COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 47, No. 1 1998

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves

by

Takakazu SATOH and Kiyomichi ARAKI

(Received January 9, 1998)

1. Introduction

Let p be a prime and $\boldsymbol{F}_p$ the finite field with p elements. An elliptic curve over $\boldsymbol{F}_p$ is said to be anomalous if the number of $\boldsymbol{F}_p$ rational point is exactly p. In this paper, we give an $O((\log p)^3)$ algorithm for discrete logarithm problem for an anomalous elliptic curve over a prime field. Our method may be considered as an elliptic curve version of Fermat quotient. For an integer a prime to p, the Fermat quotient $L_p(a)$ is defined to be $\frac{a^{p-1}-1}{p} \bmod p \in \boldsymbol{F}_p$. If integers a, b are prime to p, then $L_p(ab)=L_p(a)+L_p(b)$ in $\boldsymbol{F}_p$. Since L_p is *not* well defined as a function over $\boldsymbol{F}_p$, we cannot solve discrete logarithm over $\boldsymbol{F}_p^\times$ (note also ${}^\sharp\boldsymbol{F}_p^\times = p-1$ is prime to $\mathrm{char}(\boldsymbol{F}_p)=p$). However, it is not so strange to expect its elliptic curve analogue is applicable to discrete log problem for an anomalous elliptic curves. We do this actually. In Sect. 2, we make a review on the Fermat quotient which illustrates our idea and historical background. We also discuss its relation to the discrete log problem on $(\boldsymbol{Z}/p^r\boldsymbol{Z})^\times$ with $p \geq 3$ and $r \geq 2$. This is not new, but does not seem to be stated explicitly. Let $\tilde{E}$ be an anomalous curve over $\boldsymbol{F}_p$ and E its lifting to $\boldsymbol{Z}$. In Sect. 3, we construct an $\boldsymbol{F}_p$-valued group homomorphism λ_E on the group $\tilde{E}(\boldsymbol{F}_p)$ of $\boldsymbol{F}_p$ rational points of $\tilde{E}$ for $p \geq 7$. Let $\alpha \in \tilde{E}(\boldsymbol{F}_p) - \{\mathcal{O}\}$. Roughly speaking, we obtain $\lambda_E(\alpha)$ by viewing $pu(\alpha)$ in the formal group of E, where u is any lifting $\tilde{E}(\boldsymbol{F}_p) \to E(\boldsymbol{Q}_p)$. Corollary 3.6 describes the detailed algorithm to compute λ_E. Our algorithm uses only arithmetic operations in $\boldsymbol{Z}/p^2\boldsymbol{Z}$ and $\boldsymbol{F}_p$. This makes implementation and running time analysis simple. Then we study how to choose E so that λ_E is non-zero. Summing up, we can solve the discrete log problem of $\tilde{E}$. We discuss the cryptographic implication of our result in Sect. 4.

After the works on the discrete log problem for anomalous elliptic curves over prime fields were completed, the authors were informed that Dr. N. Smart has independently obtained same results [21] at the similar time.

The result of this paper was announced at the symposium on "algebraic number

1991 Mathematics Subject Classification code: Primary 11G07, Secondary 94A60, 11T71. Key words and phrases: Discrete logarithm, anomalous elliptic curve, Fermat quotient. Both authors are partially supported by the Telecommunications Advancement Foundation, Grant 96-01068.

theory and its related topics" held at RIMS, Kyoto University on Oct. 27–31, 1997. Later (precisely, on Nov. 3, 1997), the authors learned that Semaev [17] obtained (in 1995) an polynomial time discrete log algorithm of p-torsion points of an elliptic curves over $\boldsymbol{F}_p$ and that Rück [16] generalized it for curves of arbitrary genus. However, the method of Semaev and Rück which is algebraic geometric is quite different to ours and that of Smart. For the comparison of these two algorithms, see Voloch [22].

ACKNOWLEDGMENT. The first author appreciates Prof. Yasutaka Ihara at RIMS, Kyoto University for his suggestion.

Notation

Rings are always assumed to be commutative and unitary. Let R be a ring. We denote the unit group (the set of invertible elements) by $R^\times$. For a prime p, the finite field with p elements is denoted by $\boldsymbol{F}_p$. For $a \in \boldsymbol{Q}$, we put

$$\operatorname{ord}_p a := \begin{cases} r & \left(a = p^r \frac{v}{u},\ u, v \in \boldsymbol{Z} - p\boldsymbol{Z}\right), \\ \infty & (a = 0). \end{cases}$$

We denote the p-adic number field and the ring of p-adic integers by $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p$, respectively. By definition, $\boldsymbol{Q}_p$ is the completion of $\boldsymbol{Q}$ with respect to the metric induced from ord_p. The function ord_p uniquely extends to a continuous function $\boldsymbol{Q}_p \to \boldsymbol{Z} \cup \{\infty\}$. The following formulas are well known.

$$\operatorname{ord}_p(xy) = \operatorname{ord}_p x + \operatorname{ord}_p y \qquad (x, y \in \boldsymbol{Q}_p)$$

$$\operatorname{ord}_p(x+y) \geq \min(\operatorname{ord}_p x, \operatorname{ord}_p y)$$

$$\operatorname{ord}_p(x+y) = \min(\operatorname{ord}_p x, \operatorname{ord}_p y) \quad \text{for } \operatorname{ord}_p x \neq \operatorname{ord}_p y$$

$$\boldsymbol{Z}_p = \{x \in \boldsymbol{Q}_p : \operatorname{ord}_p x \geq 0\}$$

$$\boldsymbol{Z}_p^\times = \{x \in \boldsymbol{Q}_p : \operatorname{ord}_p x = 0\}$$

For introductory explanation of p-adic numbers, see e.g. Cassels [2], Serre [18].

