POSITIVITY OF CONSTANTS RELATED TO ELLIPTIC CURVES

KIM, SUNGJIN

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. It is known that the structure of the reduction $E(\mathbb{F}_p)$ is

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}. \tag{1}$$

with $d_p|e_p$. The constant

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]}$$

appears as the density of primes p with good reduction for E and $d_p = j$ (Under the GRH in the non-CM case, unconditionally in the CM case). We give appropriate conditions for this constant to be positive when $j > 1$.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$, and p be a prime of good reduction for E. Denote $E(\mathbb{F}_p)$ by the group of $\mathbb{F}_p$-rational points of E. It is known that the structure of $E(\mathbb{F}_p)$ is

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}. \tag{2}$$

with $d_p|e_p$. The cyclicity problem asks for the density of primes p of good reduction for E such that $d_p = 1$. We exclude the degenerate case $\mathbb{Q}(E[2]) = \mathbb{Q}$, where we have $C_E = 0$ trivially. Thus, all the works cited below are under the assumption $\mathbb{Q}(E[2]) \neq \mathbb{Q}$.

Let N be the conductor of the elliptic curve E and denote $\mathfrak{f}(x, E)$ by the number of primes p of good reduction for E such that $d_p = 1$. A. Cojocaru and M. R. Murty (see [CM]) obtained that if E does not have complex multiplication(non-CM curves), then

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_N(x^{5/6}(\log x)^{2/3}),$$

under the Generalized Riemann Hypothesis(GRH) for the Dedekind zeta functions of division fields. For elliptic curves with complex multiplication(CM curves), they obtained

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_N(x^{3/4}(\log Nx)^{1/2}),$$

under the GRH. Unconditional error term in CM case is $O(x \log x)^{-A}$ for any positive A. Precisely, A. Akbary and V. K. Murty (see [AM]) obtained

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_{A,B}(x(\log x)^{-A}),$$

for any positive constant A, B, and the $O_{A,B}$ is uniform for $N \leq (\log x)^B$. Here, $C_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$.

A. Cojocaru (see [C]) obtained the density of primes p of good reduction for E such that $d_p = j$ for $j > 1$. It is

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]},$$

under the GRH for the Dedekind zeta functions of division fields. For CM curves, it can be shown unconditionally. Denote by $A(E)$ the associated Serre's constant for the elliptic curve E, which has the property:

If $(k, A(E)) = 1$, then the Galois representation:

$$\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/k\mathbb{Z}) \text{ is surjective.}$$

The positivity of C_E in non-CM case is achievable under the GRH, and it can be done unconditionally in CM case. However, it was not known whether $C_{E,j} > 0$ for some $j > 1$. In this note, we obtain the positivity under appropriate conditions.

Theorem 1.1. *Let E be a non-CM elliptic curve over $\mathbb{Q}$, and N the conductor of E. Let $A(E)$ be the associated Serre's constant. Suppose also that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Let $j > 1$ be an integer satisfying $(j, 2NA(E)) = 1$. Then $C_{E,j} > 0$ under the GRH for the division fields.*

The prime 2 requires a special care, for an elliptic curve $y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$, let K_2 be a quadratic or cubic subfield of $\mathbb{Q}(E[2])$. Precisely, K_2 is defined as follows,

$$K_2 = \begin{cases} \mathbb{Q}(\sqrt{-4a^3 - 27b^3}) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 2, \text{ or } 6 \\ \mathbb{Q}(\alpha) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 3. \end{cases}$$

where α is a root of $x^3 + ax + b = 0$ in $\overline{\mathbb{Q}}$.

Theorem 1.2. *Let E be an elliptic curve over $\mathbb{Q}$ which has CM by the full ring of integers $\mathcal{O}_K$ in an imaginary quadratic field K. Let N be the conductor of E. Suppose that $K_2 \neq K$. Let $(j, 6N) = 1$. Then $C_{E,j} > 0$.*

2. Preliminaries

We generalize a certain properties of Euler Totient function ϕ.

