THREE SELMER GROUPS FOR ELLIPTIC CURVES WITH 3-TORSION

TONY FENG, KEVIN JAMES, CAROLYN KIM, ERIC RAMOS, CATHERINE TRENTACOSTE, AND HUI XUE

ABSTRACT. We consider a specific family of elliptic curves with rational 3-torsion subgroup. We arithmetically define 3-Selmer groups through isogeny and 3-descent maps, then associate the image of the 3-descent maps to solutions of homogeneous cubic polynomials affiliated with the elliptic curve E and an isogenous curve E'. Thanks to the work of Cohen and Pazuki, we have solubility conditions for the homogeneous polynomials. Using these conditions, we give a graphical approach to the size of 3-Selmer groups then translate the conditions on graphs into a question concerning ranks of matrices. Finally, we give an upper bound for the rank of the elliptic curve E, by calculating the size of the Selmer groups.

1. INTRODUCTION

One of the major open problems in number theory involves calculating the rank of an elliptic curve. By calculating the size of the Selmer group, we can give an upper bound for the rank of a given elliptic curve. The goal of this paper is to bound the size of the 3-Selmer groups for a family of elliptic curves with 3-torsion given by

$$E_{ab} : y^2 = x^3 + (ax + b)^2$$

and its 3-isogenous curve given by

$$E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$$

with $b' = \frac{27-4a^3}{9}$ and therefore provide a bound for the rank of E_{ab}. Specifically, we analyze the 3-Selmer groups associated to 3-descent by isogeny of such elliptic curves by relating them to graphs with certain properties then translate the graph theory into a problem involving matrix analysis. Our methods use an elementary approach involving algebra and combinatorics. These methods have been employed to study 2-Selmer groups which arise from 2-descent for the family of "Congruent Number" curves, possessing 2-torsion [4], [3], but not for curves with 3-torsion or for 3-Selmer groups. For related work, we refer the reader to [5], [6], [7], [8] and [12].

Mordell's Theorem [11] asserts that for a general elliptic curve, $E/\mathbb{Q}$, the group of rational points, $E(\mathbb{Q})$, is a finitely generated abelian group, i.e.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}},$$

where $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group and r is the *rank* of the elliptic curve. The torsion part, $E(\mathbb{Q})_{\text{tors}}$, is well understood. We have the following deep theorem of Mazur [10, Chapter 8, Theorem 7.5] which completely characterizes the possibilities for the torsion subgroup.

Theorem 1.1 (Mazur)**.** *If E is an elliptic curve, then $E(\mathbb{Q})_{tors}$ is one of the following* 15 *groups:*

(1) $\mathbb{Z}/n\mathbb{Z}$*, with* $1 \leq n \leq 10$ *or* $n = 12$*.*
(2) $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, with* $1 \leq m \leq 4$*.*

Further, given a specific elliptic curve E, $E(\mathbb{Q})_{\text{tors}}$ is easily computable by the Nagell-Lutz Theorem [10, Chapter 8, Corollary 7.2].

On the other hand, not much is known about the rank. For example, the famous Birch and Swinnerton-Dyer Conjecture (see [1] or [9]) predicts that the rank of $E/\mathbb{Q}$ equals the order of vanishing of its L-series, $L(E,s)$, at $s=1$. In general, the rank of an elliptic curve is very difficult to compute. The only way, in practice, to give an upper bound for the rank of $E/\mathbb{Q}$ has been to prove upper bounds for the size of the m-Selmer group, $\mathrm{Sel}_m(E)$ (see [9] for more details). More precisely, for every natural number m we have an exact sequence [10, Theorem 10.4.2]

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to \mathrm{Sel}_m(E) \to Ш_E[m] \to 0,$$

where $Ш_E$ is the Tate-Shafarevich group and $A[\phi]$ denotes the kernel of ϕ in the group A. Combining this with Mordell's theorem we have that

$$E(\mathbb{Q})/mE(\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^r \oplus E(\mathbb{Q})[m].$$

In particular, we show in Section 2 that $[E_{ab}(\mathbb{Q}) : 3E_{ab}(\mathbb{Q})] = 3^{r+1}$.

We begin by giving an overview of 3-descent maps and their relation to the rank of an elliptic curve with rational 3-torsion. Following the treatment given in [2], we associate the following homogeneous polynomials of degree 3 to E_{ab} and $E'_{ab'}$ respectively

$$F_u(X,Y,Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

and

$$\begin{aligned} F_{u'}(X,Y,Z) &= \left(\overline{\gamma}\left(X + Y\sqrt{-3}\right)^3 - \gamma\left(X - Y\sqrt{-3}\right)^3\right)/\sqrt{-3} \\ &\quad +2aZ\left(X + Y\sqrt{-3}\right)\left(X - Y\sqrt{-3}\right) + \left(2b'/N(\gamma)\right)Z^3. \end{aligned}$$

Using these polynomials, we arithmetically define 3-Selmer groups as opposed to the usual definition involving Galois cohomology. Finding integer solutions is difficult, so we relax the condition and define the 3-Selmer groups, $\mathrm{Sel}^{(\phi)}(E_{ab})$ and $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$, to be the set of $u \in \mathbb{Q}^*/(\mathbb{Q}^*)^3$ (respectively, $u' \in \mathbb{Q}^*(\sqrt{-3})/(\mathbb{Q}^*(\sqrt{-3}))^3$) for which $F_u(X,Y,Z) = 0$ (respectively $F_{u'}(X,Y,Z) = 0$) has local solutions for all p. Once we define Selmer groups in the above manner, it is natural to investigate when we obtain local solutions. We discuss the local solubility of the homogeneous polynomials associated to E_{ab} in Section 3. Many of these conditions involve checking if ratios of the coefficients of the homogeneous polynomials are cubes modulo a given prime.

After completely characterizing when we obtain local solutions, we begin exploring this question in terms of graph theory. Feng and Xiong [4] introduce the notion of "odd graphs" to produce certain families of congruent numbers and Faulkner and James [3] use their ideas to compute the corresponding 2-Selmer groups. We extend their methods to the computation of 3-Selmer groups of elliptic curves with 3-torsion.

For the elliptic curve, E_{ab}, we construct a directed graph G' with subgraph G. The vertices of G and G' are comprised of the primes dividing $2b$ and the discriminant of the curve. We draw directed edges between primes where local solutions are not guaranteed and label each directed edge with a cubic root of unity. Next we introduce the idea of a "three-balanced" partition, (S_1, S_2, S_3), of the subgraph G. We identify each set in the partition with a coefficient associated to the homogeneous polynomial, $F_u(X,Y,Z)$. The general idea is that a partition of a graph is three-balanced if the ratios of the associated coefficients are cubes modulo a given prime. The prime $p = 3$ is slightly more complicated, so we introduce the idea of "three-quasi-balanced" partitions as well. We show that given a three-balanced partition, we can construct an element in the 3-Selmer

group, $\mathrm{Sel}^{(\phi)}(E_{ab})$, associated to the elliptic curve E_{ab}.

For example, consider the family of elliptic curves

$$E_n/\mathbb{Q} : y^2 = x^3 + n^2,$$

and its auxiliary family

$$E'_n : y^2 = x^3 - 27n^2.$$

There are isogenies $\phi : E_n \to E'_n$ given by

$$\phi(P) = \phi((x,y)) = \left(\frac{x^3+n^2}{x^2}, \frac{y(x^3-8n)}{x^3}\right).$$

We realize a concrete identification between the associated Selmer group, $\mathrm{Sel}^{(\phi)}(E_n)$, and the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^3$ consisting of equivalence classes $[u]$ with $u = u_1u_2^2$ for which the equation

$$u_1x^3 + u_2y^3 + \frac{2n}{u_1u_2}z^3 = 0$$

has non-trivial solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p. Casting this condition into the language of graph theory, we construct a directed graph G' with subgraph G where the vertices of G are exactly the prime divisors of $2n$ and the prime 3. Partitioning G into 3 possibly empty sets, (S_1, S_2, S_3), if this partition is three-balanced, then $u = \prod_{p\in S_1} p \prod_{p\in S_2} p^2$ is an element in $\mathrm{Sel}^{(\phi)}(E_n)$. In fact, we have the following theorem.