2. Fermat quotient

Let p be a prime. In 1828, Abel [1] proposed the following problem: Can a number $a^{p-1} - 1$ be divisible by p^2, where p is a prime and a is an integer, $1 \leq a < p$? Note we always have $n^{p-1} - 1 \equiv 0 \bmod p$ for $n \in \boldsymbol{Z} - p\boldsymbol{Z}$ due to the Fermat's little theorem. Dickson [3, p. 105] states that G. Eisenstein noted the following formulas in 1850:

$$\begin{cases} L_p(ab) = L_p(a) + L_p(b) \\ L_p(a + pc) = L_p(a) - ca^{-1} \end{cases} \tag{2.1}$$

for $a, b \in \boldsymbol{Z}-p\boldsymbol{Z}$, $c \in \boldsymbol{Z}$ where

$$L_p(a) := \frac{a^{p-1}-1}{p} \bmod p \in \boldsymbol{F}_p \tag{2.2}$$

and a^{-1} is the inverse of a in $\boldsymbol{F}_p$. We call L_p the *Fermat quotient.* Lerch [9, (27)] noticed generalization of the Fermat quotient to a composite modulus $m \in \boldsymbol{N}$. For a, $m \in \boldsymbol{Z}$ with $\gcd(a, m)=1$, put $L_m(a) := \frac{a^{\varphi(m)}-1}{m} \bmod m \in \boldsymbol{Z}/m\boldsymbol{Z}$. Then,

$$\begin{cases} L_m(ab) = L_m(a) + L_m(b) \\ L_m(a+mc) = L_m(a) + \varphi(m) c a^{-1} \end{cases} \tag{2.3}$$

where $\gcd(a, m) = \gcd(b, m) = 1$ and $c \in \boldsymbol{Z}$. For more details, see Dickson [3, Chap. 4]. Concerning Abel's original problem, Jacobi [7] observed $a^{p-1} \equiv 1 \bmod p^2$ has only four solutions $(a, p) = (3, 11), (9, 11), (14, 29), (18, 37)$ for $p \leq 37$. As far as the authors know, it is open whether there are infinitely many primes satisfying $a^{p-1} \equiv 1 \bmod p^2$ for a fixed a. Ihara [5] considers this problem from modern number theoretic point of view. Ribenboim [15, Chap. 5.III] states that Crandall, Dilcher and Pomerance verified only $p = 1093$ and 3511 satisfy $2^{p-1} \equiv 1 \bmod p^2$ for $p < 4 \times 10^{12}$.

The phenomena concerning (2.2) may be paraphrased as follows: Let G be a finite group of order n consisting of $\bmod p$ objects. For $g \in G$, consider g^n in $\bmod p^2$ (via some "lifting"), which should be p-adically "close" to the identity of G. The difference between them may involve interesting information on n. We do this for an anomalous elliptic curve defined over $\boldsymbol{F}_p$ in the next section.

In order to observe relation between Fermat quotient and discrete logarithm, let us consider the discrete log problem $\bmod p^r$ for $p \geq 3$ and $r \geq 2$. Let $\omega \in \boldsymbol{Z}$ be a primitive element of $\boldsymbol{Z}/p^2\boldsymbol{Z}$. Then, as is well known, ω is a primitive element of $\boldsymbol{Z}/p^r\boldsymbol{Z}$ for all $r \geq 1$. For $\alpha \in (\boldsymbol{Z}/p^r\boldsymbol{Z})^\times$, we want $n \in \boldsymbol{Z}/p^{r-1}(p-1)\boldsymbol{Z}$ satisfying

$$\alpha \equiv \omega^n \bmod p^r . \tag{2.4}$$

For $a \in \boldsymbol{Z}-p\boldsymbol{Z}$, note $L_{p^r}(a+p^r) = L_{p^r}(a) - p^{r-1}a^{-1}$ by (2.3). Hence L_{p^r} induces a well defined map $(\boldsymbol{Z}/p^r\boldsymbol{Z})^\times \to \boldsymbol{Z}/p^{r-1}\boldsymbol{Z}$, which is again denoted by L_{p^r}. By (2.3), $L_{p^r}(\alpha) \equiv n L_{p^r}(\omega) \bmod p^{r-1}$. On the other hand, $\omega^{p-1} \equiv 1 + pL_p(\omega) \bmod p^2$. Then $\omega^{p-1} \not\equiv 1 \bmod p^2$ implies $L_p(\omega) \in \boldsymbol{F}_p^\times$, while $\omega^{(p-1)p^{r-1}} \equiv (1+pL_p(\omega))^{p^{r-1}} \bmod p^{r+1}$. Since $p \geq 3$, we see $\omega^{(p-1)p^{r-1}} \equiv 1 + p^r L_p(\omega) \bmod p^{r+1}$ (cf. Ireland and Rosen [6, Chap. 4, Sect. 1, Lemma 3 and Corollary 1]). Therefore, $L_{p^r}(\omega) \equiv L_p(\omega) \bmod p$, i.e., $L_{p^r}(\omega) \in (\boldsymbol{Z}/p^r\boldsymbol{Z})^\times$. Consequently, we obtain

