Memoirs of the Faculty of Education
Akita University (Natural Science)
28. 40—44 (1978)

Remarks on the Arithmetic of Elliptic Curves(I)

Hideji Ito

(*Received September* 10, 1977)

In [1], we investigated the law of decomposition of primes in certain galois extensions $K_\ell/\mathbf{Q}$ relating with elliptic curves. In this note, explicit laws are obtained in special cases: $\ell = 2, 3$.

§ 1. Introduction

Let E be an elliptic curve defined over $\mathbf{Q}$ such that $E(\mathbf{Q}) \neq \phi$. For a rational prime ℓ, put $E_\ell = \{a \in E \mid \ell a = 0\}$ and $K_\ell = \mathbf{Q}(E_\ell)$, i.e. K_ℓ is the number field generated over $\mathbf{Q}$ by all the coordinates of the points of order ℓ on E. Then $K_\ell/\mathbf{Q}$ is a galois extension and $\mathrm{Gal}(K_\ell/\mathbf{Q}) \cong GL_2(\mathbf{Z}/\ell\mathbf{Z})$, except for finitely many ℓ's [3]

For $\ell \geqq 5$, $GL_2(\mathbf{Z}/\ell\mathbf{Z})$ is non-solvable and it is hard to analyse their arithmetic. But for $\ell = 2, 3$, $K_\ell/\mathbf{Q}$ is a solvable extension and we know their structure well (see lemma 1). So we can state the law of decomposition of primes explicitly (these were stated without proof in [1]). Also we can paraphrase the condition "$\ell \mid (\mathfrak{o} : \mathbf{Z}[\pi])$ or not" in [1] in easier form in case $\ell = 3$.

§ 2. Our approach

Let p be a rational prime where E has good reduction. Then it is well-known that p is unramified in every $K_\ell/\mathbf{Q}$ ($\ell \neq p$). We exclusively deal with that case in this note. (Bad primes are finite innumber).

Let P an algebraic point of E i.e. $P \in E(\overline{\mathbf{Q}})$. When we view $E/\mathbf{Q}$ as defined over $\mathbf{Q}_p$, we must take some care of the rationality of P. Put $k = \mathbf{Q}(P)$ and $\mathfrak{p}$ an extension of p to k. Then P is rational over $k_\mathfrak{p}$. Thus the rationality of P in $\overline{\mathbf{Q}}_p$ depends on the choice of $\mathfrak{p}$, that is, the way of emdedding of k into $\overline{\mathbf{Q}}_p$. In particular, we can see the following fact:

P is $\mathbf{Q}_p$-rational under an embedding of $\mathbf{Q}(P)$ into $\overline{\mathbf{Q}}_p \Longleftrightarrow$ In $\mathbf{Q}(P)$, p is divisible by a prime of degree 1.

Formulating with $K_\ell = \mathbf{Q}(E_\ell)$, we see:

p splits completely in $K_\ell/\mathbf{Q} \Longleftrightarrow E(\mathbf{Q}_p) \supset E_\ell$.

As reduction map induces an isomorphism between the subgroups consisting of points of finite order prime to p of $E(\mathbf{Q}_p)$ and of $E'(F_p)$, the latter is equivalent to $E'(Fp) \supset E'_\ell$, where we put $E' = E$ mod p, $E'_\ell = \{a \in E' \mid \ell a = 0\}$. Combining the knowledge $K_\ell \supset \mathbf{Q}(\zeta_\ell)$, where ζ_ℓ is a primitive root of unity of order ℓ, we have necessary conditions for a prime p to split completely in $K_\ell/\mathbf{Q}$ as follows:

$\ell^2 \mid N_p$, $\ell \mid (p-1)$,

Whether above condition is at the same time sufficient or not is the motivation of our study and the answer turns out no (see §4 in this note or [1] theorem 1).

§ 3. Some lemmas

For E: $Y^2 = X^3 + AX + B$, A, B $\in \mathbf{Z}$, put $\delta = -2^4(4A^3 + 27B^2)$, $j = 2^8 3^3 A^3/(4A^3 + 27B^2)$ as usual.

Lemma 1. $K_2 = \mathbf{Q}(\sqrt{\delta}, P_2)$, $K_3 = \mathbf{Q}(\sqrt[3]{\delta}, \zeta_3, P_3)$, *where* $P_\ell (\neq 0) \in E_\ell$, $\ell = 2, 3$.