Theorem 1.2. *Let $E_n : y^2 = x^3 + n^2$. Suppose that n is odd, square-free, and divisible by 3, and define G to be the associated digraph. Then*

$$\left|\mathrm{Sel}^{(\phi)}(E_n)\right| = \#\{\textit{three-balanced partitions of } G\}.$$

For $E'_{ab'}$, we take a slightly different approach. In this setting we construct a graph G'' with subgraphs G' and G. The vertices of G, G' and G'' are comprised of the primes dividing $2b'$ and the discriminant. However, in this case, we place primes in different subgraphs depending on their classification; split primes, inert primes and ramified primes in $\mathbb{Q}(\zeta_3)$. The subgraph G consists only of split primes which divide $2b'$. Again, we draw directed edges between primes for which local solutions are not guaranteed and label each with a cubic root of unity. Due to complications associated with the local solubility of the primes 2 and 3, we do not require local solutions in $\mathbb{Q}_2$ and $\mathbb{Q}_3$. Hence we introduce the group $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})$, the set of local solutions for all primes not in $\mathcal{S}$ where $\mathcal{S}$ contains 2 and 3. Once we have constructed the graph, we introduce the notion of a "good" labeling on the vertices of the subgraph G. We label each vertex in G with a 0, 1 or 2 and identify the primes labeled with a 0 or a 1 to the parameters γ and $\overline{\gamma}$ in $F_{u'}(X, Y, Z)$. The idea is that a good labeling will produce an element in the modified 3-Selmer group, $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})$, associated to the isogenous elliptic curve $E'_{ab'}$.

Finally, we use the associated graphs to construct a characteristic matrix. Indexing the rows and columns by primes in the vertex set, we can relate the notion of a three-balanced partition and a good labeling to a Laplacian matrix. The primes associated with the columns will be those primes which are the heads of the directed edges and the primes associated with rows will be the primes which are the tails of the directed edges. The entries of the matrix will consist of cubic roots of unity and zeros. If a prime is associated with both a row and column, this entry will either be the sum of the other entries in the row or the negative of this sum, reduced modulo 3. Looking at the kernel of a submatrix of the Laplacian matrix, we can construct an element of the Selmer group (or modified Selmer group in the isogenous case). Employing the results of the rank-nullity theorem, we can bound the size of the 3-Selmer group. Therefore,

combining this result with the fact that the rank of the elliptic curve is bounded by the product of the sizes of the 3-Selmer groups, $\mathrm{Sel}^{(\phi)}(E_{ab})$ and $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$, we can give an upper bound for the rank of E_{ab}.

2. An overview of 3-descent

In this section, we will give a summary of the development of the 3-Selmer group through 3-descent. We will follow closely the treatment given in [2] and we refer the reader there for a detailed account. We consider the more general family of elliptic curves

$$E_D : y^2 = x^3 + D(ax+b)^2,$$

with 3-torsion points $\{\mathcal{O}, \mathcal{T}, -\mathcal{T}\}$ where $\mathcal{T} = (0, b\sqrt{D})$.

Lemma 2.1. [2, Lemma 1.2] *There exists a unique equation of E of the form $y^2 = x^3 + D(ax+b)^2$, where a, b, and D are in $\mathbb{Z}$, D is a fundamental discriminant (including 1), $b > 0$ and if we write $b = b_1 b_3^3$ with b_1 cube-free, then $(a, b_3) = 1$.*

From now on, we will assume that the equation of the curve satisfies the conditions of the above lemma. We will soon specialize to the case $D = 1$.

We recall the notion of an *isogeny* between elliptic curves.

Definition 1. *An* **isogeny** *between the elliptic curves E and E' is a morphism $\phi : E \to E'$ satisfying $\phi(\mathcal{O}) = \mathcal{O}'$. The* **dual isogeny** *to ϕ is the isogeny $\phi' : E' \to E$, satisfying $\phi(\phi'(P)) = [deg(\phi)]\, P$.*

We define the following auxiliary family of curves as in [2]

$$E'_D : y^2 = x^3 + D'\left(a'x + b'\right)^2,$$

where $D' = -3D$, $a' = a$, and $b' = \frac{27b-4a^3D}{9}$. The explicit isogeny $\phi : E \to E'$ is given by

$$\phi(P) = \phi((x,y)) = \left(\frac{x^3 + 4D(a^2x^2/3 + abx + b^2)}{x^2}, \frac{y(x^3 - 4Db(ax+2b))}{x^3}\right)$$

for $P \neq \mathcal{O}$ and $P \neq \pm\mathcal{T}$, and $\phi(P) = \mathcal{O}'$ if $P = \mathcal{O}$ or $P = \pm\mathcal{T}$. The dual isogeny $\widehat{\phi}$ is obtained by applying the same formula to E' and then dividing the x-coordinate by 9 and the y-coordinate by 27. The key fact is that the composition of ϕ and $\widehat{\phi}$ gives multiplication by 3, according to the following lemma.

Lemma 2.2. [2, Proposition 1.4] *The maps ϕ and $\widehat{\phi}$ are group homomorphisms, and $\phi \circ \widehat{\phi}$ and $\widehat{\phi} \circ \phi$ are multiplication by 3 maps on E' and E, respectively. The kernel of ϕ is $\{\mathcal{O}, \pm\mathcal{T}\}$, and that of $\widehat{\phi}$ is $\{\mathcal{O}'\}$.*

We recall the following exact sequence [10, Remark X.4.7 (pp. 300-301)]

$$0 \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{3E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \to 0,$$

where the second map is induced from $\widehat{\phi}$ and the third is induced from the identity.

This exact sequence along with Mordell's Theorem tells us that if the rank of E is r, then we have

$$3^{r+\delta} = [E(\mathbb{Q}) : 3E(\mathbb{Q})] = [E(\mathbb{Q}) : \widehat{\phi}(E'(\mathbb{Q}))][\widehat{\phi}(E'(\mathbb{Q})) : \widehat{\phi}(\phi(E(\mathbb{Q})))], \tag{2.1}$$

where

$$\delta = \begin{cases} 1 & E \text{ has rational point of order 3} \\ 0 & \text{otherwise} \end{cases}.$$

Lemma 2.2 gives the kernels of ϕ and $\widehat{\phi}$. In order to compute the rank of E, it is sufficient to understand the images of ϕ and $\widehat{\phi}$.

Let $K = \mathbb{Q}\left(\sqrt{D}\right)$. When $D = 1$, let $G_3 = \mathbb{Q}^*/(\mathbb{Q}^*)^3$, otherwise, let G_3 denote the subgroup of $K^*/(K^*)^3$ of classes whose norms are cubes. We recall the definition of the 3-descent map $\alpha : E(\mathbb{Q}) \to G_3$ defined by

$$\begin{cases} \alpha(\mathcal{O}) & = 1, \\ \alpha((0,b)) & = 1/(2b) \qquad \text{if } D = 1, \\ \alpha((x,y)) & = y - \sqrt{D}(ax+b). \end{cases}$$

One also defines $\alpha' : E'(\mathbb{Q}) \to K^*/(K^*)^3$ analogously, where $K = \mathbb{Q}\left(\sqrt{-3D}\right)$. Now, we have the following useful proposition.

Proposition 2.3. [2, Proposition 1.4.2] *The 3-descent maps α and α' are group homomorphisms. Furthermore,* $\ker(\alpha) = Im(\widehat{\phi})$ *and* $\ker(\alpha') = Im(\phi)$.

One immediately obtains the following corollary.

Corollary 2.4.

$$\frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \cong Im(\alpha), \qquad \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \cong Im(\alpha').$$

Using Theorem 2.1 and a bit of algebra we have the following result.

Proposition 2.5. [2, Proposition 2.2]

$$3^{r+\delta} = [E(\mathbb{Q}) : 3E(\mathbb{Q})] = |Im(\alpha)||Im(\alpha')|.$$

Hence to calculate r, the rank of E, it is sufficient to understand the images of the 3-descent maps α and α'.

From now on we will specialize to the cases where $D = 1$, that is to elliptic curves of the form $E_{ab} : y^2 = x^3 + (ax+b)^2$ and the isogenous curve is of the form $E'_{ab'} : y^2 =$

$x^3 - 3(ax + b')^2$ with $b' = \frac{27b-4a^3}{9}$. For $D = 1$, Cohen and Pazuki [2] prove the following theorem describing the group $\mathrm{Im}\,(\alpha)$.

