COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 48, No. 2 1999

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171-8501 JAPAN

Errata to the paper: Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves (*published in Commentarii Math. Univ. St. Pauli*, 47(1), 81–92, 1998)

by

Takakazu SATOH and Kiyomichi ARAKI

(Received March 25, 1999)

There was a critical error in the proof of Theorem 3.7(i). As a consequence, the proof of Corollary 3.8 must be modified. The problem is that Theorem 3.5(ii) is only valid for the cases stated there which are not enough for the proof of Theorem 3.7(i). The authors would like to thank Prof. Andrzej Daszkiewicz at Copernicus University, Poland, and his student Mr. Maciej Koprowski for pointing out this to the authors. The authors also appreciate Prof. Yuichiro Taguchi at Hokkaido University, Japan for discussion. It is plausible that the algorithm in the original paper raise "division by zero" with probability $1/p^2$. If this exception does not occur, the original algorithm always returns a correct answer.

To obtain the correct version of Theorem 3.7 and Corollary 3.8 (i.e., a deterministic polynomial time algorithm of discrete log problem on anomalous elliptic curve), we use a certain property on canonical lift. For an ordinary elliptic curve $\tilde{E}/\boldsymbol{F}_p$, we call a lifting $\tilde{E}^{\uparrow}/\boldsymbol{Q}_p$ of $\tilde{E}$ the *canonical lift* of $\tilde{E}$ if $\mathrm{End}(\tilde{E}^{\uparrow})$ is isomorphic to $\mathrm{End}(\tilde{E})$. The existence of such a lifting is classically studied by Deuring [1], and, in the context of modern algebraic geometry by Serre-Tate (see e.g. Messing [3]). Let K be a complete discrete valuation field of characteristic zero whose residue field k is algebraically closed field of characteristic p. Let E/K be an elliptic curve with the ordinary reduction $\tilde{E}/k$. For $S \subset E$, we denote by $K(S)$ the field generated by coordinates of all the points in $S-\{\mathcal{O}\}$. Recall that a finite extension L/K is defined to be *tamely ramified* if $e \not\equiv 0 \bmod p$ (and $e>1$), where e is the ramification index of L/K. We notice that $1 \leq e \leq [L:K]$ in any case. (See e.g. Lang [2, Part one, Chap. II] for details on this topic.) With these conventions, we can state a theorem by Serre, which is a key to our proof.

THEOREM (Serre). *Let E/K be an elliptic curve with the ordinary reduction $\tilde{E}/k$ and $\tilde{E}^{\uparrow}$ the canonical lift of $\tilde{E}$. Assume $j(\tilde{E})$ is algebraic over $\boldsymbol{F}_p$. Define $\mu(E)$ by*

$$\mu(E)=\begin{cases} 3 & (j(\tilde{E}^{\uparrow})=0), \\ 2 & (j(\tilde{E}^{\uparrow})=1728), \\ 1 & (\textit{otherwise}). \end{cases}$$

Then the following conditions are equivalent:

(1) $K(E[p])/K$ *is tamely ramified.*

(2) $j(E) \equiv j(\tilde{E}^{\uparrow}) \bmod p^{1+\mu(E)}$.

According to Nakamura [4], this theorem is obtained by Serre. However, Nakamura [4] gives an elementary proof. In what follows, we let K be the maximal unramified extension of $\boldsymbol{Q}_p$. Then, k is the algebraic closure of $\boldsymbol{F}_p$ and the condition on $j(\tilde{E})$ is automatically satisfied.

THEOREM 3.7. *Let* $p \geq 5$ *and* $E/\boldsymbol{Q}_p$ *be an elliptic curve whose reduction* $\tilde{E}/\boldsymbol{F}_p$ *is anomalous. Assume* $\lambda_E = 0$. *Then* $j(E) \equiv j(\tilde{E}^{\uparrow}) \bmod p^{1+\mu(E)}$.

Proof. Without loss of generality, we may assume E is given by the Weierstrass equation on which $-(x, y) = (x, -y)$. By Corollary 3.4, $\lambda_E = 0$ implies the group $H := E(\boldsymbol{Z}_p) \cap E[p]$ is a cyclic group of order p. Put $G := E[p] \cap \operatorname{Ker} \pi$. We show G is also a cyclic group of order p. Otherwise, $G = \{\mathcal{O}\}$ since G cannot be whole $E[p] \cong \boldsymbol{Z}/p\boldsymbol{Z} \oplus \boldsymbol{Z}/p\boldsymbol{Z}$. For $P \in E[p]$, there exists $Q \in H$ satisfying $\pi(P) = \pi(Q)$. Then $P - Q \in G$ and $P = Q$ by $G = \{\mathcal{O}\}$. Hence $E[p] \subset H$ and thus $p^2 = {}^{\#}E[p] \leq {}^{\#}H = p$, a contradiction. Therefore, only possibility is $G \cong \boldsymbol{Z}/p\boldsymbol{Z}$. By the similar argument, we obtain $E[p] = H \oplus G$ as a group. Hence $H \subset E(\boldsymbol{Z}_p)$ yields $K(E[p]) = K(G)$. Let $(\xi, \eta) \in G - \{\mathcal{O}\}$. Then $K(G) = K(\xi, \eta)$ because $G \cong \boldsymbol{Z}/p\boldsymbol{Z}$ and E is defined over $\boldsymbol{Z}_p$. By Silverman [6, Theorem VII.3.4], $K(\xi, \eta)/K$ is a ramified extension. Since $\sigma(P) \in G$ for all $P \in G$ and all $\sigma \in \operatorname{Gal}(\overline{\boldsymbol{Q}_p}/\boldsymbol{Q}_p)$, the group G is defined over $\boldsymbol{Q}_p$ (hence over K). Thus $[K(\xi) : K] \leq {}^{\#}\{x : (x, y) \in G - \{\mathcal{O}\}\} = (p-1)/2$. Of course $[K(\xi, \eta) : K(\xi)] \leq 2$. Therefore $[K(\xi, \eta) : K] \leq p - 1 < p$ and $K(E[p])/K$ must be tamely ramified. Using the above mentioned Theorem of Serre-Nakamura we complete the proof. □