$$n \equiv \frac{L_{p^r}(\alpha)}{L_{p^r}(\omega)} \bmod p^{r-1} . \tag{2.5}$$

On the other hand, $\bmod p$ of (2.4) yields $\alpha \equiv \omega^n \bmod p$. Any discrete log algorithm for $\boldsymbol{F}_p$ gives $k \in \boldsymbol{Z}/(p-1)\boldsymbol{Z}$ such that

$$n \equiv k \bmod p-1 . \tag{2.6}$$

Using Chinese remainder theorem, we obtain n from (2.5) and (2.6). Let $T(p)$ be a time complexity for discrete logarithm in $\boldsymbol{F}_p$. The time complexity of above method is $O(T(p)+(\log p^r)^2 \log r)$, which runs faster than Pohlig-Hellman algorithm [14]. We note that we only need $a^{p^r-p^{r-1}} \bmod p^{2r-1}$ to compute $L_{p^r}(a) \bmod p^{r-1}$.

3. Discrete log problems on anomalous elliptic curves

Let p be a prime. Let

$$\tilde{E}: y^2+\tilde{a}_1xy+\tilde{a}_3y=x^3+\tilde{a}_2x^2+\tilde{a}_4x+\tilde{a}_6$$

be an elliptic curve defined over $\boldsymbol{F}_p$. We say $\tilde{E}$ is *anomalous* if $^{\sharp}\tilde{E}(\boldsymbol{F}_p)$ (including the point at infinity) is exactly p. Mazur [10] studied such curves in extensively sophisticated setting. Let E be an lifting of $\tilde{E}$ to $\boldsymbol{Z}$. In other words, choose $a_i \in \boldsymbol{Z}$ satisfying $a_i \bmod p = \tilde{a}_i$ for $i=1 \sim 4$, 6 and define E by

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 .$$

We denote the reduction map $E(\boldsymbol{Q}_p) \to \tilde{E}(\boldsymbol{F}_p)$ by π. The identity element of an elliptic curve with respect to its group structure is denoted by $\mathcal{O}$. For any $\boldsymbol{Z}$-algebra R, we put

$$E(R) := \{(x:y:1) \in \boldsymbol{P}^2(R): y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\} \cup \{(0:1:0)\} .$$

We note $E(R)$ is *not* necessarily a group if R is not a field. We identify $(X: Y: 1) \in \boldsymbol{P}^2(R)$ with $(X, Y) \in \boldsymbol{A}^2(R)$. By abuse of notation, we write $(0:1:0)$ as $\mathcal{O}$. Let $\mathscr{E}$ be the Formal group associated to E. (See Silverman [20, Chap. 4] for its definition and its basic properties.) We have a following isomorphism $\mathscr{L}$:

$$\mathscr{L}: \operatorname{Ker} \pi \xrightarrow{\psi} \mathscr{E}(p\boldsymbol{Z}_p) \xrightarrow{\log_{\mathscr{E}}} p\boldsymbol{Z}_p \tag{3.1}$$

where $\psi(x:y:z)=x/y$ and

$$\begin{aligned} \log_{\mathscr{E}}(t) := t &- \frac{a_1}{2}t^2+\frac{a_1^2+a_2}{3}t^3-\frac{a_1^3+2a_1a_2+a_3}{4}t^4 \\ &+\frac{a_1^4+3a_1^2a_2+6a_1a_3+a_2^2+2a_4}{5}t^5-\cdots \end{aligned} \tag{3.2}$$

is a formal logarithm of $\mathscr{E}$. In what follows, we always assume $\tilde{E}$ is anomalous.

LEMMA 3.1. $pE(\boldsymbol{Q}_p) \subset \operatorname{Ker} \pi$.

Proof. Let $A \in E(\boldsymbol{Q}_p)$. Since π is a group homomorphism by Silverman [20, Chap. 7, proof of Prop. 2.1], anomality of $\tilde{E}$ implies $\pi(pA)=p\pi(A)=\mathcal{O}$. □

THEOREM 3.2. *Let u be any lifting from $\tilde{E}(\boldsymbol{F}_p)$ to $E(\boldsymbol{Q}_p)$, i.e. $\pi \circ u = \mathrm{id}_{\tilde{E}(\boldsymbol{F}_p)}$. Let λ_E be a composition of the following maps*

$$\lambda_E\colon \tilde{E}(\boldsymbol{F}_p) \xrightarrow{u} E(\boldsymbol{Q}_p) \xrightarrow{h_p} \operatorname{Ker}\pi \xrightarrow{\mathscr{L}} p\boldsymbol{Z}_p \xrightarrow{\bmod p^2} p\boldsymbol{Z}_p/p^2\boldsymbol{Z}_p \cong \boldsymbol{F}_p\,. \tag{3.3}$$

Here h_p is multiplication by p. Then λ_E is a group homomorphism which is independent of choice of u. Moreover, λ_E is either a zero map or an isomorphism.

