COMPUTING LOCAL CONSTANTS FOR CM ELLIPTIC CURVES

SUNIL CHETTY AND LUNG LI

Abstract. Let E/k be an elliptic curve with CM by $\mathcal{O}$. We determine a formula for (a generalization of) the arithmetic local constant of [4] at almost all primes of good reduction. We apply this formula to the CM curves defined over $\mathbb{Q}$ and are able to describe extensions $F/\mathbb{Q}$ over which the $\mathcal{O}$-rank of E grows[1].

1. Introduction

Let p be an odd rational prime. Let $k \subset K \subset L$ be a tower of number fields, with K/k quadratic, L/K p-power cyclic, and L/k Galois with a dihedral Galois group, i.e. a lift of $1 \neq c \in \mathrm{Gal}(K/k)$ acts by conjugation on $g \in \mathrm{Gal}(L/K)$ as $cgc^{-1} = g^{-1}$. In [4] Mazur and Rubin define arithmetic local constants δ_v, one for each prime v of K, which describe the growth in $\mathbb{Z}$-rank[1] of E over the extension L/K. Specifically (cf. [4, Theorem 6.4]), for $\chi : \mathrm{Gal}(L/K) \hookrightarrow \bar{\mathbb{Q}}^\times$ an injective character and S a set of primes containing all primes above p, all primes ramified in L/K, and all primes where E has bad reduction,

$$\mathrm{rank}_{\mathbb{Z}[\chi]} E(L)^\chi - \mathrm{rank}_{\mathbb{Z}} E(K) \equiv \sum_{v \in S} \delta_v \pmod{2}. \tag{1.1}$$

In [1], the theory of arithmetic local constants is generalized to address the $\mathcal{O}$-rank of varieties with complex multiplication (CM) by an order $\mathcal{O}$, and we continue in that direction with specific attention to the elliptic curve case. Following [1], we assume that $\mathcal{O} \subset \mathrm{End}_K(E)$ is the maximal order in a quadratic imaginary field $\mathbb{K}$, p is unramified in $\mathcal{O}$, and $\mathcal{O}^c = \mathcal{O}^\dagger = \mathcal{O}$ where † indicates the action of the Rosati involution (see [5, §I.14]).

Our present aim is to provide a simple formula for the local constants δ_v (see Definition 2.2) for primes $v \nmid p$ of good reduction. We then will use a result ([1, §6]) which generalizes (1.1), with $\mathbb{Z}$ replaced by $\mathcal{O}$, to determine conditions under which the $\mathcal{O}$-rank of E will grow. In §3 we will describe, via class field theory, dihedral extensions $F/\mathbb{Q}$ which satisfy those conditions, in order to give some concrete setting to the results of §2.

Date: November 3, 2010.

A portion of this work was completed as part of the second author's undergraduate capstone research project at Colorado College.

[1]To phrase their result this way, we must assume the Shafarevich-Tate Conjecture, and we will keep this assumption in the background throughout. Without this assumption all statements regarding $\mathcal{O}$-rank of E would be replaced by analogous statements regarding $\mathcal{O} \otimes \mathbb{Z}_p$-corank of the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ of E.

2. Computing the local constant

Let $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ as p is unramified[2] in $\mathcal{O}$. We denote $R = \mathcal{O}/p\mathcal{O}$ and $R_i = \mathcal{O}/\mathfrak{p}_i$ for $i = 1, 2$, so that $R \cong R_1 \oplus R_2$.

Definition 2.1. If M is an $\mathcal{O}$-module of exponent p, define the R-rank of M by

$$\mathrm{rank}_R M := (\mathrm{rank}_{R_1} M \otimes_R R_1, \mathrm{rank}_{R_2} M \otimes_R R_2).$$

The following definition is as in [1] and [4]. Fix a prime v of K and let u and w be primes of k below v and of L above v, respectively. Denote k_u, K_v, and L_w for the completions of k, K, and L at u, v, and w, respectively. If $L_w \neq K_v$, let L'_w be the extension of K_v inside L_w with $[L_w : L'_w] = p$, and otherwise let $L'_w = L_w = K_v$.