Theorem 2.6. [2, Theorem 3.1] *Let $[u] \in \mathbb{Q}^*/(\mathbb{Q}^*)^3$. Write $[u] = u_1u_2^2$ where u_1 and u_2 are square-free, coprime integers in $\mathbb{Z}$. Then $[u] \in Im(\alpha)$ if and only if $u_1u_2 \mid 2b$ and the homogeneous cubic equation $F_u(x, y, z) = 0$ has an integer solution, where*

$$F_u(x, y, z) = u_1x^3 + u_2y^3 + \frac{2b}{u_1u_2}z^3 - 2axyz. \tag{2.2}$$

The proof of the above theorem can be found in [2].

Remark 1. (1) *The divisibility of $2b$ by u_1u_2 gives an upper bound on $|Im(\alpha)|$.*

(2) *When we speak of a solution to a homogeneous equation, we mean a non-trivial solution and thus when we speak of the solution set of such a homogeneous equation being non-empty we mean that there are non-trivial solutions.*

For an integral domain R and $F \in R[x, y, z]$, let

$$C_F(R) = \{(x, y, z) \in R^3 \setminus \{(0, 0, 0)\} \mid F(x, y, z) = 0\}.$$

In light of Theorem 2.6, we would like to determine $C_{F_u}(\mathbb{Z})$ for each $u = u_1u_2^2$ with $(u_1u_2)|(2b)$. In general, however, this is not possible due to obstructions in the 3 part of the Tate-Shafarevich group. Thus we are motivated to define the Selmer group $\mathrm{Sel}^{(\phi)}(E_{ab})$ as

$$\mathrm{Sel}^{(\phi)}(E_{ab}) = \{[u] \in \mathbb{Q}^*/(\mathbb{Q}^*)^3 \mid C_{F_u}(\mathbb{R}) \neq \emptyset; C_{F_u}(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p\},$$

where $F_u(X, Y, Z)$ is defined for E_{ab} in equation (2.2).

Cohen and Pazuki [2] also also give criteria in the isogenous case. As usual, $\mathcal{O}_K$ denotes the ring of integers of $K = \mathbb{Q}(\sqrt{-3})$. The following theorem describes the group $\mathrm{Im}\,(\alpha')$.

Theorem 2.7. *Let G_3 be the subgroup of $\mathbb{Q}^*(\omega)/(\mathbb{Q}^*(\omega))^3$ of classes whose norms are cubes where ω is a primitive cubic root of unity. Let $[u'] \in G_3$. Write $u' = \gamma\overline{\gamma}^2$ with $\gamma = c + d\omega \in \mathbb{Z}[\omega]$ and $N(\gamma) = \gamma\overline{\gamma}$ is only divisible by split primes. Then $[u'] \in Im(\alpha')$ if and only if $N(\gamma) \mid (2b')$ and the homogeneous cubic equation $F_{u'}(x, y, z) = 0$ has an integer solution where*

$$F_{u'}(X,Y,Z) := 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2. \tag{2.3}$$

From Theorem 2.7 we are motivated to define the Selmer group $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$ as

$$\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'}) = \{[u'] \in \mathbb{Q}^*(\sqrt{-3})/(\mathbb{Q}^*(\sqrt{-3}))^3 \mid C_{F_{u'}}(\mathbb{R}) \neq \emptyset; C_{F_{u'}}(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p\},$$

where $F_{u'}(X, Y, Z)$ is defined for $E'_{ab'}$ in equation (2.3).

3. Local Solubility

We will study local solubility for both $E_{ab} : y^2 = x^3 + (ax + b)^2$ and $E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$ where $b' = \frac{27b-4a^3}{9}$. For additional details, we refer the reader to [2].

Let $v_p(n)$, $n \in \mathbb{N}$, be the largest power of p that divides n, i.e. $v_p(n) = -\log_p |n|_p$. We set $v_p(0) = \infty$. So by Lemma 2.1, we may assume that either $v_p(a) = 0$ or $v_p(b) \leq 2$ for E.

3.1. **The Elliptic Curve E_{ab}.** The following two propositions give the local solubility criteria for the polynomial

$$F_u(X,Y,Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

associated with E_{ab}.

Proposition 3.1. [2] *Assume $p \neq 3$. Let*

$$F_u(X,Y,Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

with p-integral coefficients where u_1 and u_2 are square-free and coprime and $u_3 = \dfrac{2b}{u_1u_2}$.

(1) *If $p \neq 2$, $v_p(b) = 0$ and $v_p(27b - 4a^3) = 0$, then $F_u(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$.*

(2) *If $p \neq 2$, $v_p(b) = 0$ and $v_p(27b - 4a^3) > 0$, then $F_u(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if u_i/u_j is a cube in $\mathbb{F}_p^*$ for some $i \neq j$.*

(3) *If $p \neq 2$ and $v_p(b) > 0$, then $F_u(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if one of the following is fulfilled:*

   (a) $v_p(a) = 0$,

   (b) $v_p(a) > 0$ *and exactly one of $\{u_1, u_2, u_3\}$ is divisible by p and the ratio of the other two is a cube in $\mathbb{F}_p^*$,*

   (c) $v_p(a) > 0$ *and exactly two of $\{u_1, u_2, u_3\}$ are divisible by p and their ratio is a cube in $\mathbb{F}_p^*$.*

(4) *If $p = 2$, then $F_u(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_2$ if and only if one of the following is fulfilled:*

   (a) *exactly one of $\{u_1, u_2, u_3\}$ is divisible by 2 and the ratio of the other two is a cube in $\mathbb{F}_2^*$,*

(b) *exactly two of* $\{u_1, u_2, u_3\}$ *is divisible by* 2 *each exactly once and their ratio is a cube in* $\mathbb{F}_2^*$.

Proposition 3.2. [2] *Let*

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

with 3*-integral coefficients where* u_1 *and* u_2 *are square-free and coprime and* $u_3 = \dfrac{2b}{u_1u_2}$.

(1) *If* $v_3(a) = 0$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

(2) *If* $v_3(a) \geq 2$ *and* $v_3(b) = 0$ *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if* u_i/u_j *is a cube mod* 9 *for some* $i \neq j$.

(3) *If* $v_3(a) \geq 2$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 3, *say* u_i, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if either the ratio of the other two is a cube mod* 9 *or* $v_3(u_i) = 1$.

(4) *If* $v_3(a) \geq 2$ *and exactly two of* $\{u_1, u_2, u_3\}$ *are divisible by* 3, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if their ratio is a cube mod* 9.

(5) *If* $v_3(a) = 1$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 3, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if either the ratio of the other two is a cube mod* 9 *or there exists* $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9$.

(6) *If* $v_3(a) = 1$ *and two of* $\{u_1, u_2, u_3\}$ *are divisible by* 3, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

(7) *If* $v_3(a) = 1$, $v_3(b) = 0$ *and* u_i/u_j *is a cube mod* 9 *for some* $i \neq j$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

(8) *If* $v_3(a) = 1$, $v_3(b) = 0$ *and* u_i/u_j *is not a cube mod* 9 *for all* $i \neq j$ *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if there exists* $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$.

3.2. **The Isogenous Curve $E'_{ab'}$.** The following propositions give the local solubility criteria for the polynomial

$$\begin{aligned} F_{u'}(X,Y,Z) &:= 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 \\ &\quad -dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2 \end{aligned}$$

associated to the isogenous elliptic curve, $E'_{ab'}$. Note that since we are working over $\mathbb{Q}\left(\sqrt{-3}\right)$, $p = 3$ is the only ramified prime. If $p \equiv 2 \pmod 3$, then p is an inert prime. And if $p \equiv 1 \pmod 3$, then p is a split prime.

Proposition 3.3. [2, Corollary 6.3] *Let p be any split prime. Then there exists $d_p \in \mathbb{Q}_p$ such that $d_p^2 = -3$. Then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if the cubic*

$$u_1X^3 + u_2Y^3 + u_3Z^3 - \mathbf{c}XYZ = 0$$

does, where $u_1 = \left(c - \frac{d}{2}\right) - \frac{d}{2}d_p$, $u_2 = \left(c - \frac{d}{2}\right) + \frac{d}{2}d_p$, $u_3 = \frac{2b'}{\gamma\overline{\gamma}}d_p$ and $\mathbf{c} = 2ad_p$.

