Bull. Aust. Math. Soc. **86** (2012), 339–347
doi:10.1017/S0004972712000019

ON THE DISTRIBUTION OF TORSION POINTS MODULO PRIMES

YEN-MEI J. CHEN✉ **and YEN-LIANG KUAN**

(Received 31 October 2011)

Abstract

Let $\mathbb{A}$ be a commutative algebraic group defined over a number field K. For a prime $\wp$ in K where $\mathbb{A}$ has good reduction, let $N_{\wp,n}$ be the number of n-torsion points of the reduction of $\mathbb{A}$ modulo $\wp$ where n is a positive integer. When $\mathbb{A}$ is of dimension one and n is relatively prime to a fixed finite set of primes depending on $\mathbb{A}_{/K}$, we determine the average values of $N_{\wp,n}$ as the prime $\wp$ varies. This average value as a function of n always agrees with a divisor function.

2010 *Mathematics subject classification*: primary 11N13; secondary 11N45, 11R18, 11G05.

Keywords and phrases: number fields, algebraic groups, torsion points, elliptic curves, complex multiplication.

1. Introduction

Let $\mathbb{A}$ be a commutative algebraic group defined over a number field K. For a prime ideal $\wp$ in K, denote the residue field by $\mathbb{F}_\wp$. If $\mathbb{A}$ has good reduction at $\wp$, let $\tilde{\mathbb{A}}$ be the reduction of $\mathbb{A}$ modulo $\wp$. Let $N_{\wp,n}$ be the number of n-torsion points in $\tilde{\mathbb{A}}(\mathbb{F}_\wp)$, the set of $\mathbb{F}_\wp$-rational points in $\tilde{\mathbb{A}}$, where n is a positive integer. If $\mathbb{A}$ has bad reduction at $\wp$, let $N_{\wp,n} = 0$. We are interested in the average value of $N_{\wp,n}$, where $\wp$ runs through the prime ideals in K, namely the limit

$$\lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{N_{\mathbb{Q}}^K \wp \le x} N_{\wp,n},$$

where $\pi_K(x)$ is the number of primes $\wp$ with $N_{\mathbb{Q}}^K \wp \le x$. We denote this limit by $M(\mathbb{A}_{/K}, n)$.

Any commutative algebraic group of dimension one over K is either $\mathbb{G}_a$, or a torus, or an elliptic curve. For the trivial case $\mathbb{A} = \mathbb{G}_{a/K}$, the average value $M(\mathbb{G}_{a/K}, n)$ is always 1 for every n. For the simplest case $\mathbb{A} = \mathbb{G}_{m/\mathbb{Q}}$, we can show the following theorem.

Research partially supported by National Science Council, Republic of China.

Theorem 1.1. *Let $d(n)$ be the number of positive divisors of n. Then*

$$M(\mathbb{G}_{m/\mathbb{Q}}, n) = d(n).$$

Proof. The set of n-torsion points of $\mathbb{G}_{m/\mathbb{Q}}$ is exactly the set $\boldsymbol{\mu}_n$ of the nth roots of unity. Since $\mathbb{F}_p^*$ is a cyclic group of order $p-1$, $N_{p,n} = \gcd(n, p-1)$. If $n = q^s$ is a prime power, then $\gcd(q^s, p-1) = q^i$ if and only if $q^i \parallel p-1$, for all $0 \le i \le s-1$. Applying Dirichlet's theorem on primes in arithmetic progressions, the set of primes p such that $q^i \parallel p-1$ has density $1/\phi(q^i) - 1/\phi(q^{i+1})$ for each $0 \le i \le s-1$, where ϕ is the Euler function. For the case $i = s$,

$$\gcd(q^s, p-1) = q^s \quad \text{if and only if } q^s \mid p-1,$$

and therefore the set of primes p such that $\gcd(q^s, p-1) = q^s$ has density $1/\phi(q^s)$. So the average value of N_{p,q^s} is equal to $s+1$. For $n \in \mathbb{N}$, by the Möbius inversion theorem on the lattice of positive divisors of n, one can compute that