Definition 2.2. Define the arithmetic local constant $\delta_v := \delta(v, E, L/K)$ by

$$\delta_v \equiv \mathrm{rank}_R E(K_v)/(E(K_v) \cap N_{L_w/L'_w} E(L_w)) \pmod 2.$$

Now, we will consider primes v of K such that E has good reduction at v, $v \nmid p$, $v^c = v$, and v ramifies in L/K (corresponding to Lemma 6.6 of [4]). Under these conditions Theorem 5.6 of [4] shows that

$$\dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap N_{L_w/L'_w} E(L_w)) \equiv \dim_{\mathbb{F}_p} E(K_v)[p] \pmod 2. \tag{2.1}$$

Proposition 2.4 below shows that we are able to replace $\dim_{\mathbb{F}_p}$ by rank_R in (2.1). We first need Lemma 2.3, which follows Lemmas 5.4-5.5 of [4], and our proof is meant only to address the change from $\dim_{\mathbb{F}_p}$ to rank_R.

Let $\mathcal{K}$ and $\mathcal{L}$ be finite extensions of $\mathbb{Q}_\ell$, with $\ell \neq p$, and suppose $\mathcal{L}/\mathcal{K}$ is a finite extension.

Lemma 2.3. *Suppose $\mathcal{L}/\mathcal{K}$ is cyclic of degree p, E is defined over $\mathcal{K}$ and has good reduction.*

(i) *$\mathrm{rank}_R E(\mathcal{K})/pE(\mathcal{K}) = \mathrm{rank}_R E(\mathcal{K})[p]$.*

(ii) *If $\mathcal{L}/\mathcal{K}$ is ramified then $E(\mathcal{K})/pE(\mathcal{K}) = E(\mathcal{L})/pE(\mathcal{L})$ and*

$$N_{\mathcal{L}/\mathcal{K}} E(\mathcal{L}) = pE(\mathcal{K}).$$

(iii) *If $\mathcal{L}/\mathcal{K}$ is unramified then $N_{\mathcal{L}/\mathcal{K}} E(\mathcal{L}) = E(\mathcal{K})$.*

Proof. When $\ell \neq p$ we have $E(\mathcal{K})/pE(\mathcal{K}) = E(\mathcal{K})[p^\infty]/pE(\mathcal{K})[p^\infty]$. Since $E(\mathcal{K})[p^\infty]$ is finite, (i) follows from the exact sequence of $\mathcal{O}$-modules

$$0 \to E(\mathcal{K})[p] \to E(\mathcal{K})[p^\infty] \to pE(\mathcal{K})[p^\infty] \to 0.$$

The content of (ii) and (iii) is on the level of sets, so the proof is exactly as in Lemma 5.5 of [4]. □

We return to the notation of Definition 2.2.

Proposition 2.4. *If $v \nmid p$ and L_w/K_v is nontrivial and totally ramified, then*

$$\delta_v \equiv \mathrm{rank}_R E(K_v)[p] \pmod 2.$$

Proof. As in [4], Lemma 2.3(ii) yields $E(K_v) \cap pE(L'_w) = pE(K_v)$. So by Definition 2.2 and Lemma 2.3(i)

$$\delta_v \equiv \mathrm{rank}_R E(K_v)/pE(K_v) \equiv \mathrm{rank}_R E(K_v)[p] \pmod 2.$$

□

[2] The simpler case of p being inert in $\mathbb{K}/\mathbb{Q}$, i.e. $\mathcal{O}/p\mathcal{O}$ is a field, is treated similarly.

Now, fix a prime v of K. We denote κ_u for the residue field of k_u, $q = \#\kappa_u$ for the size of finite field κ_u, and $\tilde{E}$ for the reduction of E to κ_u.