Making some minor adjustments to Proposition 3.1, we have all the conditions necessary to find a solution for $F_{u'}(X,Y,Z) = 0$ in $\mathbb{Q}_p$ where p is a split prime. Before stating our Corollary, we make the following observation.

Lemma 3.4. *Let $\Delta' = 27b' + 12a^3$. If $p \equiv 1 \pmod 3$, $p \mid \Delta'$ and $p \nmid b'$, then $2b'\sqrt{-3}$ is a cube mod p.*

So we can conclude that if u_i/u_j is a cube for some $i \neq j$, then this is true for all $i \neq j$.

Corollary 3.5. *Let p be any split prime. Then we can write $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and is in the upper-half plane. Let*

$$F_{u'}(X,Y,Z) \;=\; u_1X^3 + u_2Y^3 + u_3Z^3 - \boldsymbol{c}XYZ = 0$$

where $u_1 = \left(c - \frac{d}{2}\right) - \frac{d}{2}\sqrt{-3}$, $u_2 = \left(c - \frac{d}{2}\right) + \frac{d}{2}\sqrt{-3}$, $u_3 = \frac{2b'}{\gamma\overline{\gamma}}\sqrt{-3}$ *and* $\boldsymbol{c} = 2a\sqrt{-3}$ *with* $(c,d) = 1$.

(1) *If $v_p(b') = 0$ and $v_p(27b' + 12a^3) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$.*

(2) *If $v_p(b') = 0$ and $v_p(27b' + 12a^3) > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if u_1/u_2 is a cube in $\mathbb{F}_p^*$.*

(3) *If $v_\pi(b') > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}(\omega)_\pi$ if and only if one of the following is true*

   (a) *$v_\pi(a) = 0$,*

   (b) *$v_\pi(a) > 0$, π divides exactly one of $\{u_1, u_2, u_3\}$ and the ratio of the other two is a cube mod π,*

   (c) *$v_\pi(a) > 0$, π divides two of $\{u_1, u_2, u_3\}$ and their ratio is a cube mod π.*

Recall that $\gamma\overline{\gamma}$ is only divisible by split primes. So we have the following solubility propositions.

Proposition 3.6. *Assume $p \neq 2$, $p \equiv 2 \bmod 3$ and let $F_{u'}(X,Y,Z)$ be as in equation (2.3).*

(1) *If $v_p(\gamma\overline{\gamma}) = 0$, $v_p(2b') = 0$ and $v_p(27b' + 12a^3) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$.*

(2) *If $v_p(2b') = 0$ and $v_p(27b' + 12a^3) > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if $\frac{\gamma}{\overline{\gamma}}$ is a cube in $\mathbb{F}_{p^2}^*$.*

(3) *If* $v_p(2b') > 0$ *and* $v_p(\gamma\overline{\gamma}) = 0$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if one of the following is satisfied:*

(a) $v_p(2a) = 0$.

(b) $v_p(2a) > 0$ *and the class of* $\dfrac{\gamma}{\overline{\gamma}}$ *mod* p *is a cube in* $\mathbb{F}_{p^2}^*$.

Proposition 3.7. *Let* $p = 2$ *and* $F_{u'}(X,Y,Z)$ *be as in equation* (2.3).

(1) *If* $v_2(2b') \leq 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if the class of* $\dfrac{\gamma}{\overline{\gamma}}$ *mod* 2 *is a cube in* $\mathbb{Z}^*[\omega]/2\mathbb{Z}^*[\omega] \cong \mathbb{F}_4^*$. *Note that the only cube in* $\mathbb{F}_4^*$ *is* 1.

(2) *If* $v_2(2b') \geq 3$, *then*

(a) *if* $d \equiv 0 \pmod 4$ *and* $c \equiv \pm 1 \pmod 4$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$.

(b) *if* $d \equiv 2 \pmod 4$ *and* $c \equiv \pm 1 \pmod 4$ *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$.

(c) *if* $d \equiv 1 \pmod 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if either* $v_2(2b') \geq 4$ *or* $v_2(a) > 0$.

Proposition 3.8. *Let* $p = 3$ *and* $F_{u'}(X,Y,Z)$ *be as in equation* (2.3).

(1) *If* $v_3(2a) = 0$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following conditions is satisfied:*

(a) $v_3(d) > 0$,

(b) $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 0$.

(2) *If* $v_3(2a) \geq 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following conditions is satisfied:*

(a) $v_3(d) \geq 2$,

(b) $v_3(d) = v_3(b) = 1$,

(c) $v_3(d) = 0$ *and* $\dfrac{2b'}{dN(\gamma)}$ *is a cube mod* 9,

(d) $\dfrac{2b'}{N(\gamma)} \equiv \pm(6c - 3d) \ mod\ 27.$

(3) *If* $v_3(2a) = 1$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following is satisfied:*

(a) $v_3(d) \geq 2$,

(b) $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 1$,

(c) $v_3(d) = 0$ *and* $\left(\dfrac{2b'}{N(\gamma)} + 2a\right)/d$ *is a cube mod* 9,

(d) $v_3\left(\dfrac{2b'}{N(\gamma)}\right) = 1$, $v_3(d) = 0$ *and there exists* $s \in \{\pm 1\}$ *such that* $(d - 2c) \equiv s\left(\dfrac{2b'}{3N(\gamma)} + 2a\right) \pmod{27}$ *and* $s(2c - d) \equiv 2a/3 \pmod{3}$,

As one can see, the local solubility results associated with the primes 2 and 3 are complex. Therefore we exclude them when looking for solutions and define a larger group than the Selmer group.

4. Graph Theory

We can use the propositions from the previous section to give a characterization of the Selmer group in terms of graphs. For each elliptic curve, we construct a directed graph whose edges are labeled by cubic roots of unity. In the case of $E_{ab} : y^2 = x^3 + (ax + b)^2$, if we define a "three-balanced" partition in terms of the following labeling, then the size of $\mathrm{Sel}^{(\phi)}(E_{ab})$ corresponds to the number of "three-balanced" partitions of the graph. Conversely, for $E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$, we define the notion of a "good" labeling. Then the size of $\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})$ is bounded by the number of "good" labellings. We will make these notions more precise below.

4.1. **The Elliptic Curve** E_{ab}**.** We will begin by studying elliptic curves with rational 3-torsion, of the form

$$y^2 = x^3 + (ax + b)^2$$

whose discriminant is

$$\Delta \;=\; 16b^3\Delta'$$

where $\Delta' = 4a^3 - 27b$. Recall by Lemma 2.1, we know that either $v_p(b) \leq 2$ or $v_p(a) = 0$.

Let ω be a primitive cubic root of unity. If $p \equiv 1 \pmod 3$ is a rational prime (i.e. p splits in $\mathbb{Z}[\omega]$), then we will write $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and π is in the upper-half plane. Recall that if $p \equiv 2 \pmod 3$, then every number is a cube modulo p.

Using these conventions, let p and q be primes. Then we define the following:

$$\chi_p(q) = \begin{cases} \left(\frac{q}{\pi}\right)_3 & \text{if } p \equiv 1 \pmod 3 \\ 1 & \text{if } p \equiv 2 \pmod 3 . \end{cases}$$

Recall that we have the following properties of χ_p:

(1) $\chi_p(q) = 1$ if and only if q is a cube in $\mathbb{F}_p^*$

(2) $\chi_p(ab) = \chi_p(a)\chi_p(b)$.

So the above is true for all primes, p, not equal to 3. For $p = 3$, notice that $(\mathbb{Z}/9\mathbb{Z})^*$ is cyclic and generated by 2. Define χ_3 on $(\mathbb{Z}/9\mathbb{Z})^*$ by

$$\chi_3(q) = \omega^t$$

where $q = 2^t \in (\mathbb{Z}/9\mathbb{Z})^*$. Note that even though we are working mod 9, we will still use χ_3 to avoid confusion later.

One important concept to notice is that for those primes, q, which divide Δ', but do not divide $2b$, we can conclude that

$$2b \equiv \left(2\left(3^{-1}\right)a\right)^3 \pmod q$$

or equivalently that $\chi_q(2b) = 1$.