Definition 2.1. *We call a function $f : \mathbb{N} \longrightarrow \mathbb{C}$* **multiplicative function of ϕ-type** *if there is a fixed arithmetic function g and a number $N > 0$ such that*

$$f(n) = n^N \prod_{p|n} g(p).$$

Example 2.1. *The Euler's Totient function:*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Example 2.2. *The cardinality of the group $GL(2, \mathbb{Z}/n\mathbb{Z})$:*

$$\psi(n) = n^4 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)$$

Example 2.3. *The analogue of the Euler's Totient function for a quadratic field K:*

$$\Phi(n) = \left|(\mathcal{O}_K/n\mathcal{O}_K)^\times\right| = n^2 \prod_{p|n} g(p),$$

where

$$g(p) = \begin{cases} 1 - \frac{1}{p^2} & \textit{if } p \textit{ is inert in } K \\ \left(1 - \frac{1}{p}\right)^2 & \textit{if } p \textit{ splits in } K \\ 1 - \frac{1}{p} & \textit{if } p \textit{ ramifies in } K \end{cases}$$

If f is a multiplicative function of ϕ-type, then it satisfies

$$f([m,n])f((m,n)) = f(m)f(n).$$

The following lemmas are well-known facts about Galois representation of elliptic curves. They can be found in [S], also in [S2], see also [S3], and well-summarized in [K]. For the CM case, we refer to [D].

Lemma 2.1 (Serre)**.** *If E is non-CM curve, then there exists $A(E)$ such that*

$$Gal(\mathbb{Q}(E[k])/\mathbb{Q}) \simeq GL(2, \mathbb{Z}/k\mathbb{Z})$$

if $(k, A(E)) = 1$. Moreover, $\mathbb{Q}(\zeta_k)$ is the maximal abelian subextension in $\mathbb{Q}(E[k])$.

Lemma 2.2 (Deuring)**.** *If E has CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K and N be the conductor, then*

$$Gal(K(E[k])/K) \simeq (\mathcal{O}_K/k\mathcal{O}_K)^\times$$

if $(k, 6N) = 1$.

3. Proof of Theorem 1.1

By the argument given in [FK, Chapter 7], together with open image theorem by Serre, we have the following proposition with some $m(E) \in \langle 2A(E)\rangle = \{n \in \mathbb{Z} : p|n \Rightarrow p|2A(E)\}$ when E does not have CM. Let $G_k = \mathrm{Gal}(\mathbb{Q}(E[k]) : \mathbb{Q})$, and denote by m_p the maximal power of p for a prime $p|m(E)$. Similarly, let k_p be the maximal power of p that divides k. Then we have the following information about the size of G_k.

Proposition 3.1. *Let $k = hj$ with $h \in \langle m(E) \rangle = \{h : p|h \Rightarrow p|m(E)\}$, and $(j, m(E)) = 1$. Then $|G_k| = |G_h||G_j|$, and with $h_1 = (h, m(E))$, we have*

$$|G_h| = |G_{h_1}| \prod_{\substack{p^{k_p}||h \\ k_p > m_p}} p^{4(k_p - m_p)}.$$

Further, $|G_j| = \psi(j)$, and hence

$$|G_k| = |G_{h_1}| \psi(j) \prod_{\substack{p^{k_p}||h \\ k_p > m_p}} p^{4(k_p - m_p)}.$$

Corollary 3.1. *Let E be a non-CM elliptic curve. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} = \left(\sum_{k \in \langle 2NA(E) \rangle} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \right) \prod_{p \nmid 2NA(E)} \left(1 - \frac{1}{\psi(p)} \right).$$

For $j > 1$ with $(j, 2NA(E)) = 1$, similar formula holds true,

Corollary 3.2. *Let E be a non-CM elliptic curve. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}(E[j])]} = \left(\sum_{k \in \langle 2NA(E) \rangle} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \right) \prod_{p \nmid 2NA(E)} \left(1 - \frac{\psi(j)}{\psi(jp)} \right).$$

Proof. If $k \in \langle 2A(E) \rangle$ and $(2A(E), m) = 1$, then $|G_{jkm}| = |G_k||G_{jm}|$. Thus, $|G_{jkm}|/|G_j| = |G_k||G_{jm}|/|G_j|$. Since ψ is a multiplicative function of ϕ-type, we have $m \mapsto |G_{jm}|/|G_j|$ is a multiplicative function from positive integers coprime to $2A(E)$. □

Thus, positivity of $\sum \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$ is equivalent to positivity of $\sum \frac{\mu(k)}{[\mathbb{Q}(E[jk]):\mathbb{Q}]}$ when $(j, 2NA(E)) = 1$. On the other hand, positivity of former one follows from [CM, Theorem 1.1]. Therefore, we have Theorem 1.1.