Proposition 2.5. *Suppose $v \nmid p$, v is ramified in L/K, and $v^c = v$. If E has good reduction at v, then $\Big(\delta_v \equiv 1 \;\Leftrightarrow\; p \mid \#\tilde{E}(\kappa_u).\Big)$*

Proof. We follow the notation of Lemma 6.6 of [4]. Since $v^c = v$ we know that K_v/k_u is quadratic, and it is unramified by Lemma 6.5(ii) of [4]. Let Φ be the Frobenius generator of $\mathrm{Gal}(K_v^{ur}/k_u)$, so Φ^2 is the Frobenius of $\mathrm{Gal}(K_v^{ur}/K_v)$.

The proof of Lemma 6.6 of [4] shows that the product of the eigenvalues α, β of Φ is -1. Also, they show that (as sets) $E(K_v)[p] = E[p]^{\Phi^2=1}$ is equal to $E[p]$ or is trivial depending on whether or not $\{\alpha, \beta\} = \{1, -1\}$, respectively. Since E has CM by $\mathcal{O}$, $E[p]$ is a rank 1 R-module (see e.g. [7, §II.1]), so the former case yields

$$\delta_v \equiv \mathrm{rank}_R E(K_v)[p] = 1.$$

By assumption $v \nmid p$, so p is prime to the characteristic of κ_u, and therefore the reduction map restricted to p-torsion is injective ([6, §VII.3]). We also know $E[p]$ is unramified ([6, §VII.4]), and so the eigenvalues of Φ acting on $E[p]$ coincide $\pmod p$ with the eigenvalues of the q-power Frobenius map φ_q on $\tilde{E}[p]$. We know ([6, §V]) that the characteristic polynomial of φ_q is $T^2 - aT + q$, where $a = q + 1 - \#\tilde{E}(\kappa_u)$, and from the above comments $q \equiv -1 \pmod p$. Therefore, Φ having eigenvalues ± 1 is equivalent to $a \equiv 0 \pmod p$ and in turn equivalent to $\#\tilde{E}(\kappa_u) \equiv 0 \pmod p$. $\square$

Define a set $\mathfrak{S}_L$ of primes v of K by

$$\mathfrak{S}_L := \{v \mid p, \text{ or } v \text{ ramifies in } L/K, \text{ or where } E \text{ has bad reduction}\}.$$

Theorem 2.6 (Theorem 6.1 of [1]). *Let $\chi : Gal(L/K) \hookrightarrow \bar{\mathbb{Q}}^\times$ be an injective character, and $\mathcal{O}[\chi]$ the extension of $\mathcal{O}$ by the values of χ. Assuming the Shafarevich-Tate Conjecture,*

$$rank_{\mathcal{O}[\chi]} E(L)^\chi - rank_{\mathcal{O}} E(K) \equiv \sum_{v \in \mathfrak{S}_L} \delta_v \pmod 2.$$

We now consider a dihedral tower $k \subset K \subset F$ where F/K is p-power abelian. Following [4, §3], we note that there is a bijection between cyclic extensions L/K in F and irreducible rational representations ρ_L of $G = \mathrm{Gal}(F/K)$. The semisimple group ring $\mathbb{K}[G]$ decomposes as

$$\mathbb{K}[G] \cong \oplus_L \mathbb{K}[G]_L$$

where $\mathbb{K}[G]_L$ is the ρ_L-isotypic component of $\mathbb{K}[G]$. For each L, for us it suffices deal with an injective character $\chi : \mathrm{Gal}(L/K) \hookrightarrow \bar{\mathbb{Q}}^\times$ appearing in the direct-sum decomposition of $\rho_L \otimes \bar{\mathbb{Q}}^\times$, and $\mathrm{rank}_{\mathcal{O}[\chi]} E(F)^\chi$ is independent[3] of the choice of χ.

