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 $N_{p^m}=\#(E \bmod p)(\boldsymbol{F}_{p^m})$ 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 $K_\ell/\boldsymbol{Q}\Leftrightarrow[\boldsymbol{Q}_p(E_\ell):\boldsymbol{Q}_p]=f\Leftrightarrow[\boldsymbol{F}_p(E'_\ell):\boldsymbol{F}_p]=f\Leftrightarrow\pi^f\equiv 1 \bmod \ell\mathfrak{o}$, $\pi^n\not\equiv 1 \bmod \ell\mathfrak{o}$ 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 $\ell^2\mid N_q$, $\ell\mid(q-1)\Leftrightarrow\ell^2\mid(a_q)^2-4q$, $a_q\equiv 2 \pmod{\ell}$. So we can write $a_q=2+\ell a$, $(a_q)^2-4q=\ell^{2s}\cdot n^2(-d)$, $a,s,n,d\in\boldsymbol{Z}$, $s>0$, $\ell\nmid n$,