$$\begin{aligned} M(\mathbb{G}_{m/\mathbb{Q}}, n) &= \sum_{d|n} d \sum_{dd'|n} \frac{\mu(d')}{\phi(dd')} \\ &= \sum_{\substack{d,d' \\ dd'|n}} \frac{d\mu(d')}{\phi(dd')}, \end{aligned}$$

which is multiplicative. Let $n = q_1^{s_1} q_2^{s_2} \cdots q_r^{s_r}$ be the prime decomposition of n in $\mathbb{Q}$. Then

$$M(\mathbb{G}_{m/\mathbb{Q}}, n) = \prod_{j=1}^{r} (s_j + 1).$$

This concludes the proof. □

Another approach uses the action of Galois groups. Let $X = \mathbb{A}[n]$ be the set of n-torsion points of $\mathbb{A}$ and let $G = \mathrm{Gal}(K(\mathbb{A}[n])/K)$ be the Galois group of $K(\mathbb{A}[n])$ over K, where $K(\mathbb{A}[n])$ is the field obtained by adjoining to K the coordinates of n-torsion points of $\mathbb{A}$. Then G acts on X naturally. Following the ideas of [7], one can deduce the following theorem.

Theorem 1.2. *The limit $M(\mathbb{A}_{/K}, n)$ exists and it is equal to the number of orbits of G in X.*

Proof. Let

$$L = K(\mathbb{A}[n]), \quad G = \mathrm{Gal}(L/K)$$

and, for $1 \le m \le |X|$, let $G(m)$ be the set of elements $g \in G$ which have exactly m fixed points. Then $G(m)$ is a union of conjugacy classes for each m. Observe that, for a prime $\wp$ which is unramified in L, $N_{\wp,n} = m$ if and only if the Artin symbol $(\wp, L/K) \subseteq G(m)$.

https://doi.org/10.1017/S0004972712000019 Published online by Cambridge University Press

One derives

$$\begin{aligned} M(\mathbb{A}_{/K}, n) &= \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{m=1}^{|X|} \sideset{}{'}\sum_{\substack{N_{\mathbb{Q}}^K \wp \le x \\ (\wp, L/K)\subseteq G(m)}} m \\ &= \sum_{m=1}^{|X|} m \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sideset{}{'}\sum_{\substack{N_{\mathbb{Q}}^K \wp \le x \\ (\wp, L/K)\subseteq G(m)}} 1 \\ &= \sum_{m=1}^{|X|} m \frac{|G(m)|}{|G|}, \end{aligned}$$

using the Chebotarev density theorem. Here the dash means that the sum runs through primes $\wp$ which are unramified in L. Applying Burnside's lemma, the proof of the theorem is complete. □

Let us go back to the $\mathbb{G}_m$ case over an arbitrary number field K. Suppose that $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. If $n = q^s$ is a prime power, then the number of orbits of $\mathrm{Gal}(K(\zeta_{q^s})/K)$ in $\boldsymbol{\mu}_{q^s}$ is equal to $s + 1$. Applying Theorem 1.2, we have the following corollary.

Corollary 1.3. *Assume that $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. Then*

$$M(\mathbb{G}_{m/K}, n) = d(n),$$

where $d(n)$ is the number of positive divisors of n.

More generally, Corollary 1.3 can be straightforwardly extended to any one-dimensional torus $\mathbb{T}_{/K}$ over K, that is, there exists an integer constant $C_{\mathbb{T}_{/K}}$ such that the average value $M(\mathbb{T}_{/K}, n) = d(n)$ for all n prime to $C_{\mathbb{T}_{/K}}$. For the case of $\mathbb{T}_{/\mathbb{Q}}$, we can work out a precise formula for every n.