Using this observation we can conclude that

$$\begin{aligned}\chi_q(u_2/u_3) &= \chi_q(u_3/u_1)\\ &= \chi_q(u_1/u_2)\end{aligned}$$

and

$$\begin{aligned}\chi_q(u_1/u_3) &= \chi_q(u_3/u_2)\\ &= \chi_q(u_1/u_2)\end{aligned}$$

where u_1, u_2 and u_3 are as defined in Proposition 3.1. Also $\chi_q(u_i/u_j) = 1$ if and only if $\chi_q(u_j/u_i) = 1$ for $i \neq j$. Therefore it is enough to show u_1/u_2 is a cube modulo a given prime.

For clarity, we will consider different families of elliptic curves.

4.1.1. *The Family of Curves $\mathcal{E}_1$.* Consider the family $\mathcal{E}_1$ of elliptic curves given by

$$E_{ab}/\mathbb{Q} : y^2 = x^3 + (ax + b)^2$$

where $3 \nmid b$ and $\Delta = 16b^3\Delta'$, with $\Delta' = 27b - 4a^3$.

Let G be a graph with g vertices where

$$g = 1 + \sum_{p|b} v_p(b).$$

Let G' be the graph containing G with g' vertices where

$$g' = g + \sum_{\substack{p|\Delta' \\ p\nmid(2b)}} 1.$$

So

$$V(G) = \{p : p \mid b\} \cup \left\{p : p^2 \mid b\right\} \cup \{2\}$$

and

$$V(G') = V(G) \cup \{p : p \mid \Delta', p \nmid (2b)\}.$$

Draw directed edges from all primes $p \in V(G') \setminus V(G)$ to all primes $q \in V(G)$. Additionally draw directed edges from all primes $p \in V(G)$ to $q \in V(G)$ where $p \mid \Delta'$ and $p \neq q$. Label each directed edge from p to q as

$$\ell(p, q) := \chi_p(q).$$

A *partition* of $V(G)$ into three parts is an ordered triple of subsets (S_1, S_2, S_3) such that $S_1 \cup S_2 \cup S_3 = V(G)$ and $S_1 \cap S_2 = S_1 \cap S_3 = S_2 \cap S_3 = \emptyset$. We will allow for the possibility that S_1, S_2 or S_3 is empty.

Definition 2. *A partition, (S_1, S_2, S_3), of $V(G)$ is called* **three-balanced** *if and only if the following five conditions are satisfied:*

(1) *if $p \in S_1 \cup S_2$ and $p^2 \mid\mid 2b$, then the additional copy of p is in S_3 for all $p \in V(G)$*

(2) *if $4 \mid b$, then all copies of 2 are in S_3*

(3) *for every $p \in S_\nu$ such that the prime, p, is only in S_ν and $p \mid \Delta'$, we have*

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \;=\; 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, ect.)

(4) *for every* $p \in S_\eta$, $\eta = 1, 2$ *such that* p *is also in* S_3 *and* $p \mid \Delta'$, *we have*

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2\right) = 1$$

(5) *for every* $p \in V(G') \setminus V(G)$

$$\left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) = 1.$$

We will also need another definition.

Definition 3. *A partition,* (S_1, S_2, S_3), *of* $V(G)$ *is called* **three-quasi-balanced** *at* 3 *if and only if the following conditions are satisfied:*

(1) (S_1, S_2, S_3) *satisfies condition* (1) *for a three-balanced partition for all primes and satisfies the remainder of the conditions for all primes except* 3

(2) *Exclusively we have*

$$\left(\prod_{p_j \in S_1} \ell(3, p_j)\right)\left(\prod_{p_k \in S_2} \ell(3, p_k)^2\right) = 1$$

or there exists $s_1, s_2 \in \{\pm 1\}$ *such that*

$$2a \equiv s_1\left(\prod_{p_i \in S_1} p_i\right) + s_2\left(\prod_{p_j \in S_2} p_j\right) + s_1 s_2\left(\prod_{p_k \in S_3} p_k\right) \pmod{27}.$$

Using these definitions, we have the following lemma.

Lemma 4.1. *Suppose* (S_1, S_2, S_3) *is a partition of* $V(G)$. *Let*

$$u_1 = \prod_{p_i \in S_1} p_i \quad \text{and} \quad u_2 = \prod_{p_j \in S_2} p_j.$$

Then the homogeneous equation

$$u_1X^3 + u_2Y^3 + \frac{2b}{u_1u_2}Z^3 - 2aXYZ = 0 \tag{4.1}$$

has a solution in every local field $\mathbb{Q}_p$ *if and only if* $v_3(a) = 1$ *and* (S_1, S_2, S_3) *is three-quasi-balanced at* 3 *or* $v_3(a) \neq 1$ *and* (S_1, S_2, S_3) *is three-balanced.*

Proof. Let $u_3 = 2b/(u_1u_2)$. We will begin by assuming (S_1, S_2, S_3) is a three-balanced partition. By Proposition 3.1, there are three conditions we check. First, for every prime $p \in S_\nu$, if p is only in S_ν and $p \mid \Delta'$, then $\chi_p(u_{\nu+1}/u_{\nu+2}) = 1$ where we cycle the indicies. Second for every $p \in S_\eta$ with $\eta = 1$ or $\eta = 2$, such that p is also in S_3 and $p \mid \Delta'$, we have $\chi_p(u_\eta/u_3) = 1$. In addition, we must also show that for every $p \in V(G') \setminus V(G)$, $\chi_p(u_1/u_2) = 1$.

We will only prove one case since the remainding ones follow in a similar manner.

Notice that for every $p \in S_\nu$, which is only in S_ν and $p \mid \Delta'$, we have

$$\begin{aligned}
\chi_p(u_{\nu+1}/u_{\nu+2}) &= \chi_p(u_{\nu+1})\,\chi_p(u_{\nu+2})^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_p(p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \\
&= 1
\end{aligned}$$

since (S_1, S_2, S_3) is three-balanced. So $u_{\nu+1}/u_{\nu+2}$ is a cube modulo p and therefore we have a solution.

Conversely, suppose that (S_1, S_2, S_3) is not three-balanced or if $3 \,||\, a$, it is not three-quasi-balanced at 3 as well. There are a few cases we need to consider. We include one

of the cases here since the remaining ones follow either trivially or in a similar manner. Suppose there exists p in some S_ν with p not in any other S_η and $p \mid \Delta'$, such that

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p,p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p,p_k)^2\right) \neq 1.$$

Then

$$\begin{aligned}
\chi_p\left(u_{\nu+1}/u_{\nu+2}\right) &= \chi_p\left(u_{\nu+1}\right)\chi_p\left(u_{\nu+2}\right)^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_p(p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(p,p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p,p_k)^2\right) \\
&\neq 1,
\end{aligned}$$

where we cycle the indices. Hence by Proposition 3.1, equation (4.1) does not have a solution in $\mathbb{Q}_p$.

□

So we obtain the following theorem giving the size of the Selmer group, $\mathrm{Sel}^{(\phi)}(E_{ab})$, for the family $\mathcal{E}_1$.

Theorem 4.2. *Let $E_{ab} : y^2 = x^3 + (ax+b)^2$ with $3 \nmid b$. Let G and G' be defined as above. Then if $3 \,||\, a$, we have*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| = \#\left\{\mathrm{three-quasi-balanced\ at\ 3\ partitions\ of\ } V(G)\right\}.$$

Otherwise, we have

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| = \#\left\{\mathrm{three-balanced\ partitions\ of\ } V(G)\right\}.$$

4.1.2. *The Family of Curves $\mathcal{E}_2$.* Next, consider the family $\mathcal{E}_2$ of elliptic curves given by

$$E_{ab}/\mathbb{Q} : y^2 = x^3 + (ax + b)^2$$

where $3 \mid b$ and $\Delta = 16b^3\Delta'$, with $\Delta' = 27b - 4a^3$. Again, recall that we may assume for every prime p, either $v_p(a) = 0$ or $v_p(b) \leq 2$.

Let G be a graph with g vertices where

$$g = 1 + \sum_{p|b} v_p(b).$$

Let G' be the graph, containing G, with g' vertices where

$$g' = g + \sum_{\substack{p|\Delta' \\ p\nmid(2b)}} 1.$$

So

$$V(G) = \{p : p \mid b\} \cup \left\{p : p^2 \mid b\right\} \cup \{2\}$$

and

$$V(G') = V(G) \cup \{p : p \mid \Delta', p \nmid (2b)\}.$$

Draw directed edges from all primes $p \in V(G') \setminus V(G)$ to all primes $q \in V(G)$. Additionally draw directed edges from all primes $p \in V(G)$ to $q \in V(G)$ where $p \mid \Delta'$ and $p \neq q$. Label each directed edge from p to q as

$$\ell(p, q) := \chi_p(q).$$

Again, a *partition* of $V(G)$ into three parts is an ordered triple of subsets (S_1, S_2, S_3) such that $S_1 \cup S_2 \cup S_3 = V(G)$ and $S_1 \cap S_2 = S_1 \cap S_3 = S_2 \cap S_3 = \emptyset$. We will allow for the possibility that S_1, S_2 or S_3 is empty.

