The discrete logarithm problem on elliptic curves defined over Q

Masaya Yasuda

FUJITSU LABORATORIES LTD.

myasuda@labs.fujitsu.com

1. Introduction

THE purpose of this study is to give an algorithm for the discrete logarithm problem on elliptic curves defined over Q.

THE discrete logarithm problem on elliptic curves defined over a field K is:

Definition 1 *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 such that $T = [d]S$.*

In the case where K 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 is the field of rational numbers is not well known.

2. Main Idea

LET E be an elliptic curve over Q. Fix a point $S \in E(Q)$. Assume that the order of S is of infinite. The subset $\{[d]S \mid d \geq 0\}$ 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]).

2.1 Mathematical Foundations

FIX a prime number p at which E has good reduction. Denote $\widetilde{E}$ the reduction of E modulo p and let N be the order of the group $\widetilde{E}(\mathbb{F}_p)$. For finding the positive integer d such that $T = [d]S$, we use the following maps:

$$h_p : E(\mathbb{Q}) \xrightarrow{\iota} E(\mathbb{Q}_p) \xrightarrow{[N]} E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p),$$
$$\mathcal{E}(p^n\mathbb{Z}_p)/\mathcal{E}(p^{n+1}\mathbb{Z}_p) \simeq \mathbb{Z}/p\mathbb{Z} \quad (n \geq 1)$$

where $\mathcal{E}$ is the formal group associated to E (see [3]).

3. Main Theorem

Theorem 1 *For each p, the following algorithm gives the p-adic expansion of the integer d such that $T = [d]S$.*

4. Algorithm

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. $d \leftarrow d_0 + d_1p + d_2p^2 + \cdots + d_{n-1}p^{n-1}$.
6. Return(d).

5. The discrete logarithm problem on elliptic curves defined over a finite field

LET p be a prime. Our method is also applicable for solving the discrete logarithm problem on ellipitc curves defined over a p-adic field Q_p. If we could reduce the discrete logarithm problem on elliptic curves defined over a prime field with p elements to the discrete logarithm problem on elliptic curves defined over Q or Q_p, we can solve the discrete logarithm problem on elliptic curves defined over a prime field with p elements using our method.

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), pp.81-92.

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