COROLLARY 3.8. *Let* $p \geq 5$ *and* $E : y^2 = x^3 + a_4 x + a_6$ *with* $a_4, a_6 \in \boldsymbol{Z}$ *be an elliptic curve. Assume* $0 \leq a_4 < p^2$ *and* $0 \leq a_6 < p^2$. *We denote its reduction modulo* p *by* $\tilde{E} : y^2 = x^3 + \tilde{a}_4 x + \tilde{a}_6$. *Assume* $\tilde{E}$ *is anomalous and* $\lambda_E = 0$. *Then,* $\lambda_{E'} \neq 0$ *where* E' *is defined by*

$$\begin{aligned} &y^2 = x^3 + px + a_6 && (\tilde{a}_4 = 0), \\ &y^2 = x^3 + a_4 x + p && (\tilde{a}_6 = 0), \\ &y^2 = x^3 + (a_4 + p)x + a_6 && (\textit{otherwise}). \end{aligned}$$

Especially, we can solve the discrete logarithm problem in $\tilde{E}(\boldsymbol{F}_p)$ *with* $O((\log p)^3)$ *bit operation time complexity.*

Proof. In case of $\tilde{a}_4 = 0$ (hence $\tilde{a}_6 \neq 0$): Let $\omega \in \overline{\boldsymbol{F}_p}$ be a primitive third root of unity. The automorphism $[\omega]$ defined by $[\omega](x, y) := (\omega x, y)$ is of order 3. By the definition of the canonical lifting, $[\omega]$ lifts to an element $[\omega]^{\uparrow}$ of $\operatorname{Aut}(\tilde{E}^{\uparrow})$ and the order of $[\omega]^{\uparrow}$ is 3. Hence $j(\tilde{E}^{\uparrow}) = 0$ by Silverman [6, Theorem III.10.1]. Since

$$j(E') = \frac{1728 \cdot 4p^3}{4p^3 + 27a_6^2} \not\equiv 0 \bmod p^4,$$

Theorem 3.7 gives $\lambda_{E'} \neq 0$. Similarly in case of $\tilde{a_6}=0$, using automorphism $[\varrho](x, y) := (-x, \varrho y)$ with $\varrho^2 = -1$, we see $^{\#}\mathrm{Aut}(\tilde{E})=4$ and $j(\tilde{E}^{\uparrow})=1728$. Then, $j(E')=1728\,(1-27p^2/(4a_4^3)+O(p^3))$. Hence $\lambda_{E'} \neq 0$.

Finally, assume $\tilde{a_4} \neq 0$ and $\tilde{a_6} \neq 0$. Note $j(\tilde{E}^{\uparrow})$ is neither 0 nor 1728. Hence $\lambda_E = 0$ implies $j(E) \equiv j(\tilde{E}^{\uparrow}) \bmod p^2$ by Theorem 3.7. Using

$$\frac{\partial j}{\partial a_4} = 1728 \frac{12 \cdot 27 \cdot a_4^2 a_6^2}{(4a_4^3+27a_6^2)^2} \not\equiv 0 \mod p,$$

we see $j(E') \not\equiv j(E) \bmod p^2$, and therefore $\lambda_{E'} \neq 0$ again by Theorem 3.7. The proof of the remaining assertion is the same as in the original paper. □

REMARKS. (i) The curve $y^2 = x^3 + 3x$ over $\boldsymbol{F}_5$ is the only anomalous curve for which $\tilde{a_6}=0$ by Olson [5, Corollary 2.2].

(ii) We have concerned how to construct quickly a lifting of $\tilde{E}$ "away from" its canonical lift. On the contrary, Voloch [7] obtains the third approach for discrete log problem of p-part of elliptic curves over finite fields. This method *uses* the canonical lift and the theory of p-descent.

Other misprints: p. 86, line 2 and p. 88, line 7: insert a "$-$" just after $\lambda_E(\alpha) =$.

References

[1] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg, **14**, 197–272 (1941).

[2] Lang, S.: Algebraic number theory. Reading. Mass.: Addison-Wesley Pub., 1970.

[3] Messing, W.: The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes. Lect. Notes in Math., 264. Berlin-Heidelberg-New York: Springer 1972.

[4] Nakamura, T.: A note on elliptic curves with ordinary reduction. Arch. Math., **60**, 440–445 (1980).

[5] Olson, L. D.: Hasse invariants and anomalous primes for elliptic curves with complex multiplication. J. Number Theory, **8**, 397–414 (1976).

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

[7] Voloch, J. F.: The discrete logarithm problem on elliptic curves and descents, (1998). preprint

Takakazu Satoh
Dept. Mathematics, Fac. Sci.
Saitama University
255 Shimo-ookubo, Urawa
Saitama 338–8570, Japan
E-mail: 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
E-mail: araki@ss.titech.ac.jp