Proof. Let $\alpha, \beta \in \tilde{E}(\boldsymbol{F}_p)$ and put $\Delta := u(\alpha)+u(\beta)-u(\alpha+\beta)$. Since π is a group homomorphism and u is a lifting, we see $\pi(\Delta)=\mathcal{O}$, i.e. $\Delta \in \operatorname{Ker}\pi$. By (3.1) there is $t_0 \in \boldsymbol{Z}_p$ satisfying $\mathscr{L}(\Delta)=pt_0$. Therefore $\mathscr{L}(h_p(\Delta))=p^2t_0 \in p^2\boldsymbol{Z}_p$. We consequently have $F(\Delta)=0$, where $F := (\bmod p^2)\circ\mathscr{L}\circ h_p$. Since F is a homomorphism, $F(u(\alpha))+F(u(\beta))=F(u(\alpha+\beta))$, i.e., λ_E is a homomorphism. Let v be an another lifting $\tilde{E}(\boldsymbol{F}_p)\to E(\boldsymbol{Q}_p)$. Then $\pi(u(\alpha)-v(\alpha))=\pi(u(\alpha))-\pi(v(\alpha))=\mathcal{O}$ for any $\alpha \in \tilde{E}(\boldsymbol{F}_p)$. Hence we have $u(\alpha)-v(\alpha) \in \operatorname{Ker}\pi$. By the same argument as above we see that $F(u(\alpha))=F(v(\alpha))$ and that λ_E is independent of choice of u. To show the last statement, simply note $\tilde{E}(\boldsymbol{F}_p)$ has no nontrivial proper subgroup. Therefore either $\operatorname{Ker}\lambda_E$ is $\tilde{E}(\boldsymbol{F}_p)$, which implies λ_E is a zero map, or $\operatorname{Ker}\lambda_E$ is trivial, which implies λ_E is injective. In the latter case, λ_E is also surjective since $\#\tilde{E}(\boldsymbol{F}_p)=p=\#\boldsymbol{F}_p$. Hence λ_E is an isomorphism. □

REMARK 3.3. Although λ_E is independent of choice of u, it depends on the choice of E. Cf. Theorem 3.7.

COROLLARY 3.4. *Let $\tilde{E}$ be an anomalous elliptic curve defined over $\boldsymbol{F}_p$ and E its lifting to $\boldsymbol{Z}$. Then, the following conditions on E are equivalent:*

(i) *The map λ_E is a zero map.*

(ii) *There exists $\alpha \in \tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$ satisfying $\lambda_E(\alpha)=0$.*

(iii) *There exists a p-torsion point belonging to $E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$.*

Proof. The implication (i)→(ii) is trivial. (ii)→(i): Let $\lambda_E(\alpha)=0$ with $\alpha \in \tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$ and let $\beta \in \tilde{E}(\boldsymbol{F}_p)$ be arbitrary. Since $\tilde{E}(\boldsymbol{F}_p)$ is a cyclic group of order p, α is its generator. Hence there exists $n \in \boldsymbol{N}$ satisfying $\beta=n\alpha$. Therefore $\lambda_E(\beta)=n\lambda_E(\alpha)=0$.

(ii)→(iii): Let $\alpha \in \tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$ with $\lambda_E(\alpha)=0$. Then there is $t_1 \in \boldsymbol{Z}_p$ satisfying $\mathscr{L}(pu(\alpha))=p^2t_1$. Put $B := \mathscr{L}^{-1}(pt_1) \in \operatorname{Ker}\pi$. Since $\mathscr{L}$ is an isomorphism, $pB=pu(\alpha)$. Letting $A := u(\alpha)-B$, we see A is a p-torsion point belonging to $E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$.

(iii)→(ii): Assume $A \in E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$ and $pA=\mathcal{O}$. Put $\alpha := \pi(A)$. Then

$$\lambda_E(\alpha)=((\bmod p^2)\circ\mathscr{L})(pA)=\mathcal{O}\,.$$

On the other hand, $\alpha \neq \mathcal{O}$ by $A \in E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$. □

In what follows let $p \geq 5$ for simplicity. Then without loss of generality, we may assume $\tilde{a}_1=\tilde{a}_2=\tilde{a}_3=0$ (in $\boldsymbol{F}_p$) and $a_1=a_2=a_3=0$ (in $\boldsymbol{Z}$).

THEOREM 3.5. *Let $p \geq 5$ be a prime. Let $\alpha \in \tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$. Assume $A := (x_1, y_1) \in E(\boldsymbol{Z}_p)$ satisfies $\pi(A)=\alpha$. For those $n \in \boldsymbol{N}$ such that $nA \neq \mathcal{O}$, put $(x_n, y_n) := nA$. If λ_E is a non-zero map, we have the following:*

(i) *$nA \in E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$ for $1 \leq n < p$,*

(ii) $x_n \not\equiv x_m \bmod p$ *for* $1 \leq n < m < p$ *with* $n+m \neq p$,

(iii) $y_{p-1} - y_1 \in \boldsymbol{Z}_p^\times$, $\dfrac{x_{p-1}-x_1}{p} \in \boldsymbol{Z}_p^\times$ *and* $\lambda_E(\alpha) = \dfrac{x_{p-1}-x_1}{p(y_{p-1}-y_1)} \bmod p$.

Proof. (i) First of all, we note $nA \neq \mathcal{O}$ for $1 \leq n < p$. Indeed, $nA = \mathcal{O}$ implies $n\alpha = \pi(nA) = \mathcal{O}$. Since $\tilde{E}$ is anomalous, we obtain $\alpha = \mathcal{O}$, which is a contradiction. So we have only to prove $nA \in E(\boldsymbol{Z}_p)$. For $n=1$, this is a part of assumptions. For $n=2$, we note

$$y_1 \not\equiv 0 \bmod p\,. \tag{3.4}$$

Otherwise, we obtain $2\alpha = 2\pi(A) = 2(x_1 \bmod p, 0) = \mathcal{O}$, which contradicts to $\alpha \neq \mathcal{O}$ since $\tilde{E}$ is anomalous. Therefore, we have $y_1 \in \boldsymbol{Z}_p^\times$. Addition formula of E yields

$$x_2 = c_2^2 - 2x_1\,, \qquad y_2 = -c_2 x_2 - d_2\,,$$

where

$$c_2 = \frac{3x_1^2 + a_4}{2y_1}\,, \qquad d_2 = \frac{-x_1^3 + a_4 x_1 + 2a_6}{2y_1}\,.$$

