32. A Note on the Law of Decomposition of Primes in Certain Galois Extension

By Hideji ITO
Department of Mathematics, Akita University

(Communicated by Kôsaku YOSIDA, M. J. A., Sept. 12, 1977)

Let E be an elliptic curve defined over $\boldsymbol{Q}$, and ℓ a rational prime. Put $E_\ell=\{a\in E\mid \ell a=0\}$ and $K_\ell=\boldsymbol{Q}(E_\ell)$ i.e. the number field generated over $\boldsymbol{Q}$ by all the coordinates of the points of order ℓ on E. Then $K_\ell/\boldsymbol{Q}$ is a galois extension and $\mathrm{Gal}(K_\ell/\boldsymbol{Q})\subsetneq \mathrm{GL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$. When E has no complex multiplication, $\mathrm{Gal}(K_\ell/\boldsymbol{Q})\cong \mathrm{GL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$ except for finitely many ℓ's ([6]). And we know that $\mathrm{GL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$ is non-solvable for $\ell>3$.

The aim of this note is to investigate the law of decomposition of primes in $K_\ell/\boldsymbol{Q}$. Let p be a rational prime $(\neq\ell)$ where E has good reduction. Then p is unramified in $K_\ell/\boldsymbol{Q}$. We deal exclusively in that case. (Note that the method in [7] enables one to determine the degrees of most primes but not all, especially the complete splitting case cannot be determined.)

Let $\pi=\pi_p$ be the p-th power endomorphism of E mod p. Put $N_{p^m}=\sharp(E \bmod p)(\boldsymbol{F}_{p^m})$ and $a_{p^m}=\mathrm{tr}\,(\pi^m)$, where trace is taken with respect to ℓ-adic representation of $E \bmod p$. Then $N_{p^m}=1-a_{p^m}+p^m$. (Note that we can calculate a_{p^m} by the value a_p). As $\mathrm{End}_{\boldsymbol{F}_p}(E \bmod p)$ is isomorphic to an order $\mathfrak{o}$ of an imaginary quadratic field k, hereafter we identify them (so $\pi\in\mathfrak{o}$, $k=\boldsymbol{Q}(\pi)$).

Theorem 1. *Let $\ell>2$ and f be the degree of p in $K_\ell/\boldsymbol{Q}$, and m the smallest rational integer >0 which satisfies $\ell^2\mid N_{p^m}$ and $\ell\mid(p^m-1)$. Then the following assertions hold.* (1) *If $\ell^2\nmid((a_p)^2-4p)$, then $f=m$.* (2) *If $\ell^2\mid((a_p)^2-4p)$, then $f=m$ or ℓm, according as $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi])$ or not, where $\mathfrak{o}=\mathrm{End}_{\boldsymbol{F}_p}(E \bmod p)$.*

Corollary 1. *p decomposes completely in $K_\ell/\boldsymbol{Q}\Leftrightarrow\ell^2\mid N_p$, $\ell\mid(p-1)$, $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi])$.*

Corollary 2. *If $\ell\,\|\,N_p$, $\ell\mid(p-1)$, then $f=\ell$ and $\ell^2\mid N_{p^\ell}$.*

Proof. We put $E'=E \bmod p$, $E'_\ell=\{a\in E'\mid \ell a=0\}$. First we note that the degree f is nothing but the order of π in $(\mathfrak{o}/\ell\mathfrak{o})^\times$. Indeed, $f=$the degree of p in $K_\ell/\boldsymbol{Q}\Leftrightarrow[\boldsymbol{Q}_p(E_\ell):\boldsymbol{Q}_p]=f\Leftrightarrow[\boldsymbol{F}_p(E'_\ell):\boldsymbol{F}_p]=f\Leftrightarrow\pi^f\equiv1 \bmod \ell\mathfrak{o}$, $\pi^n\not\equiv1 \bmod \ell\mathfrak{o}$ for all $n<f$. (For the second $\Leftarrow$, see [4] p. 672.) And this shows especially that $\ell^2\mid N_{p^f}$ and $\ell\mid(p^f-1)$. Put $p^m=q$. When $\ell>2$, we see $\ell^2\mid N_q$, $\ell\mid(q-1)\Leftrightarrow\ell^2\mid(a_q)^2-4q$, $a_q\equiv2 \pmod{\ell}$. So we can write $a_q=2+\ell a$, $(a_q)^2-4q=\ell^{2s}\cdot n^2(-d)$, $a,s,n,d\in\boldsymbol{Z}$, $s>0$, $\ell\nmid n$,