4. Proof of Theorem 1.2

Let E be an elliptic curve over $\mathbb{Q}$ with CM by the full ring of integers $\mathcal{O}_K$ in an imaginary quadratic field K. First, notice that

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}(E[j])][\mathbb{Q}(E[j]) : \mathbb{Q}]}.$$

We prove positivity of $C_{E,j}[\mathbb{Q}(E[j]) : \mathbb{Q}]$.

Since $(j, 6N) = 1$, we know that $\mathbb{Q}(E[j])$ contains K (see [M, Lemma 6, p 165]). Proving positivity of $C_{E,j}[\mathbb{Q}(E[j]) : \mathbb{Q}]$ is equivalent to proving that of

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[jk]) : K(E[j])]}.$$

We now regard E as an elliptic curve defined over K. Consider a prime ideal $\mathfrak{p}$ of a good reduction for E. Then the structure of reduction modulo $\mathfrak{p}$ is:

$$\mathbb{Z}/d_1(\mathfrak{p})\mathbb{Z} \oplus \mathbb{Z}/d_2(\mathfrak{p})\mathbb{Z},$$

where $d_1(\mathfrak{p})|d_2(\mathfrak{p})$.

The following is essential toward our proof of Theorem 1.2.

Theorem 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ with CM by the full ring of integers $\mathcal{O}_K$ in an imaginary quadratic field K. Then*

$$|\{N\mathfrak{p} \leq x : E \text{ has a good reduction at } \mathfrak{p}, d_1(\mathfrak{p}) = 1\}| \gg \frac{x}{\log^2 x}.$$

We quote a lemma from sieve theory (see [GM, Lemma 3]). We need to include one more congruence condition on the primes p required in the lemma.

Lemma 4.1 (Gupta, Murty)**.** *Let $S_\epsilon(x)$ be the set of primes $p \leq x$ such that all odd prime divisors of $p-1$ are distinct and $\geq x^{\frac{1}{4}+\epsilon}$, p does not split completely in the field K_2, p splits completely in the imaginary quadratic CM field K, and E has good reduction at p. Then if $K_2 \neq \mathbb{Q}$ there is an $\epsilon > 0$ such that $|S_\epsilon(x)| \gg x/\log^2 x$.*

Proof of Theorem 4.1. Note that the number of primes $\mathfrak{p}$ in K with $N\mathfrak{p} \leq x$ that lie above p, and p is inert in K, is $O(\frac{\sqrt{x}}{\log x})$. We are now ready to prove Theorem 1.2. We enumerate prime ideals $\mathfrak{p}$ in K with $N\mathfrak{p} \leq x$ such that $N\mathfrak{p} = p \in S(a,x) := \{p \in S_\epsilon(x) | a_p = a\}$ and $d_1(\mathfrak{p}) > 1$. Then there exists an odd prime q such that $q^2 | N\mathfrak{p} + 1 - a_\mathfrak{p} = p + 1 - a_p$. Since p splits completely in K, p splits completely in $\mathbb{Q}(E[q])$, consequently in $\mathbb{Q}(\zeta_q)$. Thus $p \equiv 1 \pmod{q}$. We follow the proof of [GM, Lemma 3]. Then it follows that

$$|\{\mathfrak{p} : N\mathfrak{p} = p \in S_\epsilon(x)\} \cap \{N\mathfrak{p} \leq x : E \text{ has a good reduction at } \mathfrak{p}, d_1(\mathfrak{p}) \neq 1\}| \ll x^{1-2\epsilon}.$$

By the above and Lemma 4.1, Theorem 4.1 now follows. □

The following proposition is proved in [CM].