Since $y_1 \in \boldsymbol{Z}_p^\times$, we see $x_2, y_2 \in \boldsymbol{Z}_p$ and (i) holds for $n=2$. For $3 \leq n < p$, we use induction on n. Suppose $A, (n-1)A \in E(\boldsymbol{Z}_p) - \{\mathcal{O}\}$. Especially,

$$\pi(A) = (x_1 \bmod p,\ y_1 \bmod p)$$

$$\pi((n-1)A) = (x_{n-1} \bmod p,\ y_{n-1} \bmod p)\,.$$

Assuming $x_1 \equiv x_{n-1} \bmod p$, we obtain $\pi(A) = \pm\pi((n-1)A)$, i.e., $n\alpha = \mathcal{O}$ or $(n-2)\alpha = \mathcal{O}$. By the anomality of $\tilde{E}$, we have $\alpha = \mathcal{O}$, which is again a contradiction. Therefore we obtain $x_1 \not\equiv x_{n-1} \bmod p$ and, a fortiori, $x_1 \neq x_{n-1}$. Then,

$$x_n = c_n^2 - x_1 - x_{n-1}\,, \qquad y_n = -c_n^3 + c_n(x_1 + x_{n-1}) - d_n\,, \tag{3.5}$$

where

$$c_n = \frac{y_{n-1} - y_1}{x_{n-1} - x_1}\,, \qquad d_n = \frac{y_1 x_{n-1} - y_{n-1} x_1}{x_{n-1} - x_1}\,. \tag{3.6}$$

By $x_{n-1} \not\equiv x_1 \bmod p$, we see $x_{n-1} - x_1 \in \boldsymbol{Z}_p^\times$ and hence $c_n, d_n \in \boldsymbol{Z}_p$. Therefore $x_n, y_n \in \boldsymbol{Z}_p$.

The proof of (ii) is similar. Assume $x_n \equiv x_m \bmod p$. Then $\pi(nA) = \pm\pi(mA)$, i.e., $(m \pm n)\alpha = \mathcal{O}$, which yields a contradiction as in (i).

(iii): Since $\lambda_E \neq 0$, we see $pA \neq \mathcal{O}$ (cf. Corollary 3.4). Note (3.5) and (3.6) hold for $n=p$. Let $(x_p, y_p) := pA$. Then $\pi((x_p : y_p : 1)) = \mathcal{O} = (0:1:0)$ implies $\mathrm{ord}_p y_p < 0$ and $\mathrm{ord}_p x_p > \mathrm{ord}_p y_p$. By (ii), we have $A, (p-1)A \in E(\boldsymbol{Z}_p)$. Let $s := \mathrm{ord}_p c_p$. Assume $s \geq 0$, i.e. $c_p \in \boldsymbol{Z}_p$. Using

$$d_p = y_1 - x_1 c_p\,, \tag{3.7}$$

we have $d_p \in \boldsymbol{Z}_p$, and hence $y_p \in \boldsymbol{Z}_p$, a contradiction. So, s must be negative. Then,

by (3.5), we see

$$\mathrm{ord}_p x_p = 2s . \tag{3.8}$$

By (3.7), we also obtain

$$\begin{aligned}\mathrm{ord}_p d_p &\geq \min(\mathrm{ord}_p y_1, \mathrm{ord}_p x_1 + \mathrm{ord}_p c_p)\\ &\geq \mathrm{ord}_p c_p = s .\end{aligned}$$

Moreover $\mathrm{ord}_p(c_p(x_1+x_{p-1}))\geq s$, while $\mathrm{ord}_p c_p^3 = 3s < s$. Hence

$$\mathrm{ord}_p y_p = 3s . \tag{3.9}$$

Therefore, $\mathrm{ord}_p \psi(pA) = \mathrm{ord}_p(x_p/y_p) = -s > 0$. Using (3.2), we see $\mathrm{ord}_p \mathscr{L}(pA) = -s$. By assumption $\lambda_E(A)\neq 0$. So $\mathrm{ord}_p \mathscr{L}(pA) = 1$. Summing up, we obtain $s=-1$, $\frac{x_p}{py_p}\in \boldsymbol{Z}_p^{\times}$ and $\lambda_E(A) = \frac{x_p}{py_p} \bmod p$. By the anomality of $\tilde{E}$, we see $\pi((p-1)A) = -\pi(A)$ and hence $y_{p-1}\equiv -y_1 \bmod p$. Therefore, $y_{p-1}-y_1 \equiv -2y_1 \not\equiv 0 \bmod p$. So, we have proved $y_{p-1}-y_1 \in \boldsymbol{Z}_p^{\times}$. Since $\mathrm{ord}_p c_p = -1$, we obtain

$$\frac{x_{p-1}-x_1}{p} \in \boldsymbol{Z}_p^{\times} . \tag{3.10}$$

Let $\hat{x} := p^2 x_p$ and $\hat{y} := p^3 y_p$. By $s=-1$, (3.8) and (3.9), we see $\hat{x}, \hat{y} \in \boldsymbol{Z}_p^{\times}$. Hence $\lambda_E(A) = \frac{\hat{x}}{\hat{y}} \bmod p = \frac{\hat{x} \bmod p}{\hat{y} \bmod p}$. Note $pc_p \in \boldsymbol{Z}_p^{\times}$ since $s=-1$. Therefore,

$$\begin{aligned}\hat{x} \bmod p &= (p^2 c_p^2 - p^2(x_1+x_{p-1})) \bmod p\\ &= (pc_p)^2 \bmod p\end{aligned}$$

and

$$\begin{aligned}\hat{y} \bmod p &= -p^3 c_p^3 + (pc_p)p^2(x_1+x_{p-1}) - p^3 d_p \bmod p\\ &= -(pc_p)^3 \bmod p .\end{aligned}$$