Theorem 1.4. *Let $\mathbb{T}_{/\mathbb{Q}}$ be a one-dimensional torus defined by the quadratic equation $x^2 - my^2 = 1$, where m is a square-free integer, and denote the discriminant of $\mathbb{Q}(\sqrt{m})$ by D_m. For $n \in \mathbb{N}$, denote the number of positive divisors of n by $d(n)$. Then*

$$M(\mathbb{T}_{/\mathbb{Q}}, n) = \begin{cases} d(n) + d\left(\dfrac{n}{D_m}\right) & \text{if } m < 0 \text{ and } D_m \mid n, \\ d(n) & \text{otherwise.} \end{cases}$$

In the case of elliptic curves $E_{/K}$, we have $\mathrm{Gal}(K(E[n])/K)$ acting on $E[n]$ so that

$$\phi_n : \mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

A result due to Serre [6, Section 4.2, Theorem 2] asserts that, for any elliptic curve $E_{/K}$ without complex multiplication (CM), there exists an integer constant $C_{E_{/K}}$ such that ϕ_ℓ is surjective for any prime $\ell \nmid C_{E_{/K}}$. It follows [2, Appendix] that ϕ_n is surjective

https://doi.org/10.1017/S0004972712000019 Published online by Cambridge University Press

for all n prime to $C_{E_{/K}}$. Then one computes the number of orbits of $\mathrm{Gal}(K(E[n])/K)$ in $E[n]$, which is equal to $d(n)$. Applying Theorem 1.2 again, one has the following corollary.

COROLLARY 1.5. *Let $E_{/K}$ be an elliptic curve without CM. There exists an integer constant $C_{E_{/K}}$ such that, for all n prime to $C_{E_{/K}}$,*

$$M(E_{/K}, n) = d(n),$$

where $d(n)$ is the number of positive divisors of n.

We conclude this section with the case of elliptic curves $E_{/K}$ with CM by an order in a quadratic imaginary field k. Here we are not requiring that K contains k. Denote by $d_k(n)$ the number of ideal divisors of n in k. We shall prove the following in Section 3.

THEOREM 1.6. *Let $E_{/K}$ be an elliptic curve with CM by an order in a quadratic imaginary field k. There exists an integer constant $C_{E_{/K}}$ such that, for all n prime to $C_{E_{/K}}$,*

$$M(E_{/K}, n) = \begin{cases} \frac{1}{2}(d_k(n) + d(n)) & \text{if } k \not\subseteq K, \\ d_k(n) & \text{if } k \subseteq K. \end{cases}$$

In particular, in the case of $K = \mathbb{Q}$, $C_{E_{/K}}$ may be taken to be $6\Delta_E$, where Δ_E is the discriminant of E.

REMARK. For any commutative algebraic group $\mathbb{A}_{/K}$ of dimension one and n relatively prime to finitely many primes (depending on K and $\mathbb{A}$), the average value $M(\mathbb{A}_{/K}, n)$ is given by a simple 'divisor' function from the fraction field of endomorphisms of $\mathbb{A}$. In the case of $\mathbb{G}_m$, tori $\mathbb{T}$, and elliptic curves without CM, this is the usual $d(n)$, since their fraction field of endomorphisms is $\mathbb{Q}$. In the case of elliptic curves $E_{/K}$ with CM by k, the average value $M(E_{/K}, n) = d_k(n)$, provided that $k \subseteq K$. The 'exceptional primes' in each case depend on the base field K and the places where $\mathbb{A}$ has bad reduction.

2. The case of one-dimensional tori

This section is devoted to the proof of Theorem 1.4. If $\mathbb{T}_{/\mathbb{Q}}$ is a one-dimensional torus which is not isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$, then $\mathbb{T}_{/\mathbb{Q}}$ can be defined by a quadratic equation of the form

$$x^2 - my^2 = 1,$$

where m is a square-free integer. An explicit isomorphism between $\mathbb{T}$ and $\mathbb{G}_m$, defined over $\mathbb{Q}(\sqrt{m})$, is

$$\phi : \mathbb{T} \to \mathbb{G}_m, \quad (x, y) \mapsto x + y\sqrt{m}.$$

From this isomorphism, we can compute that

$$[n](x, y) = \left(\frac{(x + y\sqrt{m})^n + (x - y\sqrt{m})^n}{2}, \frac{(x + y\sqrt{m})^n - (x - y\sqrt{m})^n}{2\sqrt{m}} \right).$$

https://doi.org/10.1017/S0004972712000019 Published online by Cambridge University Press

Observe that the multiplication by $[n]$ is a morphism defined over $\mathbb{Q}$ and the set of n-torsion points in $\mathbb{T}$ is equal to

$$\mathbb{T}[n] = \left\{ \left(\frac{\zeta_n^i + \zeta_n^{-i}}{2}, \frac{\zeta_n^i - \zeta_n^{-i}}{2\sqrt{m}} \right) : 1 \le i \le n \right\}.$$

Denote by D_m the discriminant of $\mathbb{Q}(\sqrt{m})$. We have the following lemma.