Definition 4. *A partition, (S_1, S_2, S_3), of $V(G)$ is called* **three-balanced** *if and only if the following conditions are satisfied:*

(1) *if $p \in S_1 \cup S_2$ and $p^2 \,||\, 2b$, then the additional copy of p is in S_3 for all $p \in V(G)$*

(2) *if $4 \mid b$, then all copies of 2 are in S_3*

(3) *for every $p \in S_\nu$, with $p \mid \Delta'$ and $p \neq 3$, such that the prime, p, is only in S_ν, we have*

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \;=\; 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, ect.)

(4) *for every $p \in S_\eta$, with $p \mid \Delta'$, $\eta = 1$ or 2 and $p \neq 3$, such that $p \in S_3$, we have*

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2\right) \;=\; 1$$

(5) *for every $p \in V(G') \setminus V(G)$,*

$$\left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) \;=\; 1$$

We will need two other definitions.

Definition 5. *A partition, (S_1, S_2, S_3), of $V(G)$ is called* **three-quasi-balanced** *at 3 if and only if the following conditions are satisfied:*

(1) *(S_1, S_2, S_3) is three-balanced*

(2) *if $p = 3$ is in only one S_ν, then either*

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(3, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(3, p_k)^2\right) \;=\; 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, ect.)

or there exists $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv s_1 \left(\prod_{p_i \in S_1} p_i \right) + s_2 \left(\prod_{p_j \in S_2} p_j \right) + s_1 s_2 \left(\prod_{p_k \in S_3} p_k \right) \pmod 9 .$$

Definition 6. *A partition, (S_1, S_2, S_3), of $V(G)$ is called* **three-quasi-balanced** *at 9 if and only if the following conditions are satisfied:*

(1) *(S_1, S_2, S_3) is three-balanced*

(2) *if $9 \mid b$ and $3 \notin S_1 \cup S_2$ then*

$$\left(\prod_{p_j \in S_1} \ell(3, p_j) \right) \left(\prod_{p_k \in S_2} \ell(3, p_k)^2 \right) \;=\; 1.$$

Using our definitions for this family of elliptic curves $\mathcal{E}_2$, we have the following lemma.

Lemma 4.3. *Suppose (S_1, S_2, S_3) is a partition of $V(G)$. Let*

$$u_1 = \prod_{p_i \in S_1} p_i \quad \text{and} \quad u_2 = \prod_{p_j \in S_2} p_j.$$

Then the homogeneous equation

$$u_1 X^3 + u_2 Y^3 + \frac{2b}{u_1 u_2} Z^3 - 2aXYZ = 0 \tag{4.2}$$

has a solution in every local field $\mathbb{Q}_p$ if and only if $3 \nmid a$ and (S_1, S_2, S_3) is three-balanced or if $3 \mid\mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 3 or if $9 \mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 9.

The proof is similar to that of Lemma 4.1, so we omit it.

The following theorem gives us the size of the Selmer group $\mathrm{Sel}^{(\phi)}(E_{ab})$ in terms of graphs for the family of elliptic curves $\mathcal{E}_2$.

Theorem 4.4. *Let $E_{ab} : y^2 = x^3 + (ax + b)^2$ with $3 \mid b$. Let G and G' be defined as above. Then if $3 \nmid a$, we have*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-balanced\ partitions\ of\ } V(G)\right\}.$$

If $3 \,||\, a$, then

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-quasi-balanced\ partitions\ at\ 3\ of\ } V(G)\right\}.$$

Otherwise, if $9 \mid a$, then

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-quasi-balanced\ partitions\ at\ 9\ of\ } V(G)\right\}.$$

4.2. **The Isogenous Curve $E'_{ab'}$.** In this section, we will be studying elliptic curves of the form

$$y^2 = x^3 - 3(ax + b')^2$$

whose discriminant is

$$\Delta = -144\left((b')^3\Delta'\right)$$

where $\Delta' = 27b' + 12a^3$. Recall by Lemma 2.1, we know that for every prime, p, either $v_p(b') \leq 2$ or $v_p(a) = 0$.

Once again, let ω be a primitive cubic root of unity. If $p \equiv 1 \pmod 3$, then we know that we can write $p = \pi\overline{\pi}$ with $\pi \equiv 2 \pmod 3$ and π in the upper-half plane. Define

$$\chi_p(q) = \chi_\pi(q) = \left(\frac{q}{\pi}\right)_3.$$

For $p \equiv 2 \pmod 3$, define

$$\chi_{p^2}(\delta) = \omega^i$$

where $\delta^{(p^2-1)/3} \equiv \omega^i \pmod p$.

Recall that we have the following properties of χ_p:

(1) $\chi_p(q) = 1$ if and only if q is a cube in $\mathbb{F}_p^*$
(2) $\chi_p(ab) = \chi_p(a)\chi_p(b)$.

So the above is true for all primes, p, not equal to 3. For $p = 3$, notice that $(\mathbb{Z}/9\mathbb{Z})^*$ is cyclic and generated by 2. Define χ_3 on $(\mathbb{Z}/9\mathbb{Z})^*$ by

$$\chi_3(q) = \omega^t$$

where $q = 2^t \in (\mathbb{Z}/9\mathbb{Z})^*$. Note that even though we are working mod 9, we will still use χ_3 to avoid confusion later.

Recall

$$\begin{aligned} F_{u'}(X,Y,Z) &= 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{\gamma\overline{\gamma}}Z^3 \\ &\quad -dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2 \end{aligned}$$

with $\gamma = c + d\omega$ where $\gamma\overline{\gamma}$ is only divisible by primes $p \equiv 1 \pmod 3$.

Consider the family $\mathcal{E}_3$ of elliptic curves given by

$$E'_{ab'} : y^2 = x^3 - 3(ax + b')^2.$$

Let G be a graph with vertex set $V(G) = \{p : p \equiv 1 \pmod 3,\ p \mid (2b')\}$. Additionally, let G' be a graph containing G with vertex set

$$V(G') = \{q : q \text{ satisfies one of (1), (2) below}\} \cup V(G)$$

(1) $q \equiv 2 \pmod 3$, $q \mid \Delta'$
(2) $q \equiv 1 \pmod 3$, $q \mid \Delta'$ and $q \nmid (2b')$.

Finally, let G'' be a graph containing G' with

$$V(G'') = V(G') \cup \{q : q \text{ satisfies one of } (3),(4),(5),(6) \text{ below}\} \cup \{\sqrt{-3}\}$$

(3) $q \equiv 1 \pmod 3$, $q^2 \mid (2b')$

(4) $q \not\equiv 1 \pmod 3$, $q^2 \mid (2b')$

(5) $q = 2$, $q^3 \mid (2b')$

(6) $q \mid b'$, $q = 3$.

Clearly, if $v_2(b') < 2$, then we do not need the additional copy of 2. And similarly, with the prime $q = 3$, we only include it if $3 \mid b'$.

Draw directed edges from all primes $p \in V(G'')$ to $q \in V(G'')$ where $p \mid (2b')$, $p \mid \Delta'$ and $q \mid (2b'\sqrt{-3})$.

Draw directed edges from all primes $p \in V(G')$ with $p \nmid (2b')\sqrt{-3}$ to primes $q \in V(G)$.

Label each directed edge from p to q as

$$\ell(p,q) = \begin{cases} \chi_\pi(q) & p \equiv 1 \pmod 3,\ p \mid (2b') \\ \chi_p(q) & p \equiv 1 \pmod 3, p \nmid (2b') \\ \chi_{p^2}(q) & p \equiv 2 \pmod 3 \end{cases}.$$

For each point p in $V(G)$, label it with $\mathcal{L}(p) \in \{0,1,2\}$.

Let $S_1 = \{p \in V(G) : \mathcal{L}(p) = 1\}$ and $S_2 = \{p \in V(G) : \mathcal{L}(p) = 2\}$.