Consequently,

$$\lambda_E(\alpha) = \frac{(pc_p)^2 \bmod p}{-(pc_p)^3 \bmod p} = \left(-\frac{1}{p}\,\frac{x_{p-1}-x_1}{y_{p-1}-y_1}\right) \bmod p . \tag{3.11}$$

This completes the proof. □

COROLLARY 3.6. *Let $p\geq 5$. Let*

$$\tilde{E}\colon y^2 = x^3 + \tilde{a}_4 x + \tilde{a}_6$$

be an anomalous elliptic curve defined over $\boldsymbol{F}_p$. Choose integers a_4, a_6 satisfying $a_4 \bmod p = \tilde{a}_4$ and $a_6 \bmod p = \tilde{a}_6$. Define an elliptic curve E by

$$E\colon y^2 = x^3 + a_4 x + a_6 .$$

Let λ_E be a homomorphism defined by (3.3). *Then, the following procedure computes $\lambda_E(\alpha)$ for $\alpha:=(s,t)\in\tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$ with $O((\log p)^3)$ time complexity.*

(i) *Find $A:=(X_1, Y_1)\in E(\boldsymbol{Z}/p^2\boldsymbol{Z})$ satisfying $X_1 \bmod p=s$ and $Y_1 \bmod p=t$.*

(ii) *Compute $(X_{p-1}, Y_{p-1}):=(p-1)A\in E(\boldsymbol{Z}/p^2\boldsymbol{Z})$ by using elliptic curve addition.*

(iii) *If $X_{p-1}\neq X_1$, then*

$$\lambda_E(\alpha)=\left(\frac{X_{p-1}-X_1}{p} \bmod p\right)((Y_{p-1}-Y_1) \bmod p)^{-1}.$$

Otherwise $\lambda_E(\alpha)=0$.

Proof. Note, under the same notation as in Theorem 3.5, we have only to compute $y_{p-1}-y_1 \bmod p$ and $\frac{1}{p}(x_{p-1}-x_1) \bmod p$. For (i), simply take any X_1, $y\in\boldsymbol{Z}/p^2\boldsymbol{Z}$ satisfying $X_1 \bmod p=s$ and $y \bmod p=t$. Then solve the following equation on w:

$$(y+pw)^2=X_1^3+a_4X_1+a_6 \bmod p^2,$$

$$\text{i.e.}\quad 2tw=\frac{X_1^3+a_4X_1+a_6-y^2}{p} \bmod p.$$

Note the right hand side is well defined. By (3.4), we obtain $w\in\boldsymbol{F}_p$. Then put $Y_1:=y+pw$. See Serre [18, Chap. 2, §2.2]. Then Theorem 3.5 (ii) guarantees computation of $(p-1)A \bmod p^2$ involves only operations over $\boldsymbol{Z}/p^2\boldsymbol{Z}$. By (3.10), we see $X_{p-1}\neq X_1$ under the condition $\lambda_E\neq 0$. In this case Theorem 3.5 (iii) ensures validity of Step (iii). Otherwise λ_E must be a zero map. So, $\lambda_E(\alpha)=0$.

The number of arithmetic operations over $\boldsymbol{Z}/p^2\boldsymbol{Z}$ involved in steps (i) and (iii) are indifferent to p or $\tilde{E}$. Step (ii) requires at most $2\log_2 p$ elliptic curve addition. Summing up, $O((\log p)^3)$ is enough to compute $\lambda_E(\alpha)$. □

THEOREM 3.7. *Let E and $\tilde{E}$ be as in Corollary* 3.6, *$A:=(x_1, y_1)\in E(\boldsymbol{Z}_p)-\{\mathcal{O}\}$. Assume*

$$3x_1^2\not\equiv -a_4 \bmod p. \tag{3.12}$$

Define an elliptic curve E' by

$$E': y^2=x^3+a_4'x+a_6',$$

where $a_4':=a_4+p$ and $a_6':=a_6-px_1$. (Note $A\in E'(\boldsymbol{Z}_p)$.) Let $(x_{p-1}, y_{p-1}):=(p-1)A$ in E and $(x'_{p-1}, y'_{p-1}):=(p-1)A$ in E'. Then, we have the following:

(i) *Either $x_{p-1}\not\equiv x'_{p-1} \bmod p^2$ or $y_{p-1}\not\equiv y'_{p-1} \bmod p^2$.*