Proposition 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ which has CM by $\mathcal{O}_K$. Then we have*

$$C_E \geq \frac{1}{2}$$

if $K \subseteq \mathbb{Q}(E[2])$. On the other hand,

$$C_E \geq \frac{1}{4}$$

if $K \nsubseteq \mathbb{Q}(E[2])$.

We provide an alternative proof of this proposition based on our theory. In fact, we have

$$C_E = \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[k]) : K]}$$

if $K \subseteq \mathbb{Q}(E[2])$. This is because $2[K(E[k]):K] = 2[\mathbb{Q}(E[k]):K] = [\mathbb{Q}(E[k]):\mathbb{Q}]$ for all $k \geq 2$. On the other hand,

$$C_E = \frac{1}{2} - \frac{1}{2[K(E[2]):K]} + \frac{1}{2}\sum_{k=1}^{\infty}\frac{\mu(k)}{[K(E[k]):K]}$$

if $K \not\subseteq \mathbb{Q}(E[2])$. This case yields $2[K(E[k]):K] = 2[\mathbb{Q}(E[k]):K] = [\mathbb{Q}(E[k]):\mathbb{Q}]$ only for $k \geq 3$. Since $E[2]$ is not rational over $\mathbb{Q}$, we see that $[K(E[2]):K] = [\mathbb{Q}(E[2]):\mathbb{Q}] \geq 2$ in this case. Moreover,

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{[K(E[k]):K]} \geq 0$$

because the density of prime ideals $\mathfrak{p}$ such that $N\mathfrak{p} \leq x$, $d_1(\mathfrak{p}) = 1$, and E has a good reduction at $\mathfrak{p}$ must be nonnegative. (Here, GRH is not necessary, see [M, page 164-165] for details.)

Let $[K(E[k]):K] = |G_k|$ where G_k is the image under the following Galois representation,

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[k]) \simeq (\mathcal{O}_K/k\mathcal{O}_K)^*$$

As in [FK, Chapter 7], we adopt the same idea in the CM case. We have a homomorphism of groups

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow G := \prod_{l:\text{primes in } K}(\mathcal{O}_{K,l})^*$$

There is natural projection $\pi_k : G \longrightarrow (\mathcal{O}_K/k\mathcal{O}_K)^*$ for each k.
Let $\Gamma_k = \mathrm{Ker}(\pi_k)$. Then $H := \rho(\mathrm{Gal}(\overline{K}/K))$ has a finite index in G by Serre's open image theorem. The image of the composition $\pi_k \circ \rho$ is isomorphic to G_k, hence by the first isomorphism theorem,

$$H/H \cap \Gamma_k \simeq G_k.$$

The analogue of the claim in [FK, Chapter 7, page 24] in the CM case, is as follows:
They take m to be the smallest positive integer that $\Gamma_m < H$, but m does not have to be the smallest with the property. Instead, we can take $m \in \langle 6N\rangle := \{h : p|h \Rightarrow p|6N\}$. Write $m = \prod_{p|m} p^{m_p}$, $k = \prod_{p|k} p^{k_p}$.
Claim: If $k_p \geq m_p$ for some p and $a \geq 1$, then

$$|H/H \cap \Gamma_{p^a k}| = |H/H \cap \Gamma_k| \cdot |\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}|$$

Moreover, if $k_p = 0$, we have $|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = |\Gamma_1/\Gamma_{p^a}| = \Phi(p^a)$, and if $k_p > 0$, then

$$|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = |\Gamma_p/\Gamma_{p^2}|^a = p^{2a}.$$

From this claim, we obtain that

Proposition 4.2. *Let $k = hj$ with $h \in \langle m \rangle := \{h : p|h \Rightarrow p|m\}$, and $(j, m) = 1$. Then $|G_k| = |G_h||G_j|$, and with $h_1 = (h, m)$, we have*

$$|G_h| = |G_{h_1}| \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{2(\nu_p - m_p)}.$$

