maps

$$h_p : E(\mathbb{Q}) \xrightarrow{\iota} E(\mathbb{Q}_p) \xrightarrow{[N]} E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p), \tag{2}$$

where ι is the inclusion map and $[N]$ is multiplication by N. For a point $Q \in E(\mathbb{Q})$, we can compute $h_p(Q) \in \mathcal{E}(p\mathbb{Z}_p)$ as follows:

$$h_p(Q) = -\frac{x}{y} \quad (\text{where } [N]Q = (x, y) \in E_1(\mathbb{Q}_p)).$$

Combining the map (2) with the isomorphisms (1), we give the following algorithm for finding the positive integer d such that $T = [d]S$:

*FUJITSU LABORATORIES LTD. 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki myasuda@labs.fujitsu.com

Input: E : elliptic curve over $\mathbb{Q}$, S : rational point of E of infinite order, $T \in \langle S \rangle_+$. Output: $d \in \mathbb{Z}_{\geq 0}$ s.t. $T = [d]S$.

1. $a \leftarrow 0$.
2. While $a = 0$ do:
    2.1. Choose a prime p at which E has good reduction.
    2.2. Compute the order of $\widetilde{E}(\mathbb{F}_p)$ and $N \leftarrow \sharp\widetilde{E}(\mathbb{F}_p)$.
    2.3. Compute $[N]S = (x, y)$ and $z \leftarrow -x/y$.
    2.4. $a \leftarrow z/p \pmod p$.
3. $n \leftarrow 0$ and $\ell \leftarrow 1$.
4. While $T \neq 0$ do:
    4.1. Compute $[N]T = (x, y)$ and $w \leftarrow -x/y$.
    4.2. $b \leftarrow w/p^\ell$.
    4.3. $\bar{d_n} \leftarrow b/a \pmod p$ and $d_n \leftarrow \mathrm{lift}(\bar{d_n})$.
    4.4. $T \leftarrow T - [d_n]S$ and $S \leftarrow [p]S$.
    4.5. $n \leftarrow n + 1$ and $\ell \leftarrow \ell + 1$.
5. $d \leftarrow d_0 + d_1 p + d_2 p^2 + \cdots + d_{n-1} p^{n-1}$.
6. Return(d).

For example, let E be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

$$E : y^2 + y = x^3 - x.$$

The Mordell-Weil group $E(\mathbb{Q})$ has rank 1 and a point $S = (0, 0)$ is a generator for $E(\mathbb{Q})$. Moreover, the elliptic curve E has good reduction outside 37. Let $T = [d]S = (x(T), y(T)) \in \langle S \rangle_+$ be as follows:

$$x(T) = -\frac{31489296812857 40316}{2846153597907293521}, \quad y(T) = -\frac{2181616293371330311419201915}{4801616835579099275862827431}.$$

The above algorithm is dependent on the choice of the prime p where E has good reduction. At first, set $p = 3$. Then the above algorithm gives $d_0 = 2,\ d_1 = 0,\ d_2 = 0,\ d_3 = 1$ and

$$d = 2 + 0 \cdot p + 0 \cdot p^2 + 1 \cdot p^3 = 29.$$

Secondly, set $p = 5$. Then the above algorithm gives $d_0 = 4,\ d_1 = 0,\ d_2 = 1$ and

$$d = 4 + 0 \cdot p + 1 \cdot p = 29.$$

This shows that for each p, the above algorithm gives the p-adic expansion of d.

The result is as follows:

Theorem. *For each p, the above algorithm gives the p-adic expansion of d.*

References

[1] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, Cambridge University Press (1999).

[2] T. Satoh and K. Araki, “Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves,” Comm. Math. Univ Sancti Pauli **47** (1998)Cpp.81-92.

[3] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math. Springer-Verlag, Berlin-Heidelberg-New York (1986).