Lemma 2.1. *Let $\mathbb{T}_{/\mathbb{Q}}$ be a one-dimensional torus defined by the quadratic equation $x^2 - my^2 = 1$, where m is a square-free integer. Then the degree of $\mathbb{Q}(\mathbb{T}[n])$ over $\mathbb{Q}$ is equal to $\phi(n)/2$ if $m < 0$ and $D_m \mid n$, and it is equal to $\phi(n)$ otherwise.*

Proof. Since $\mathbb{T}[n]$ is a cyclic group, $\mathbb{Q}(\mathbb{T}[n]) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, (\zeta_n - \zeta_n^{-1})/\sqrt{m})$. Note that $((\zeta_n - \zeta_n^{-1})/\sqrt{m})^2 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and thus the degree of $\mathbb{Q}(\mathbb{T}[n])$ over $\mathbb{Q}$ is equal to $\phi(n)$ or $\phi(n)/2$. Observe that $(\zeta_n - \zeta_n^{-1})/\sqrt{m} \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ if and only if $(\zeta_n - \zeta_n^{-1})/\sqrt{m}$ is fixed by complex conjugation and $\sqrt{m} \in \mathbb{Q}(\zeta_n)$, which is equivalent to $m < 0$, and n is divisible by the discriminant of $\mathbb{Q}(\sqrt{m})$ [4, Ch. IV] □

Lemma 2.2. *Let $\mathbb{T}_{/\mathbb{Q}}$ be a one-dimensional torus defined by the quadratic equation $x^2 - my^2 = 1$, where m is a square-free integer. For $d, n \in \mathbb{N}$ with $d \mid n$, let U_d be the set of points of order d in $\mathbb{T}[n]$. Then the number of orbits of* $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ *in U_d is equal to*

$$\frac{\phi(d)}{[\mathbb{Q}(\mathbb{T}[d]) : \mathbb{Q}]},$$

where $[\mathbb{Q}(\mathbb{T}[d]) : \mathbb{Q}]$ *is the degree of* $\mathbb{Q}(\mathbb{T}[d])$ *over* $\mathbb{Q}$.

Proof. Since the restriction map $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\mathbb{T}[d])/\mathbb{Q})$ is surjective, the number of orbits of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ in U_d equals that of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[d])/\mathbb{Q})$ in U_d. Let $G = \mathrm{Gal}(\mathbb{Q}(\mathbb{T}[d])/\mathbb{Q})$. Note that the cardinality of U_d is equal to $\phi(d)$. Also note that, for each $x \in U_d$, the orbit $G \cdot x$ has cardinality equal to the order of G due to the bijection $G \to G \cdot x$ by $\sigma \mapsto x^\sigma$. Hence the number of orbits of G in U_d is equal to

$$\frac{\phi(d)}{[\mathbb{Q}(\mathbb{T}[d]) : \mathbb{Q}]}.$$

This concludes the proof. □

We are now ready to prove Theorem 1.4. Because $\mathbb{T}[n]$ is the disjoint union of U_d for all $d \mid n$ and U_d is stable under of the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$, in order to apply Theorem 1.2 we only need to compute the number of orbits of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ in U_d. For square-free integer m and positive integer d, define $\epsilon_m(d)$ by

$$\epsilon_m(d) = \begin{cases} 1 & \text{if } m < 0 \text{ and } D_m \mid d, \\ 0 & \text{otherwise.} \end{cases}$$

Combining Lemmas 2.1 and 2.2, the number of orbits of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ in U_d is equal to $1 + \epsilon_m(d)$. So the number of orbits of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ in $\mathbb{T}[n]$ is equal to $\sum_{d|n}(1+\epsilon_m(d))$. One can compute

$$\begin{aligned}\sum_{d|n}(1+\epsilon_m(d)) &= \sum_{d|n} 1 + \sum_{d|n}\epsilon_m(d)\\ &= \begin{cases} d(n) + \sum_{D_m|d|n} 1 & \text{if } m<0 \text{ and } D_m \mid n,\\ d(n) & \text{otherwise.}\end{cases}\\ &= \begin{cases} d(n) + d\Big(\dfrac{n}{D_m}\Big) & \text{if } m<0 \text{ and } D_m \mid n,\\ d(n) & \text{otherwise.}\end{cases}\end{aligned}$$

This completes the proof of Theorem 1.4.