(ii) *Either λ_E or $\lambda_{E'}$ is non-zero.*

Proof. (i): Assume $x_{p-1}\equiv x'_{p-1} \bmod p^2$ and $y_{p-1}\equiv y'_{p-1} \bmod p^2$. For $1\leq n\leq p-1$, let $(x_n, y_n):=nA$ in E and $(x'_n, y'_n):=nA$ in E'. Writing elliptic curve addition

formula for $(n-1)A=nA+(-A)$ in E explicitly, we have

$$x_{n-1}=\hat{c}_n^2-x_1-x_n, \qquad y_{n-1}=-\hat{c}_n^3+\hat{c}_n(x_1+x_n)-\hat{d}_n$$

where

$$\hat{c}_n=\frac{y_n+y_1}{x_n-x_1}, \qquad \hat{d}_n=-\frac{y_1x_n+y_nx_1}{x_n-x_1}$$

for $n\geq 3$. The similar formulas hold for (x'_{n-1}, y'_{n-1}). But these formulas do not contain coefficients of the Weierstrass equation. By Theorem 3.5 (ii), $x_n\equiv x'_n \bmod p^2$ and $y_n\equiv y'_n \bmod p^2$ implies $x_{n-1}\equiv x'_{n-1} \bmod p^2$ and $y_{n-1}\equiv y'_{n-1} \bmod p^2$. On the other hand, the duplication formula on E and E' yield

$$\begin{aligned} x'_2-x_2&=\left(\frac{3x_1^2+a'_4}{2y_1}\right)^2-2x_1-\left(\left(\frac{3x_1^2+a_4}{2y_1}\right)^2-2x_1\right)\\ &=p\frac{6x_1^2+2a_4+p}{4y_1^2}\\ &\not\equiv 0 \bmod p^2 \end{aligned}$$

by (3.12), which is a contradiction.

(ii): Assume both λ_E and $\lambda_{E'}$ are zero maps. By (3.11), $\mathrm{ord}_p(x_{p-1}-x_1)\geq 2$ and $\mathrm{ord}_p(x'_{p-1}-x_1)\geq 2$. Hence $x_{p-1}\equiv x'_{p-1} \bmod p^2$. Then,

$$\begin{aligned} y'_{p-1}-y_{p-1}&=x'^3_{p-1}-x^3_{p-1}+a'_4x'_{p-1}-a_4x_{p-1}+a'_6-a_6\\ &\equiv x_1(a'_4-a_4)+(a'_6-a_6) \bmod p^2\\ &\equiv 0 \bmod p^2 \end{aligned}$$

which contradicts to (i). □

COROLLARY 3.8. *Let $p\geq 7$. Let $\tilde{E}$ be an anomalous elliptic curve defined over $\boldsymbol{F}_p$. Then we can solve discrete logarithm for $\tilde{E}(\boldsymbol{F}_p)$ with $O((\log p)^3)$ time complexity.*

Proof. Let $\alpha, \beta\in\tilde{E}(\boldsymbol{F}_p)-\{\mathcal{O}\}$. Since $\tilde{E}$ is anomalous, there exists $n\in\boldsymbol{F}_p$ satisfying $\beta=n\alpha$. Define E as in Corollary 3.6. Since λ_E is a homomorphism by Theorem 3.2, we have $\lambda_E(\beta)=n\lambda_E(\alpha)$. In case of $\lambda_E(\alpha)\neq 0$, we obtain $n=\frac{\lambda_E(\beta)}{\lambda_E(\alpha)}$. Otherwise, λ_E is a zero map by Corollary 3.4. By Theorem 3.5 (ii), at least one of $u(\alpha)$, $u(2\alpha)$, or $u(3\alpha)$ has an x-coordinate satisfying (3.12). (Note $p\geq 7$.) Therefore we can form a non-zero $\lambda_{E'}$ by Theorem 3.7 in $O((\log p)^2)$ time complexity. Thus, $n=\frac{\lambda_{E'}(\beta)}{\lambda_{E'}(\alpha)}$. The total running time of above procedure is clearly $O((\log p)^3)$. □

4. Concluding remarks†

4.1. Non-prime field case

Let p be a prime, $q:=p^r$ with $r\geq 1$, and K be an unramified extension of $\boldsymbol{Q}_p$ whose residue field is $\boldsymbol{F}_p$. See Serre [19, Chap. I, Sect. 6] for explicit construction of K. Let $\tilde{E}$ be an elliptic curve defined over $\boldsymbol{F}_q$. Let $A\in\tilde{E}(\boldsymbol{F}_q)$ and N its order, i.e., the cardinality of the cyclic group $\langle A\rangle$ generated by A. We write $N=p^e m$ where m is prime to p. We consider the discrete log problem for $\langle A\rangle$ in case of $e\geq 1$. Let $B=nA$ with $n\in\boldsymbol{Z}/N\boldsymbol{Z}$. Even if $m>1$, we obtain $n \bmod p^e$ in polynomial time as follows. There exist integers $n_0, \cdots, n_{e-1}$ satisfying $n\equiv\sum_{i=0}^{e-1} n_i p^i \bmod p^e$ and $0\leq n_i<p$. We put $A_0:=mp^{e-1}A$ and $B_0:=mp^{e-1}B$. Then $pA_0=\mathcal{O}$ and $B_0=n_0A_0$. In case of a small p, we obtain n_0 by checking whether $B_0=n_0A_0$ for $n_0=0, 1, \cdots, p-1$. Otherwise (at least $p\geq 7$), we use the elliptic Fermat quotient. Recall that the essential points of Sect. 3 are the following:

(i) The order of the base point A is p.

(ii) The formal logarithm $\log_{\mathcal{E}}$ is defined over $\psi(\mathrm{Ker}\,\pi)$.

Since $K/\boldsymbol{Q}_p$ is unramified, (ii) also holds for an elliptic curve over K. Choosing a lifting E of $\tilde{E}$ to the valuation ring of K, we obtain n_0 by $\lambda_E(B_0)/\lambda_E(A_0)$. In order to obtain n_i for $i\geq 1$, we use Pohlig-Hellman algorithm [14]. Assume we have obtained $n_0, \cdots, n_{k-1}$. Then $B_k:=mp^{e-k-1}(B-(\sum_{i=0}^{k-1} n_i p^i)A)$ satisfies $B_k=n_kA_0$, which yields n_k by the same method as above. Repeating this process, we obtain $n \bmod p^e$.