Define

$$u_1 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \pi \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \overline{\pi}$$

and

$$u_2 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \overline{\pi} \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \pi.$$

Then

$$u_3 = \frac{2b'\sqrt{-3}}{u_1 u_2}.$$

Definition 7. *We say a labeling, $\mathcal{L}$, on $V(G)$ is **good** if and only if it satisfies the following properties:*

(1) *For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 0$, then*

$$\left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\eta)\ell(p,\overline{\eta})^2\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\ell(p,\eta)^2\right) = 1.$$

(2) *For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 1$ and $p \notin V(G'') \setminus S_1$, then*

$$\left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q\mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

(3) *For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 2$ and $p \notin V(G'') \setminus S_2$, then*

$$\left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q\mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

(4) *For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 1$ and $p \in V(G'') \setminus S_1$, then*

$$\left(\prod_{\substack{q\in S_1\setminus\{p\}\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2\cup\{p\})\\ q\mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

(5) *For all* $p \in V(G)$ *with* $p \mid \Delta'$, *if* $\mathcal{L}(p) = 2$ *and* $p \in V(G'') \setminus S_2$, *then*

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p, \overline{\eta})\right)\left(\prod_{\substack{q \in S_2 \setminus \{p\} \\ q = \eta\overline{\eta}}} \ell(p, \eta)\right)\left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2 \cup \{p\}) \\ q \mid 2b'\sqrt{-3}}} \ell(p, q)^2\right) = 1.$$

(6) *For all* $q \in V(G') \setminus V(G)$, $q \neq 2$, *then*

$$\left(\prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \ell(q, \pi)\ell(q, \overline{\pi})^2\right)\left(\prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \ell(q, \overline{\pi})\ell(q, \pi)^2\right) = 1.$$

Using this definition, we have the following lemma.

Lemma 4.5. *Suppose* $\mathcal{L}$ *is a labeling of* $V(G)$. *Then the homogeneous cubic equation* $F_{u'}(X, Y, Z) = 0$ *has a solution in every local field* $\mathbb{Q}_p$ *with* $p \neq 2, 3$ *if and only if* $\mathcal{L}$ *is a good labeling.*

Proof. Let

$$u_1 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \pi \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \overline{\pi}$$

and

$$u_2 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \overline{\pi} \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \pi.$$

Then, when necessary, let

$$u_3 = \frac{2b'\sqrt{-3}}{u_1 u_2}.$$

Assume that $\mathcal{L}$ is a good labeling. We need to check the following for every prime $p \in V(G)$ with $p \mid \Delta'$,

(1) if $\mathcal{L}(p) = 0$, then $\chi_p(u_1/u_2) = 1$.

(2) if $\mathcal{L}(p) = 1$, $p \notin V(G') \setminus S_1$, then $\chi_p(u_2/u_3) = 1$.

(3) if $\mathcal{L}(p) = 2$, $p \notin V(G') \setminus S_2$, then $\chi_p(u_1/u_3) = 1$.

(4) if $\mathcal{L}(p) = 1$ and $p \in V(G') \setminus S_1$, then $\chi_p(u_1/u_3) = 1$.

(5) if $\mathcal{L}(p) = 2$ and $p \in V(G') \setminus S_2$, then $\chi_p(u_2/u_3) = 1$.

Additionally, we must check for every $q \in V(G') \setminus V(G)$, $q \neq 2$, then $\chi_q(u_1/u_2) = 1$.

We will just check one condition. Assume $p \in V(G)$ with $p \mid \Delta'$. Suppose $\mathcal{L}(p) = 0$, then

$$\begin{aligned}
\chi_\pi(u_1/u_2) &= \chi_\pi(u_1)\chi_\pi(u_2)^2 \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\chi_\pi(\overline{\eta})^2\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\chi_\pi(\eta)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\eta)\ell(p,\overline{\eta})^2\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\ell(p,\eta)^2\right) \\
&= 1.
\end{aligned}$$

Therefore u_1/u_2 is a cube modulo p and hence we have a solution.

The remaining cases follow in a similar fashion.

Conversely assume $\mathcal{L}$ is not a good labeling of $V(G)$. There are a few cases we need to consider. Once again, we will go through one case since the remaining ones follow easily.

Suppose there exists a $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 1$, $p \notin V(G') \setminus S_1$ and

$$\left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q\mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) \neq 1.$$

But this implies that $\chi_\pi(u_2/u_3) \neq 1$, so u_2/u_3 is not a cube mod π. This violates Corollary 3.5.3.b, so we would not have a solution in $\mathbb{Q}_p$. □

Let $G_3 = \mathbb{Q}^*\left(\sqrt{-3}\right) / \left(\mathbb{Q}^*\left(\sqrt{-3}\right)\right)^3$. Let $\mathcal{S}$ be a set of primes containing 2 and 3. Define

$$\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right) = \left\{[u'] \in G_3 : C_{F_{u'}}(\mathbb{R}) \neq \emptyset, C_{F_{u'}}(\mathbb{Q}_p) \neq \emptyset \ \forall\ p \notin \mathcal{S}\right\}.$$

One can check that $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$ is a group.

The following theorem bounds the size of the Selmer group $\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})$.

Theorem 4.6. *Let $E'_{ab'} : y^2 = x^3 - 3(ax+b')^2$. Let G, G' and G'' be the graphs with vertices defined above. Let $\mathcal{S} = \{2, 3\}$. Then*

$$\left|\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})\right| \leq \left|\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)\right| = \#\{\textit{good labeling of } V(G)\}.$$

5. Linear Algebra

Given a graph G with vertex set $V(G)$, as defined in the previous section, we can construct a characteristic matrix.

5.1. **The Elliptic Curve E_{ab}.** Consider an elliptic curve $E_{ab} : y^2 = x^3 + (ax+b)^2$ with $\Delta' = 27b - 4a^3$. Assume we have a graph G' with vertex set $V(G')$ and subgraph G with vertex set $V(G)$, as defined in the Sections 4.1.1 and 4.1.2. We want to construct a characteristic matrix to relate the graph theory problem with three-balanced and three-quasi-balanced partitions to a linear algebra problem.

We will index the rows and columns of the characteristic matrix by primes and we begin by ordering primes. Let $p_1, \ldots, p_l$ be the distinct primes which divide $2b$ exactly once and divide Δ'. Let $p_{l+1}, \ldots, p_r$ be the distinct primes which divide $2b$ exactly twice and divide Δ'. Next, let $p_{r+1}, \ldots, p_n$ be the distinct primes which divide $2b$ but do

not divide Δ'. Also, let $p_{n+1}, \ldots, p_t$ be the second copy of the primes which divide $2b$ exactly twice. If $v_2(b) = 2$, then 2 is not one of the primes, p_i, for $1 \leq i \leq n$, so let $p_{t+1} = p_{t+2} = p_{t+3} = 2$. Let $q_1, \ldots, q_m$ be the distinct primes dividing Δ', but not $2b$.

Define

$$t' = \begin{cases} t & \text{if } v_2(b) < 2 \\ t+3 & \text{if } v_2(b) = 2 \end{cases}$$

$$r' = \begin{cases} r & \text{if } v_2(b) < 2 \\ r+1 & \text{if } v_2(b) = 2 \end{cases}$$

and

$$p_{r'} = \begin{cases} p_r & \text{if } v_2(b) < 2 \\ 2 & \text{if } v_2(b) = 2 \end{cases}.$$

Define the $(r'+m) \times t'$ matrix $A(G')$ by

$$a_{ij} = \begin{cases} \log_\omega \left(\ell\left(p_i, p_j\right)\right) & 1 \leq i \leq r', 1 \leq j \leq t', p_i \neq p_j \\ \log_\omega \left(\ell\left(q_{i-r'}, p_j\right)\right) & r'+1 \leq i \leq r'+m, 1 \leq j \leq t' \\ 0 & \text{otherwise} \end{cases}.$$

Let $D(G')$ be the $(r'+m) \times t'$ matrix with entries

$$d_{ij} = \begin{cases} \sum_{k=1}^{t'} a_{ik} & 1 \leq i \leq l, i = j \\ -\sum_{k=1}^{t'} a_{ik} & l+1 \leq i \leq r, i = j \\ 0 & \text{otherwise} \end{cases}.$$

Let

$$L'\left(G'\right) = A(G') - D(G')$$

and define $L(G)$ be the $(r'+m)\times n$ submatrix of $L'(G')$ with the $n+1$ to t' columns removed.