3. The case of elliptic curves with complex multiplication

Let $E_{/K}$ be an elliptic curve over a number field K with CM by an order in a quadratic imaginary field k. Denote by O_k the ring of integers of k. It is well known that if $k \subseteq K$, there exists an integer constant $A_{E_{/K}}$ such that $\mathrm{Gal}(K(E[n])/K) \cong (O_k/nO_k)^*$ for all n prime to $A_{E_{/K}}$ (see [6, Section 4.5]).

Lemma 3.1. *Let* $\mathfrak{q}$ *be a prime in* k *with* $\gcd(\mathfrak{q}, A_{E_{/K}}) = 1$. *If* $k \subseteq K$, *then the number of orbits of* $\mathrm{Gal}(K(E[\mathfrak{q}^s])/K)$ *in* $E[\mathfrak{q}^s]$ *is equal to* $s+1$.

Proof. Since $k \subseteq K$, the endomorphism $[\mathfrak{q}^s]$ is defined over K. For each $0 \le i \le s$, let u_i be the set of elements which have order exactly $\mathfrak{q}^i$ in $E[\mathfrak{q}^s]$. Since $E[\mathfrak{q}^s]$ is a cyclic $O_k/\mathfrak{q}^sO_k$-module and $\mathrm{Gal}(K(E[\mathfrak{q}^s])/K)$ is isomorphic to $(O_k/\mathfrak{q}^s)^*$, each u_i is stable under of the Galois action and $\mathrm{Gal}(K(E[\mathfrak{q}^s])/K)$ acts transitively on u_i for each i. So the number of orbits of $\mathrm{Gal}(K(E[\mathfrak{q}^s])/K)$ in $E[\mathfrak{q}^s]$ is equal to $s+1$. □

Applying Lemma 3.1 and Theorem 1.2, we consider the prime decomposition of n in k and therefore deduce the average value $M(E_{/K}, n) = d_k(n)$ under the assumption of $k \subseteq K$, where $d_k(n)$ denotes the number of ideal divisors of n in k.

From now on, we always assume that $k \not\subseteq K$ and $\gcd(n, A_{E_{/K}}) = 1$. Let $L = Kk$ and let $\wp$ be a prime in K, which has absolute degree one (over $\mathbb{Q}$). If $\wp$ splits in L, say $\wp O_L = \mathfrak{P}_1\mathfrak{P}_2$, then $N_{\wp,n} = N_{\mathfrak{P}_i,n}$ for $i = 1, 2$, since $\mathbb{F}_\wp = \mathbb{F}_{\mathfrak{P}_i}$. So

$$\sum_{\substack{N^K_{\mathbb{Q}}\wp \le x, \deg(\wp)=1\\ \wp \text{ splits in } L}} N_{\wp,n} = \frac{1}{2}\sum_{\substack{N^L_{\mathbb{Q}}\mathfrak{P}\le x\\ \deg(\mathfrak{P})=1}} N_{\mathfrak{P},n}$$

and

$$\begin{aligned}\lim_{x\to\infty}\frac{1}{\pi_K(x)}\sum_{\substack{N^K_{\mathbb{Q}}\wp \le x\\ \wp \text{ splits in } L}} N_{\wp,n} &= \frac{1}{2}\lim_{x\to\infty}\frac{1}{\pi_L(x)}\sum_{\substack{N^L_{\mathbb{Q}}\mathfrak{P}\le x\\ \deg(\mathfrak{P})=1}} N_{\mathfrak{P},n}\\ &= \frac{1}{2}\lim_{x\to\infty}\frac{1}{\pi_L(x)}\sum_{N^L_{\mathbb{Q}}\mathfrak{P}\le x} N_{\mathfrak{P},n}.\end{aligned}$$