$d=$ squarefree >0. Therefore $\pi^m=\pi_q=(a_q+\sqrt{(a_q)^2-4q})/2=1+\ell(a+\ell^{s-1}n\sqrt{-d})/2$. Put $w_q=(a+\ell^{s-1}n\sqrt{-d})/2$. Then $w_q\in\mathfrak{o}_k$, the maximal order of k, and $\pi_q=1+\ell w_q$, $(\boldsymbol{Z}[w_q]:\boldsymbol{Z}[\pi_q])=\ell$. Hence we see i) if $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi_q])$, then as $\mathfrak{o}\supset\boldsymbol{Z}[w_q]$, $f=m$, ii) if $\ell\nmid(\mathfrak{o}:\boldsymbol{Z}[\pi_q]$, then as $\mathfrak{o}\not\supset\boldsymbol{Z}[w_q]$, $f=\ell m$. (Note that for two orders R, R' in k with conductors c, c' it holds that $R\supset R'\Leftrightarrow c\mid c'$). Indeed in case ii) we have $\pi^m\not\equiv 1 \bmod \ell\mathfrak{o}$. Since $\pi^{m\ell}=1+\ell^2$ (a polynomial of w_q) and $\ell\boldsymbol{Z}[w_q]\subset\boldsymbol{Z}[\pi_q]\subset\mathfrak{o}$, we have $\pi^{m\ell}\equiv 1 \bmod \ell\mathfrak{o}$. So $f\mid\ell m$. As $f\neq m$, we have $f=\ell s$, $s\mid m$. Then $\ell\mid(t-1)$, where $t=p^s$. So if $\ell^2\mid N_t$ then $s=m$; if $\ell\| N_t$ then $\ell^2\nmid(a_t)^2-4t$, but as $\ell^2\mid(a_q)^2-4q$, we see $\ell\mid(\boldsymbol{Z}[\pi_t]:\boldsymbol{Z}[\pi_q])$ and this leads $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi_q])$, a contradiction; if $\ell\nmid N_t$, then considering the rationality of the points of E'_ℓ, we know that ℓ must divide m/s, but this contradicts $\pi^m\equiv 1 \bmod \ell\mathfrak{o}$. Case i) is evident.

Now the assertions (1) and the first part of (2) are obvious, since the assumptions lead $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi_q])$. So hereafter we assume $\ell^2\mid(a_p)^2-4p$, $\ell\nmid(\mathfrak{o}:\boldsymbol{Z}[\pi])$. Under the first assumption we easily see that $\ell\mid(\boldsymbol{Z}[\pi]:\boldsymbol{Z}[\pi^r])\Leftrightarrow\ell\mid r$. In view of above ii), what we must show is $\ell\nmid(\mathfrak{o}:\boldsymbol{Z}[\pi^m])$. Assume the contrary: $\ell\mid(\mathfrak{o}:\boldsymbol{Z}[\pi^m])$. Then $m=\ell r$, for some $r\in\boldsymbol{Z}$. Putting $p^r=u$, this leads $\ell^2\mid N_u$ or $\ell^2\mid N_{u^2}$ (and $\ell\mid(u-1)$) which violate the minimality of m. Indeed, since $\ell^2\mid(a_p)^2-4p$, we see $\ell^2\mid(a_u)^2-4u$, so $a_u\equiv\pm 2 \bmod \ell$. If $a_u\equiv 2 \bmod \ell$, then $N_u\equiv 0 \bmod \ell$. Suppose $\ell\| N_u$, then $(a_u)^2-4u=(1-u)^2-2(1+u)N_u+(N_u)^2\not\equiv 0 \bmod \ell^2$. So we have $\ell^2\mid N_u$. If $a_u\equiv -2 \bmod \ell$, then $N_{u^2}=N_u(1+a_u+u)\equiv 0 \bmod \ell$. In the same way as above wee see $\ell^2\mid N_{u^2}$. This completes the proof of our theorem.