Proof. When $j \neq 0$, 1728, our assertions are readily verified by virtue of Hilfsatz 1.1, 1.2, 1.4 in [2]. When $j = 0$ or 1728, E can be written in Weierstrass form as $Y^2 = X^3 - D$, $Y^2 = X^3 - DX$ (resp.). So we can verify in each case by writing down the equations which x-coordinates of points of order 1 must satisfy. For example, when $j = 1728$, $\sqrt[3]{\delta} = 4D$ and x-coordinates of 3-section points are given by $3X^4 - 6DX^2 - D^2 = 0$. Hence $x = \pm\sqrt{\frac{3 \pm 2\sqrt{3}}{3}D}$. As

$\sqrt{\frac{3+2\sqrt{3}}{3}D} \times \sqrt{\frac{3-2\sqrt{3}}{3}D} = \frac{D}{3}\sqrt{-3}$, we have $\mathbf{Q}$(x-coordinates of E_3) $=$

$\mathbf{Q}(\zeta_3$, one x). So by Hilfsatz 1.1 in [2], we have our assertion.

Lemma 2. *Let $k/\mathbf{Q}$ be a finite galois extension, $k'/\mathbf{Q}$ a finite extension, both having an embedding into $\mathbf{Q}_p$. If p is unramified in both k and k', then there is an embedding of kk' into $\mathbf{Q}_p$.*

Proof. Let K be the smallest galois extension of Q containing kk'. By the assumption, there is an extension $\mathfrak{P}$ of p to K for which the restriction of $\mathfrak{P}$ to k' is of degree 1. Since $k/\mathbf{Q}$ is galois, $k \subsetneq \mathbf{Q}_p$ means that any extension of p to k, especially the restriction of $\mathfrak{P}$ to k, is of degree 1. Therefore, the decomposition field of $\mathfrak{P}$ (with respect to $\mathbf{Q}$) contains k and k'. So, the restriction of $\mathfrak{P}$ to kk' gives the desired embedding $kk' \subsetneq \mathbf{Q}_p$, q.e.d.

Remark 1. In general even if $k \subsetneq \mathbf{Q}_p$ and $k' \subsetneq \mathbf{Q}_p$, kk' cannot necessarily be embeddable into $\mathbf{Q}_p$. For example, let $F = \mathbf{Q}(\zeta_3, \sqrt[3]{7})$, $K_i = Q(\zeta^i \sqrt[3]{7})$, $i = 0, 1, 2$. Then $K_i \subsetneq \mathbf{Q}_5$ for all i, but $F = K_1 K_2 \not\subset \mathbf{Q}_5$. Indeed, since $X^3 - 7 \equiv (X-3)(X^2+3X+4) \pmod 5$, 5 has the decomposition of type $5 = \mathfrak{p}_1 \mathfrak{p}_2$, $N\mathfrak{p}_1 = 5^2$, $N\mathfrak{p}_2 = 5$ in K_i (X^2+3X+4 is irreducible over $\mathbf{Z}/5\mathbf{Z}$). On the other hand, 5 remains prime in $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$. Therefore $5 = \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$, $N\mathfrak{P}_i = 5^2$ in F. Hence $F \not\subset \mathbf{Q}_5$. (In our situation, if $\mathrm{Gal}(K_\ell/\mathbf{Q}) \cong GL_2(\mathbf{Z}/\ell\mathbf{Z})$, then for any non-zero P, $P' \in E_\ell$, $\mathbf{Q}(P) = \mathbf{Q}(P')$ or they are conjugate to each other. So $\ell \mid N_p$ means that p is divided by a prime of degree 1 in every $\mathbf{Q}(P)$. But this does not mean p splits completely in $K_\ell = \bigcup_{P \in E_\ell} \mathbf{Q}(P)$).

§ 4. Decomposition of primes in K_2, K_3

Recall that $\mathrm{Gal}(K_\ell/\mathbf{Q}) \subsetneq GL_2(\mathbf{Z}/\ell\mathbf{Z})$ in any case.

Theorem 1. *In $K_2/\mathbf{Q}$, P decomposes completely if and only if* (1) $2 \mid N_p$ *and* (2) *p splits in* $\mathbf{Q}(\sqrt{\delta})$.