The second equality follows from the fact that the set of primes $\mathfrak{P}$ whose residue degree is greater than 1 in L has density 0 [4, Ch. VIII, p. 168]. Since $k \subseteq L$,

$$\lim_{x\to\infty} \frac{1}{\pi_L(x)} \sum_{N_{\mathbb{Q}}^{L}\mathfrak{P}\le x} N_{\mathfrak{P},n} = d_k(n).$$

Assume now that $\wp$ is an absolute degree-one prime which stays prime in L lying above p. Recall that, assuming that $E_{/K}$ has good reduction at $\wp$, $\wp$ stays prime in L if and only if $E_{/K}$ has supersingular reduction at $\wp$ [8, Ch. II, p. 184]. Adapting the proof of Theorem 1.1 in [5], one can conclude the following lemma.

Lemma 3.2. *Let $E_{/K}$ be an elliptic curve over a number field K with CM by an order in a quadratic imaginary field k and $\wp$ an absolute degree-one prime in K lying above p. Assume that $E_{/K}$ has good reduction at $\wp$. Suppose that $k \not\subseteq K$ and $E_{/K}$ has supersingular reduction (mod $\wp$). Then the odd part of $\tilde{E}(\mathbb{F}_\wp)$ is cyclic and $\#\tilde{E}(\mathbb{F}_\wp) = p + 1$.*

Proof. If $\tilde{E}(\mathbb{F}_\wp)$ contains a subgroup of type (ℓ, ℓ) for some prime ℓ, then this subgroup is contained in the set of fixed points of the Frobenius endomorphism $\pi_\wp$. Since $\ker[\ell] \subseteq \ker(\pi_\wp - 1)$, there is an endomorphism $h : \tilde{E} \to \tilde{E}$ such that $(\pi_\wp - 1) = h \circ [\ell]$, and one deduces that $(\pi_\wp - 1)/\ell$ is an algebraic integer. Let $L = Kk$ and $\mathfrak{P}$ a prime in L lying above $\wp$. Since $E_{/K}$ has supersingular reduction modulo $\wp$, $\wp$ stays prime in L and $\wp O_L = \mathfrak{P}$. From the CM theory, the Frobenius endomorphism $\pi_{\mathfrak{P}} = [-p]$, via $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\tilde{E})$ [8, Ch. II, Proposition 4.4]. Since $\pi_{\mathfrak{P}} = \pi_\wp^2$, $\pi_\wp = \pm\sqrt{-p}$. But $(\pm\sqrt{-p} - 1)/\ell$ is never an algebraic integer, if $\ell > 2$. Hence the odd part of $\tilde{E}(\mathbb{F}_\wp)$ is cyclic. Since $\wp$ is an absolute degree-one prime and $E_{/K}$ has supersingular reduction modulo $\wp$, $\#\tilde{E}(\mathbb{F}_\wp) = p + 1$. □

From Lemma 3.2, $N_{\wp,n} = \gcd(n, p + 1)$. Suppose that n is odd and $L \cap \mathbb{Q}(\zeta_n)$ is equal to $\mathbb{Q}$. For $d \mid n$, write

$$C_1 = \{\sigma \in \mathrm{Gal}(L/K) : \sigma|_L \neq id\},$$
$$C_d = \{\sigma \in \mathrm{Gal}(L(\zeta_d)/K) : \sigma|_L \neq id \text{ and } \sigma|_{K(\zeta_d)} \text{ is of order two}\}, \quad \text{if } d > 1.$$

Note that $\#C_d = 1$ for all $d \mid n$. Observe that for $d \mid n$ and $d > 1$, $d \mid p + 1$ if and only if the Artin symbol $(\wp, K(\zeta_d)/K)$ has order two. So $\wp$ stays prime in L and $d \mid p + 1$ if and only if the Artin symbol $(\wp, L(\zeta_d)/K) \subseteq C_d$.