4.2. Density of vulnerable curves

It is natural to ask how often an elliptic curve is anomalous. By McKee [11, Theorem 2], the density of anomalous curves over $\boldsymbol{F}_p$ is at most $O\left(\frac{1}{\sqrt{p}}\log p \log\log p\right)$. In case of a large p, this is fairly small. For $q=p^r$, the probability of $p\,|\,{}^{\#}\tilde{E}(\boldsymbol{F}_q)$ converges to $1/(p-1)$ as $r\to\infty$ by Howe [4, Theorem 1.1].

4.3. Cryptographic implication

Since Miller [13] and Koblitz [8] independently proposed the elliptic curve cryptosystem, many works are done about this cryptosystem and a number of cryptographic apparatuses using elliptic curve discrete log problem are now commercially available. Among them, Menezes-Okamoto-Vanstone [12] showed that the discrete logarithm problem of supersingular curves is reduced to that of multiplicative group of some extensions of the base field. Since the discrete logarithm of finite filed is still considered to be difficult (sub-exponential time), the elliptic curve cryptosystem is believed to be no less secure than cryptosystem based on the discrete log problem of a finite field. However, our result indicates that we should choose the elliptic curve and its base point carefully. At least we should

† After the release of the first version of this paper, the authors received several comments and questions on it. Some of them fit better in the previous section. However, to be fair, we describe them here.

choose a base point whose order is divisible by a large prime other than the characteristic of a base field. This automatically excludes anomalous curves. Of course, this condition is one of necessary conditions for unvulnerability, *not* a sufficient condition.

References

[1] Abel, N. H.: Aufgabe aus der Zahlentheorie. J. Reine Angew. Math. **3**, 212 (1828) (=Œuvers, 2e ed, p. 619).

[2] Cassels, J. W. S.: Lectures on elliptic curves. London Mathematical Society Student Texts, 24. Cambridge: Cambridge UP 1991.

[3] Dickson, L. E.: History of the theory of numbers. New York: Chelsea publishing company 1966 (first print: 1919).

[4] Howe, E. W.: On the group orders of elliptic curves over finite fields. Compositio Math. **85**, 229–247 (1993).

[5] Ihara, Y.: On Fermat quotients and "the differential of numbers," Algebraic analysis and number theory, Koukyuuroku, **810**, 324–341, Kyoto: RIMS, Kyoto Univ., 1992. (in Japanese)

[6] Ireland, K. and Rosen, M.: A classical introduction to modern number theory. GTM, 84. Berlin-Heidelberg-New York: Springer 1982.

[7] Jacobi, C.: Beantwortung der Aufgabe Seite 212 des 3$^{\text{ten}}$ Bandes des Crelleschen Journals: "Kann $\alpha^{\mu-1}$, wenn μ eine Primzhal und α eine Ganze Zahl und kleiner als μ und grösser als 1 ist, durch $\mu\mu$ theilbar sein?". J. Reine Angew. Math. **3**, 301–302 (1828). (=Werke vol. 6, pp. 328–329)

[8] Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. **48**, 203–209 (1987).

[9] Lerch, M.: Zur Theorie des Fermatschen Quotienten $\dfrac{a^{p-1}-1}{p}=q(a)$. Math. Ann. **60**, 471–490 (1905).

[10] Mazur, B.: Rational points of Abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972).

[11] McKee, J.: Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field, (1997). to appear in J. London Math. Soc.

[12] Menezes, A. J., Okamoto, T. and Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Info. Theory **39**, 1639–1646 (1993).

[13] Miller, V. S.: Use of elliptic curves in cryptography, Advances in cryptology-CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci. **218**, 417–426, Berlin-Heidelberg-New York: Springer, 1986.

[14] Pohlig, S. C. and Hellman, M. E.: An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. IEEE Trans. Info. Theory **24**, 106–110 (1978).

[15] Ribenboim, P.: The new book of prime number records, 3rd ed. Berlin-Heidelberg-New York: Springer 1995.

[16] Rück, H. G.: On the Discrete Logarithm in the Divisor Class Group of Curves, (1997). preprint.

[17] Semaev, I. A.: Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p. Math. Comp. **67**, 353–356 (1998).

[18] Serre, J.-P.: A course in arithmetic. GTM, 7. Berlin-Heidelberg-New York: Springer 1973.

[19] Serre, J.-P.: Local fields. GTM, 67. Berling-Heidelberg-New York: Springer 1979.

[20] Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1985.

[21] Smart, N. P.: The discrete logarithm problem on elliptic curves of trace one, (1997). To appear in J. Cryptology.

[22] Voloch, J. F.: Relating the Smart-Satoh-Araki and Semaev approaches to the discrete logarithm

problem on anomalous elliptic curves, (1997). preprint, Available at http://www.ma.utexas.edu/users/voloch

Takakazu SATOH
Dept. Mathematics, Fac. Sci., Saitama University
255 Shimo-ookubo, Urawa, Saitama 338–8570 Japan
tsatoh@rimath.saitama-u.ac.jp

Kiyomichi ARAKI
Dept. Computer Eng., Fac. Eng., Tokyo Institute of Technology
2–12–1 Oh-okayama, Meguro, Tokyo 152–8552 Japan
araki@ss.titech.ac.jp