Proof of Corollaries. Corollary 1 is obvious. Corollary 2. Use [7] Lemma 1 or argue as follows. In general for $P(\neq 0)\in E_\ell$, we have $(K_\ell:\boldsymbol{Q}(P,\zeta))=1$ or ℓ, where ζ is a primitive root of unity of degree ℓ. Indeed,

$$\mathrm{Gal}\,(K_\ell/\boldsymbol{Q}(P,\zeta))\subsetneq\left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}\in \mathrm{GL}_2\,(\boldsymbol{Z}/\ell\boldsymbol{Z})\right\}.$$

Our assumption means that p is divided by a prime of absolute degree 1 in $\boldsymbol{Q}(P,\zeta)$, for some $P\in E_\ell$. Therefore $f=1$ or ℓ. But if $f=1$ then $\ell^2\mid N_p$, so $f=\ell$, and we have $\ell^2\mid N_p\ell$. Q.E.D.

It is perhaps worthwhile to note that for a prime p to split completely in $K_\ell/\boldsymbol{Q}$ for some $E_{/\boldsymbol{Q}}$, it is necessary that $p>(\ell-1)^2$ (but not sufficient). For example, $p=11$ cannot split completely in $K_5/\boldsymbol{Q}$ for all $E_{/\boldsymbol{Q}}$ (assuming $p=11$ is a good prime for E).

To calculate f we must know the index $(\mathfrak{o}:\boldsymbol{Z}[\pi])$. If $E \bmod p$ is supersingular, then the conductor of $\boldsymbol{Z}[\pi]$ is 1 or 2, so for our purpose, we can assume $E \bmod p$ is not supersingular. Then we have the following

Theorem 2. *Assume $E \bmod p$ is not supersingular. Then* $\ell\mid(\mathfrak{o}:$

$Z[\pi]) \Leftrightarrow J_\ell(X, j(E)) \equiv 0 \pmod p$ *splits into a product of linear polynomial in* $F_p[X]$, *where* $J_\ell(X, j)$ *is the modular polynomial of order* ℓ *and* $j(E)$ *is the j-invariant of* E.

Proof. First note that $J_\ell(X, j(E)) \equiv 0 \pmod p$ splits etc.$\Leftrightarrow$all elliptic curves A_i whih are ℓ-isogenous to E' can be defined over F_p (i.e. $j(A_i) \in F_p$). It is known that there is an elliptic curve E_1 defined over $k(j(\mathfrak{o}))$ (=the ring class field of k corresponding to $\mathfrak{o}$) such that E_1 has good reduction at $\mathfrak{p}$ (=a prime of $k(j(\mathfrak{o}))$ lying above p) and that $E_1 \bmod \mathfrak{p}$ $\cong E'$ (over F_p), End $(E_1) \cong$ End $(E') = \mathfrak{o}$. As $\ell \neq p$, ℓ-isogenies from E_1 and E' correspond each other under reduction. Since the conductor m of $\mathfrak{o}$ is prime to p, one can assume End (A_i) is of conductor ℓm, or m, or m/ℓ ([1] p. 20). $\Leftarrow$) Since A_i can be defined over F_p, all $\mathfrak{o}_i$ $=$End $(A_i) \supset Z[\pi]$. As at least one of $\mathfrak{o}_i$'s is of conductor ℓm, ℓ must divides $(\mathfrak{o} : Z[\pi])$. $\Rightarrow$) The condition $\ell \mid (\mathfrak{o} : Z[\pi])$ implies all $\mathfrak{o}_i \supset Z[\pi]$. Therefore by the first main theorem of complex multiplication theory [1] p. 23, p splits completely in $k(j(\mathfrak{o}_i))/Q$. As there is an elliptic curve defined over $k(j(\mathfrak{o}_i))$ which reduces to A_i modulo a prime of $k(j(\mathfrak{o}_i))$ lying above p, A_i can be defined over F_p. Hence all $j(A_i) \in F_p$. This ends the proof of our theorem.