For $d \mid n$, write

$$S_d = \{\wp : \wp \text{ stays prime in } L, \text{ absolute degree one and } \gcd(n, p + 1) = d\},$$
$$T_d = \{\wp : \wp \text{ stays prime in } L, \text{ absolute degree one and } d \mid p + 1\}.$$

Applying the Chebotarev density theorem, the density of T_d can be given by

$$\mathrm{den}(T_d) = \frac{\#C_d}{[L(\zeta_d) : K]} = \frac{1}{2\phi(d)}.$$

https://doi.org/10.1017/S0004972712000019 Published online by Cambridge University Press

Since T_d is equal to the disjoint union of $S_{dd'}$ for all d' dividing n/d,

$$\mathrm{den}(T_d) = \sum_{d'|n/d} \mathrm{den}(S_{dd'}).$$

This implies that

$$\mathrm{den}(S_d) = \sum_{d'|n/d} \mu(d')\, \mathrm{den}(T_{dd'}) = \sum_{d'|n/d} \frac{\mu(d')}{2\phi(dd')}.$$

Since

$$\begin{aligned}\sum_{\wp \text{ stays prime in } L}{}' N_{\wp,n} &= \sum_{\wp \text{ stays prime in } L}{}' \gcd(d, p+1)\\ &= \sum_{d|n} d \cdot \#\{\wp \in S_d : N_{\mathbb{Q}}^{K}\wp \le x\},\end{aligned}$$

where the dash means that the sum runs through all absolute degree-one primes $\wp$ with $N_{\mathbb{Q}}^{K}\wp \le x$ in K, we can write

$$\begin{aligned}\lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{\substack{N_{\mathbb{Q}}^{K}\wp \le x\\ \wp \text{ stays prime in } L}} N_{\wp,n} &= \sum_{d|n} d \cdot \mathrm{den}(S_d)\\ &= \sum_{\substack{d,d'\\ dd'|n}} \frac{d\mu(d')}{2\phi(dd')}\\ &= \frac{1}{2} d(n).\end{aligned}$$

The last equality follows from the proof of Theorem 1.1.

Set $C_{E_{/K}} = 2 \cdot A_{E_{/K}} \cdot \mathrm{disc}(L)$, where $\mathrm{disc}(L)$ denotes the discriminant of L. In the case of $E_{/\mathbb{Q}}$ with CM by k, one can simply choose $C_{E_{/\mathbb{Q}}} = 6\Delta_E$, where Δ_E is the discriminant of E, since $\mathrm{Gal}(k(E[n])/k)$ is isomorphic to $(O_k/nO_k)^*$ for all n prime to $6\Delta_E$ (see [1, Lemma 5] and [3, Theorem 2]). We conclude the proof of Theorem 1.6.

Acknowledgements

This joint work was motivated by Professor Serre's lectures at the National Center for Theoretical Sciences (Hsinchu, Taiwan) in 2009. The authors are grateful to Professor Winnie Wen-Ching Li for arranging Professor Serre's visit and all related activities. The authors would also like to thank the referee for helpful suggestions.

References

[1] J. Coates and A. Wiles, 'On the conjecture of Birch and Swinnerton-Dyer', *Invent. Math.* **39** (1977), 223–251.

[2] A. C. Cojocaru, 'On the surjectivity of the Galois representations associated to non-CM elliptic curves', *Canad. Math. Bull.* **48**(1) (2005), 16–31.

[3] R. Gupta, 'Ramification in the Coates-Wiles tower', *Invent. Math.* **81** (1985), 59–69.
[4] S. Lang, *Algebraic Number Theory* (Springer, Berlin, 1994).
[5] M. R. Murty, 'On the supersingular reduction of elliptic curves', *Proc. Indian Acad. Sci. Math. Sci.* **97** (1987), 247–250.
[6] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15** (1972), 259–331.
[7] J.-P. Serre, 'On a theorem of Jordan', *Bull. Amer. Math. Soc. (N.S)* **40**(4) (2003), 429–440.
[8] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* (Springer, Berlin, 1994).

YEN-MEI J. CHEN, Department of Mathematics, National Central University, Jhongli City, Taoyuan County 32001, Taiwan
e-mail: ymjchen@math.ncu.edu.tw

YEN-LIANG KUAN, Department of Mathematics, National Central University, Jhongli City, Taoyuan County 32001, Taiwan
e-mail: 952201001@cc.ncu.edu.tw

https://doi.org/10.1017/S0004972712000019 Published online by Cambridge University Press