Further, $|G_j| = \Phi(j)$, and hence

$$|G_k| = |G_{h_1}|\Phi(j) \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{2(\nu_p - m_p)}.$$

Applying methods shown in [FK, Chapter 7] to CM case, we have

Corollary 4.1. *Let E be an elliptic curve that has CM by $\mathcal{O}_K$. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{|G_k|} = \left(\sum_{k \in \langle 6N \rangle} \frac{\mu(k)}{|G_k|} \right) \prod_{p \nmid 6N} \left(1 - \frac{1}{\Phi(p)} \right).$$

For $j > 1$ with $(j, 6N) = 1$, similar formula holds true,

Corollary 4.2. *Let E be an elliptic curve that has CM by $\mathcal{O}_K$. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[jk]) : K(E[j])]} = \left(\sum_{k \in \langle 6N \rangle} \frac{\mu(k)}{|G_k|} \right) \prod_{p \nmid 6N} \left(1 - \frac{\Phi(j)}{\Phi(jp)} \right).$$

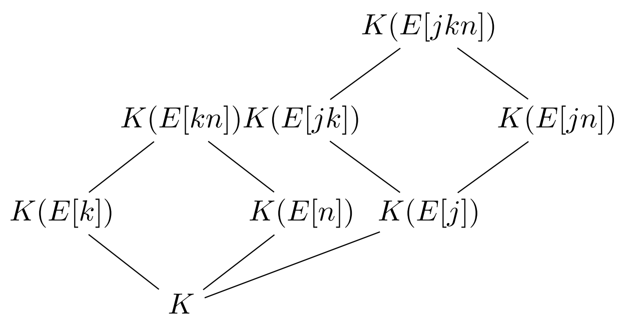

FIGURE 1. CM Case Illustration

Proof of Corollary 4.2. If $k \in \langle 6N \rangle$ and $(6N, n) = 1$, then $|G_{jkn}| = |G_k||G_{jn}|$. Thus, $|G_{jkn}|/|G_j| = |G_k||G_{jn}|/|G_j|$. Since Φ is a multiplicative function of ϕ-type, we have $n \mapsto |G_{jn}|/|G_j|$ is a multiplicative function from positive integers coprime to $6N$. $\square$

These corollaries show that positivity of any one of the constants mentioned, would provide positivity of the other. The LHS of Corollary 4.1 represents the density of prime ideals $\mathfrak{p}$ such that $N\mathfrak{p} \leq x$, E has a good reduction at $\mathfrak{p}$, and $d_1(\mathfrak{p}) = 1$. This density must be positive because of Theorem 4.1, otherwise the number of the prime ideals above would be $O(\frac{x}{\log^3 x})$ (by taking $A = 3$ in [AM]) which contradicts Theorem 4.1.

References

[AM] A. Akbary, K. Murty, *Cyclicity of CM Elliptic Curves Mod p*, Indian Journal of Pure and Applied Mathematics, 41 (1) (2010), 25-37

[C] A. Cojocaru, *Questions About the Reductions Modulo Primes of an Elliptic Curve*, Centre de Recherches Mathematiques CRM Proceedings and Lecture Notes Volume 36, 2004

[CM] A. Cojocaru, M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linniks problem*, Math. Ann. 330, 601.625 (2004)

[D] M. Deuring, *Die KlassenKörper der Komplexen Multiplikation*, Enz. Math. Wiss., Band 1-2, Heft 10, Teil II. Stuttgart: Teubner 1958.

[FK] T. Freiberg, P. Kurlberg, *On the Average Exponent of Elliptic Curves Modulo p*, Int Math Res Notices 2013 : rns280v1-29

[GM] R. Gupta, M. R. Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. 101, 225-235, 1990

[K] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. 21 (2006), 19-114.

[M] R. Murty, *On Artin's Conjecture*, Journal of Number Theory, Vol 16, no.2, April 1983

[S] J-P. Serre, *Abelian L-Adic Representations and Elliptic Curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 0263823

[S2] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications mathématiques de l'I.H.É.S., tome 54(1981), p. 123-201.

[S3] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.*, Inventiones mathematicae volume 15; pp. 259 - 331