Theorem 2.7. *Suppose that for every prime v satisfying $v^c = v$ and which ramifies in F/K, we have $v \nmid p$ and E has good reduction at v. For m equal to the number of such v with $p \mid \#\tilde{E}(\kappa_u)$, if $rank_{\mathcal{O}} E(K) + m$ is odd then*

$$rank_{\mathcal{O}} E(F) \geq ([F : K], [F : K]).$$

[3] We could instead write that $\dim_{\bar{\mathbb{Q}}}(E(F) \otimes \bar{\mathbb{Q}})^\chi$ is independent of the choice of χ.

Proof. Fix a cyclic extension L/K inside F. If v is a prime of K and $v^c \neq v$ then $\delta_v + \delta_{v^c} \equiv 0 \pmod 2$ by Lemma 5.1 of [4]. If $v^c = v$ and v is unramified in L/K, then v splits completely in L/K by Lemma 6.5(i) of [4]. It follows that N_{L_w/L'_w} is surjective and so $\delta_v \equiv 0$ by Definition 2.2. By assumption, Proposition 2.5 applies to the remaining primes v, and so $\sum_v \delta_v \equiv m \pmod 2$. Thus,

$$\mathrm{rank}_{\mathcal{O}[\chi]} E(L)^{\chi} \equiv \mathrm{rank}_{\mathcal{O}} E(K) + m \pmod 2$$

and we have assumed that the right-hand side is odd.

From Corollary 3.7 of [4] it follows that

$$\mathrm{rank}_{\mathcal{O}} E(F) = \sum_{L} (\dim_{\mathbb{Q}} \rho_L) \cdot (\mathrm{rank}_{\mathcal{O}[\chi]} E(L)^{\chi}).$$

As the previous paragraph applies for every cyclic L/K in F, we see from the decomposition of $\mathbb{K}[G]$ that $E(F) \otimes \mathbb{Q}$ contains a submodule isomorphic to $\mathbb{K}[G]$ and the claim follows. ☐

3. CM elliptic curves defined over $\mathbb{Q}$

Here, we will consider the CM elliptic curves E defined over $\mathbb{Q}$ (as in [7, A.3]). For each E, our aim is to determine[4] examples of dihedral towers $\mathbb{Q} \subset K \subset F$ over which, according to Theorem 2.7, the $\mathcal{O}$-rank of E grows. As we have assumed $\mathcal{O} \subset \mathrm{End}_K(E)$, we will consider towers in which $K = \mathbb{K}$ (see §1). All of our calculations will be done using Sage [8].

Let $E_D/\mathbb{Q}$ be an elliptic curve[5] defined over $\mathbb{Q}$ with CM by $K_D = \mathbb{Q}(\sqrt{-D})$. We determine computationally[6] $\mathrm{rank}_{\mathbb{Z}} E_D(K_D)$, and for $D = 3$ we see that this group is finite. For $D = 4, 7$, the situation is less certain, as Sage only tells us that $E_D(\mathbb{Q})$ is finite and $\mathrm{rank}_{\mathbb{Z}} E_D(K_D) \leq 2$. For each of the remaining CM curves E_D defined over $\mathbb{Q}$, one can (provably) calculate that $\mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) = 1$. We also have that $\mathrm{rank}_{\mathbb{Z}} E_D(K_D) \geq \mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) = 1$ and $\mathrm{rank}_{\mathbb{Z}} E_D(K_D)$ cannot be even, so $\mathrm{rank}_{\mathcal{O}} E_D(K_D) \geq 1$. For $D = 8$, 11, 19, 43, 67, and 163, Sage gives an upper bound[7] of 3 for $\mathrm{rank}_{\mathbb{Z}} E_D(K_D)$ and so for these D we can conclude that in fact $\mathrm{rank}_{\mathcal{O}} E_D(K_D) = 1$.

3.1. **Dihedral Extensions of $\mathbb{Q}$.** Recall that p is a fixed odd rational prime. Presently, we also fix $D \in \{3, 4, 7, \ldots, 163\}$ and let $E = E_D$, $K = K_D$. We are interested in abelian extensions F/K which are dihedral over $\mathbb{Q}$, and these are exactly the extensions contained in the ring class fields of K (see [3], Theorem 9.18).