Owing to [2], we know the explicit formula of $J_\ell(X, j)$ for $\ell = 2, 3, 5, 7$. Combining the knowledge of class equations (Fricke, Algebra Bd. 3), we can systematically exploit in some degree the complete splitting case using Theorem 2 (or rather by the relationships between the structure of End ($E \bmod p$) and F_p-isogenies).

Examples. $\ell = 3$. When $p = 7$, $a_p = -1$ gives $N_p = 3^2$, and $\pi_p = (-1 + 3\sqrt{-3})/2$. Since $j(-1 + \sqrt{-3}/2) = 0$, $p = 7$ splits completely in K_3/Q, if $j(E) \equiv 0 \pmod 7$ and $a_p = -1$. (By the way, as $j(-1 + 3\sqrt{-3}/2) = 1$, on E_1 with $j(E_1) \equiv 1 \pmod 7$ and $N_7 = 3^2$, $p = 7$ has degree 3 in K_3/Q). When $p = 67$, $a_p = 5$ gives $N_p = 3^2 7$, $\pi_p = (5 + 3^2\sqrt{-3})/2$. So assuming $a_p = 5$, when $j \equiv 0$ (maximal order) or $j \equiv 1$ (conductor 3), $p = 67$ splits completely in K_3/Q, while when $j \equiv 41, 46, 63$ (conductor 3^2; these together with $j \equiv 0$ constitute the solutions of $J_3(X, 1) \equiv 0 \bmod 67$), $p = 67$ has degree 3 in K_3/Q.

Remark. When $\ell = 2, 3$, we know the structure of K_2, K_3 well, so we can state explicitly how p splits in them. For $E : Y^2 = X^3 + AX + B$, put $\Delta = -2^4(4A^3 + 27B^2)$. Assume Gal $(K_\ell/Q) \cong \mathrm{GL}_2(Z/\ell Z)$ for $\ell = 2, 3$. Then $K_2 = Q(\sqrt{\Delta}, P_2)$, $K_3 = Q(\zeta, P_3, \sqrt[3]{\Delta})$ where $P_\ell(\neq 0) \in E_\ell$, $\zeta = (-1 + \sqrt{-3})/2$ ([5]). Hence we see p splits completely in $K_2/Q \Leftrightarrow 2 \mid N_p$, p splits in $Q\sqrt{\Delta}$); p splits completely in $K_3/Q \Leftrightarrow 3 \mid (p-1)$, $3 \mid N_p$, p is divided by a prime of absolute degree 1 in $Q(\sqrt[3]{\Delta})$. (Note that if k/Q is finite galois, k'/Q finite, both having an embedding into Q_p, and p is unramified in kk', then kk' has an embedding into Q_p.)

References

[1] M. Deuring: Die Klassenkörper der Komplexen Multiplikation. Enzyklopädie der Math. Wiss. Band I, 2. Teil, Heft 10, II (1958).

[2] O. Herrmann: Über die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$. J. Reine Angew. Math. 274/275, 187–195 (1975).

[3] S. Lang: Elliptic Functions. Addison Wesley, Reading (1973).

[4] S. Lang-J. Tate: Principal homogenous space over abelian varieties. Amer. J. Math., **80**, 659–684 (1958).

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

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

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

[8] W. C. Waterhouse: Abelian varieties over finite fields. Ann. Éc. Norm., (4), II, 521–560 (1969).