Proof. As is explained in §2, $2 \mid N_p \Longleftrightarrow$ p has an extension of degree 1 in $\mathbf{Q}(P)$ for some $P(\neq 0) \in E_2$. By lemma 1, $K_2 = \mathbf{Q}(\sqrt{\delta}, P)$. So applying lemma 2 we see if part. Only if part is obvious, q. e. d.

Corollary. *If $2 \| N_p$, i. e. $N_p = 2d$, $2 \nmid d$, then p remains prime in* $\mathbf{Q}(\sqrt{\delta})$.

As an example, let us take $E = X_0(11)$. For $\ell \neq 5$, it is known that $\mathrm{Gal}(K_\ell/\mathbf{Q}) \cong GL_2(\mathbf{Z}/\ell\mathbf{Z})$ and $\mathbf{Q}(\sqrt{\delta}) = \mathbf{Q}(\sqrt{-11})$ ([3] p. 309).

From the table of the values of $a_p (= 1 - N_p + p)$ given in [4], we know the first 10 primes satisfying $2 \| N_p$ are p = 7, 13, 29, 41, 43, 61, 73, 79, 83, 107. In every case we can see $\left(\frac{-11}{p}\right) = -1$.

Theorem 2. *In $K_3/\mathbf{Q}$, p splits completely if and only if*

(1) $3 \mid (p-1)$, (2) $3 \mid N_p$, (3) $\delta \bmod p \in (\mathbf{F}_p)^3$.

Proof. By lemma 1, if part is obvious. Assume the conditions (1), (2), (3) hold. Put $k = \mathbf{Q}(\zeta_3, \sqrt[3]{\delta})$. Then (1), (3) mean that p splits completely in k by lemma 2. As $3 \mid N_p$ means that p is divided by a prime of degree 1 of $\mathbf{Q}(P)$ for some $P \in E_3$ and $K_3 = k(P)$, where $k/\mathbf{Q}$ is a galois extension, again by lemma we see the validity of if part, q. e. d.

Let us again consider $E = X_0(11)$. By [4], $a_{79} = -10$, so $N_{79} = 90 = 2 \cdot 3^2\, 5$. Thus the prime $p = 79$ satisfies $3 \mid (p-1)$, and $3^2 \mid N_p$. But the condition (3) is not satisfied as can be seen by direct calculation. Hence the degree of 79 in $K_3/\mathbf{Q}$ is 3. (In general $\ell^2 \mid N_p$, $\ell \mid (p-1)$ lead that the degree of p in $K_l/\mathbf{Q}$ is either 1 or ℓ, which can be seen by matrix representation [4] or by theorem 1 in [1]). When $p = 337$, then $a_{337} = -22$. So $N_{337} = 360 = 2^3\, 3^2\, 5$. As $3 \mid (337-1)$ and $-11 \equiv (10)^3 \mod 337$, $p = 337$ splits completely in $K_3/\mathbf{Q}$.

§ 5. The 3-part of $(\mathfrak{o}_p : \mathbf{Z}[\pi_p])$

Let $\mathfrak{o}_p$ be the algebra of $\mathbf{F}_p$ endomorphisms of E mod p, i. e. $\mathfrak{o}_p = \mathrm{End}_{\mathbf{F}_p}$ (E mod p), and π_p be the p-th power endomorphism of E mod p. Then the corollary 1 of theorem in [1] asserts that for $\ell > 2$, p splits completely in $K_\ell/\mathbf{Q}$ if and only if $\ell^2 \mid N_p$, $\ell \mid (p-1)$ and $\ell \mid (\mathfrak{o}_p : \mathbf{Z}[\pi_p])$. In view of our theorem 2, we are naturally led to investigate the relation between $(\mathfrak{o}_p : \mathbf{Z}[\pi_p])$ and δ.

First we need the following

Lemma 3. *There is a submodule $A\,(\neq \{0\}, E'_\ell)$ of E'_ℓ which is $\mathbf{F}_p$-rational if and only if $\ell \mid N_{p^{\ell-1}}$*

Proof. (Only if part). We can write $E'_\ell = A \oplus B$, for some $B \supset E'_\ell$, $|B| = \ell$. Representing π_p with respect to above decomposition, we have $\pi_p = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ over $\mathbf{F}_\ell$. Then $(\pi_p)^{\ell-1} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, which means that all the points of A are $\mathbf{F}_{p^{\ell-1}}$-rational. So $\ell \mid N_{p^{\ell-1}}$.