Let $\mathcal{O}_f$ be an order in $\mathcal{O}_K$ of conductor f. We have a simple formula for the class number $h(\mathcal{O}_f)$ of $\mathcal{O}_f$ using, for example, Theorem 7.24 of [3], and noting that we have $h(\mathcal{O}_K) = 1$,

$$h(\mathcal{O}_f) = \frac{f}{[\mathcal{O}_K^{\times} : \mathcal{O}_f^{\times}]} \cdot \prod_{\text{primes } \ell | f} \left(1 - \left(\frac{-D}{\ell}\right) \frac{1}{\ell}\right).$$

For $D \neq 3, 4$ we have $\mathcal{O}_K^{\times} = \{\pm 1\}$ and for $D = 4$ we have $\#\mathcal{O}_K^{\times} = 4$, so in both of these cases $[\mathcal{O}_K^{\times} : \mathcal{O}_f^{\times}]$ is prime to p. For $D = 3$, one can show that $[\mathcal{O}_K^{\times} : \mathcal{O}_f^{\times}] = 3$

---

[4]Determined up to the correspondence of class field theory.

[5]See p.483 of [7], with $f = 1$ (in Silverman's notation), for a Weierstrauss equation.

[6]Specifically with Sage's interface to John Cremona's 'mwrank' and Denis Simon's 'simon_two_descent.'

when $f > 1$. The following paragraphs require only minor adjustments for the case $p = D = 3$.

Taking f to be an odd rational prime such that $(-D/f) = \pm 1$, the class number becomes $h(\mathcal{O}_f) = f \mp 1$ and so the ring class field $H_{\mathcal{O}_f}$ associated to $\mathcal{O}_f$ is an abelian extension of K of degree $f \mp 1$. Thus, for $f \equiv \pm 1 \pmod p$ we have a (non-trivial) p-power subextension F/K which is dihedral over $\mathbb{Q}$.

Next we need to understand the ramification in F/K. As K has class number 1, we know there are no unramified extensions of K, and so we must ensure that F satisfies the hypotheses of Theorem 2.7. A prime v of K ramifies in $H_{\mathcal{O}_f}/K$ if and only if $v \mid f\mathcal{O}_K$ (see for example exercise 9.20 in [3] and recall f is odd). If we choose f so that $-D$ is not a square $\pmod f$, f is inert in $K/\mathbb{Q}$, and so $f\mathcal{O}_K$ is prime and moreover the only prime that ramifies in $H_{\mathcal{O}_f}/K$. If $f\mathcal{O}_K$ does not ramify in F/K then the p-extension F/K is contained in the Hilbert class field H_K of K. As $H_K = K$, this is impossible, so $f\mathcal{O}_K$ ramifies in F/K and no other primes ramify in F/K. Taking f such that $f \nmid D$ and $-D$ is a square $\pmod f$, we have that f is not inert and does not ramify in $K/\mathbb{Q}$. As in the previous case, the primes of K above f both ramify in the p-extension F/K contained in $H_{\mathcal{O}_f}$.

Now, suppose $\mathrm{rank}_{\mathcal{O}} E(K)$ is odd[7]. To apply Theorem 2.7, we must have an even number m of primes v such that $v^c = v$, v ramifies in F/K, E has good reducation at v and for which $p \mid \#\tilde{E}(\mathbb{Z}/f\mathbb{Z})$. First, we can guarantee $m = 0$ if the only primes v which ramify in F/K do not satisfy $v^c = v$, e.g. taking $f \nmid D$ with $(-D/f) = 1$. Table 3.1 below gives, for each D and for $p = 3, 5, 7$, the smallest prime f which gives an extension of degree p following this recipe. We note that we do not need Proposition 2.5 for this case.