(If part). By the hypothesis, with respect to a suitable basis, $\pi^{\ell-1}$ can be written as $\pi^{\ell-1} = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$, a, $b \in \mathbf{F}_\ell$. Let the characteristic roots of π be c and $d \in \mathbf{F}_{\ell^2}$. Then $c^{\ell-1} = 1$(say), i. e. $c \in \mathbf{F}_\ell$. As $c + d = \mathrm{tr}(\pi) \in \mathbf{F}_\ell$, we also have $d \in \mathbf{F}_\ell$. Therefore over $\mathbf{F}_\ell$, $\pi = \begin{pmatrix} c & * \\ 0 & d \end{pmatrix}$. This means that some subgroup of E'_ℓ of order ℓ is $\mathbf{F}_p$-rational, q. e. d.

Remark 2. It holds that $N_{p^2} = 1 - a_{p^2} + p^2 = (1 - a_p + p)(1 + a_p + p)$. So if $p \equiv 1 \pmod 3$, then $3 \mid N_{p^2}$ iff $a_p \equiv \pm 2 \pmod 3$, while if $p \equiv 2 \pmod 3$, then $3 \mid N_{p^2}$ iff $a_p \equiv 0 \pmod 3$.

Theorem 3. *Following two assertions are equivalent for $p>3$:*

(1) $3 \mid (\mathfrak{o}_p : \mathbf{Z}[\pi_p])$, (2) $\delta \bmod p \in (\mathbf{F}_p)^3$, $3^2 \mid N_{p^2}$, $3 \mid (p-1)$.

Proof. (1) $\Rightarrow$ (2) By theorem 2 in [1], we know $3 \mid (\mathfrak{o}_p : \mathbf{Z}[\pi_p]) \Longleftrightarrow$ all 3-isogenies from E′ are defined over $\mathbf{F}_p$. But the kernels of 3-isogenies are the subgroups of order 3. So they are $\mathbf{F}_p$-rational. Hence π_p can be written in the following form : $\pi_p = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Therefore π_p^2 = identity (since $\ell = 3$), $3 \mid (p-1)$. That is to say, $f = (\mathbf{F}_p(E'_1) : \mathbf{F}_p) = 1$ or 2. So $3^2 \mid N_{p^2}$. As we know that $3 \mid f$ iff $\delta \bmod p$ $\in (\mathbf{F}_p)^3$. ...... (*) (cf. [3] p. 305), we see $\delta \bmod p \in (\mathbf{F}_p)^3$. (2) $\Rightarrow$ (1) By lemma 3, π_p can be written as $\pi_p = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$. As δ mod $\in (\mathbf{F}_p)^3$, the equivalence (*) leads $b = 0$. So $\pi_p = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, since $\det \pi p = 1$, which means that two subgroups of order 3 of E'_3 are $\mathbf{F}_p$-rational. From this we easily see that all subgroups of order 3 are $\mathbf{F}_p$ rational, q. e. d.

Corollary. *If* $3 \parallel N_{p^2}$ *and* $3 \mid (p-1)$ *then* $\delta \bmod p \in (\mathbf{F}_p)^3$.

Remark 3. In [1], theorems 1 and 2 are independent to each other. Using theorem 2, the part (2) of theorem 1 can be strengthend as follows : if $\ell^2 \mid (a_p)^2 - 4p$ then $f \mid \ell(\ell-1)$, moreover if $\ell \mid (\mathfrak{o}_p : \mathbf{Z}[\pi_p])$ then $f \mid (\ell-1)$, if $\ell \nmid (\mathfrak{o}_p : \mathbf{Z}[\pi_p])$ then $\ell \mid f$. These are verified in the similair way as the first part of the proof the above theorem 3.

References

[1] H. Ito, A note on the law of decomposition of primes in certain galois extension, Proc. Japan Acad. **53**, No.4 115—118 (1977)

[2] O. Neumann, Zur Reduktion der elliptischen Kurven, Math. Nachr, **46**, 285—310 (1970).

[3] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes élliptiques, Invent. math. **15**, 259—331 (1972).

[4] G. Shimura, A reciprocity law in non-solvable extensions, J. Reine Angew. Math. **221**, 209—220 (1966).

Department of Mathematics
AKITA UNIVERSITY
AKITA, JAPAN