If we wish to allow for primes v satisfying $v^c = v$, we choose two p-extensions F_1, F_2 from two distinct rational primes f_i as above with $f_i \equiv -1 \pmod p$ and $(-D/f_i) = -1$, for $i = 1, 2$. The compositum $F = F_1F_2$ will satisfy our requirements. Indeed, firstly F is an abelian p-extension of K and is contained in the ring class field $H_{\mathcal{O}_{f_1 f_2}}$, hence dihedral over $\mathbb{Q}$ with only $f_1\mathcal{O}_K$ and $f_2\mathcal{O}_K$ ramifying in F/K. Secondly, as each f_i is inert in $K/\mathbb{Q}$, it is a supersingular prime for E (see, for example, exercise 2.30 of [7]) and hence p divides $\#\tilde{E}(\mathbb{Z}/f_i\mathbb{Z}) = f_i + 1$. Thus, E and the p-extension F/K satisfy the hypotheses of Theorem 2.7. Table 3.2 below gives, for each D and for $p = 3, 5, 7$, the smallest pair of distinct primes f_1, f_2 which give extensions of degree p^2 following this recipe.

Next, suppose $\mathrm{rank}_{\mathcal{O}} E(K)$ is even.[8] In this case, we need m to be odd in order to apply Theorem 2.7. The same ideas as above still work, and in Table 3.3 we list, for each D and for $p = 3, 5, 7$, the smallest prime f for which Theorem 2.7 guarantees rank $\geq p$.

Remark 3.1. Though there are algorithms in the literature to compute the defining polynomial of a class field (e.g. [2, §6], [3, §§11-3]) and such computational problems are of interest independently, we make no attempt here to explicitly determine the ring class fields $H_{\mathcal{O}_f}$. As is apparent from Table 3.2, our method of determining a field to which Theorem 2.7 applies involves ring class fields of large degree in a computationally inefficient way.

[7]The cases $D = 8, 11, \ldots, 163$ and possibly $D = 4, 7$.

[8]The case $D = 3$ and possibly $D = 4, 7$.

	$p=3$		$p=5$		$p=7$	
D	f	$[F:K]$	f	$[F:K]$	f	$[F:K]$
4	13	3	41	5	29	7
7	43	3	11	5	29	7
8	43	3	11	5	43	7
11	31	3	31	5	71	7
19	7	3	11	5	43	7
43	13	3	11	5	127	7
67	103	3	71	5	29	7
163	43	3	41	5	43	7

TABLE 3.1. Case $m=0$

	$p=3$			$p=5$			$p=7$		
D	f_1	f_2	$[F:K]$	f_1	f_2	$[F:K]$	f_1	f_2	$[F:K]$
4	11	23	9	19	59	25	83	139	49
7	5	41	9	19	59	25	13	41	49
8	5	23	9	29	79	25	13	167	49
11	2	29	9	29	79	25	13	41	49
19	2	29	9	29	59	25	13	41	49
43	2	5	9	19	29	25	223	349	49
67	2	5	9	79	109	25	13	41	49
163	2	5	9	19	29	25	13	139	49

TABLE 3.2. Case $m=2$

	$p=3$		$p=5$		$p=7$	
D	f	$[F:K]$	f	$[F:K]$	f	$[F:K]$
3	17	3	29	5	41	7
4	11	3	19	5	83	7
7	5	3	19	5	13	7

TABLE 3.3. Case $m=1$

REFERENCES

[1] S. Chetty. Arithmetic local constants for abelian varieties with complex multiplication. in preparation, preliminary draft: `http://personalwebs.coloradocollege.edu/~schetty/`.

[2] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer, 2000.

[3] D. Cox. *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*. Wiley Interscience, 1989.

[4] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics*, 166(2):581–614, 2007.

[5] J.S. Milne. Abelian Varieties. In G. Cornell and J. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986. available at `http://www.jmilne.org/math/`.

[6] J. Silverman. *Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[7] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[8] W. A. Stein et al. *Sage Mathematics Software (Version 4.2.1)*. The Sage Development Team, 2009. `http://www.sagemath.org`.

Sunil Chetty
sunil.chetty@coloradocollege.edu

Lung Li
leonli319@yahoo.com