Remark 2. *Notice that* $\ker L(G) = \left\{\vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G')\right\}$.

Let $\vec{w} = (w_1, w_2, \ldots, w_n)^T \in \mathbb{F}_3^n$. For each $\vec{w}$, associate subsets as follows:

$$S_1 = \{p_i : w_i = 1\}$$

$$S_2 = \{p_i : w_i = 2\}$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t'}\}.$$

Now we will reduce to the case given in Section 4.1.1.

5.1.1. *The Family of Curves* $\mathcal{E}_1$. Assume E_{ab} has the property that $3 \nmid b$.

Then, if $v_3(a) = 1$, then we need to make the following adjustments. In this case we know that 3 must be one of the q_i's, so assume $q_m = 3$. Define $L_3(G')$ to be the $(r'+m-1)\times n$ submatrix of $L'(G')$ with the m-th row removed as well as the $n+1$ to t' columns removed.

Remark 3. *Again, notice that* $\ker L_3(G') = \left\{\vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G')\right\}$.

The following lemma gives the relationship between partitions of the graph G and the submatrices $L(G)$ and $L_3(G')$ of the Laplacian matrix $L'(G')$.

Lemma 5.1. (1) *If* $v_3(a) \neq 1$, *then the partition* (S_1, S_2, S_3) *corresponding to the vector* $\vec{w}$ *is three-balanced if and only if* $\vec{w} \in \ker L(G)$.

(2) *If* $v_3(a) = 1$, *then the partition* (S_1, S_2, S_3) *corresponding to the vector* $\vec{w}$ *is three-quasi-balanced if and only if either* $\vec{w} \in \ker(L(G))$ *or* $\vec{w} \in \ker(L_3(G'))$ *and there*

exists $s_1, s_2 \in \{\pm 1\}$ *such that*

$$2a \equiv s_1 \left(\prod_{\substack{p_i \in S_1 \\ p_i | 2b}} p_i \right) + s_2 \left(\prod_{\substack{p_j \in S_2 \\ p_j | 2b}} p_j \right) + s_1 s_2 \left(\prod_{\substack{p_k \in S_3 \\ p_k | 2b}} p_k \right) \pmod{27}.$$

Proof. Assume that $v_2(b) < 2$, so 2 is one of the primes $p_1, \ldots, p_r$ and $p'_r = p_r$. Next assume that $p_i \in S_1$ for $1 \leq i \leq l$. So there is only one copy of p_i. It is enough to show that $L'(G')\vec{w}' = \vec{0}$ with $\vec{w}' = (w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) w_j - \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) \left(w_j - w_i\right) \\
&= \sum_{w_j = 2} \log_\omega \left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j = 0} 2 \log_\omega \left(\ell\left(p_i, p_j\right)\right).
\end{aligned}$$

This is equivalent to zero mod 3 if and only if

$$\left(\prod_{p_j \in S_2} \ell\left(p_i, p_j\right) \right) \left(\prod_{p_k \in S_3} \ell\left(p_i, p_k\right)^2 \right) = 1.$$

The cases that $p_i \in S_2$ and $p_i \in S_3$ with $1 \leq i \leq l$ are identical.

Now assume $p_i \in S_1$ with $l+1 \leq i \leq r$. So we know that p_i appears in more than one S_j. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i,p_j\right)\right) w_j + \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i,p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i,p_j\right)\right)\left(w_j + w_i\right) \\
&= \sum_{w_j=0} \log_\omega\left(\ell\left(p_i,p_j\right)\right) + \sum_{w_j=1} 2\log_\omega\left(\ell\left(p_i,p_j\right)\right).
\end{aligned}$$

This is equivalent to zero mod 3 if and only if

$$\left(\prod_{\substack{p_j \in S_3 \\ p_j \neq p_i}} \ell\left(p_i,p_j\right)\right)\left(\prod_{\substack{p_k \in S_1 \\ p_k \neq p_i}} \ell\left(p_i,p_k\right)^2\right) = 1.$$

Once again, the cases that $p_i \in S_2$ and $p_i \in S_3$ follow in a similar manner.

The case that $v_2(b) = 2$ requires a slight adjustment, but follows easily. Additionally, one can check the conditions on the remaining cases.

□

Corollary 5.2. (1) *If $v_3(a) \neq 1$, the number of three-balanced partitions of G is 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$.*

(2) *If $v_3(a) = 1$, then the number of three-quasi-balanced partitions of G is between 3^{n-s_1} and 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$ and s_1 is the rank of the $(r'+m-1) \times n$ matrix $L_3(G')$.*

As a result of Lemma 5.1 and Corollary 5.2, we can construct an element of $\mathrm{Sel}^{(\phi)}(E_{ab})$ for the family of elliptic curves $\mathcal{E}_1$.

Corollary 5.3. (1) *If* $v_3(a) = 1$, *then* $\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| = 3^{n-s}$ *where* s *is the rank of the* $(r'+m) \times n$ *matrix* $L(G)$.

(2) *If* $v_3(a) \neq 1$, *then* $3^{n-s_1} \leq \left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \leq 3^{n-s}$ *where* s *is the rank of the* $(r'+m) \times n$ *matrix* $L(G)$ *and* s_1 *is the rank of the* $(r'+m-1) \times n$ *matrix* $L_3(G')$, *with possible equality on the right.*

5.1.2. *The Family of Curves* $\mathcal{E}_2$. Now we will assume that E_{ab} has the property that $3 \mid b$. Construct the matrix $L'(G')$ as before.

So in this case, we know that 3 is one of the primes p_i with $1 \leq i \leq t$. Let $\overline{L(G')}$ be the $(r'+m-1) \times t'$ submatrix of $L'(G')$ with the $\log_\omega(\ell(3,-))$ row removed. Then define $L_3(G)$ to be the $(r'+m-1) \times n$ submatrix of $\overline{L(G')}$ with the $n+1$ to t' columns removed.

Remark 4. *Notice that* $\ker L_3(G) = \left\{\vec{w} : (w, 0, \ldots, 0)^T \in \ker \overline{L(G')}\right\}$.

Recall given $\vec{w} = (w_1, w_2, \ldots, w_n)^T \in \mathbb{F}_3^n$, for each $\vec{w}$, we associate subsets as follows:

$$S_1 = \{p_i : w_i = 1\}$$

$$S_2 = \{p_i : w_i = 2\}$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t'}\}.$$

Lemma 5.4. (1) *If* $v_3(a) = 0$, *then the partition* (S_1, S_2, S_3) *corresponding to the vector* $\vec{w}$ *is three-balanced if and only if* $\vec{w} \in \ker L(G)$.

(2) *If* $v_3(a) = 1$, *then the partition* (S_1, S_2, S_3) *corresponding to the vector* $\vec{w}$ *is three-quasi-balanced at* 3 *if and only if one of the following holds:*

(a) $p_i = 3$ *is in only one* S_j *and* $\vec{w} \in \ker L(G)$

(b) $p_i = 3$ *is in only one* S_j, $\vec{w} \in \ker L_3(G)$ *and there exists* $s_1, s_2 \in \{\pm 1\}$ *such that*

$$2a \equiv s_1 \left(\prod_{\substack{p_i \in S_1 \\ p_i | 2b}} p_i \right) + s_2 \left(\prod_{\substack{p_j \in S_2 \\ p_j | 2b}} p_j \right) + s_1 s_2 \left(\prod_{\substack{p_k \in S_3 \\ p_k | 2b}} p_k \right) \pmod 9 .$$

(c) $p_i = 3$ *is in two* S_j*'s and* $\vec{w} \in \ker L(G_E)$.

(3) *If* $v_3(a) = 2$, *then the partition* (S_1, S_2, S_3) *corresponding to the vector* $\vec{w}$ *is three-quasi-balanced at* 9 *if and only if one of the following holds:*

(a) *if* $v_3(b) = 2$, $p_i = 3$ *is in* S_3 *only then* $\vec{w} \in \ker L(G)$

(b) *if* $v_3(b) \neq 2$ *or* $p_i = 3$ *is in more than one* S_j *then* $\vec{w} \in \ker L_3(G)$.

The proof of this lemma is similar to that of Lemma 5.1.

Corollary 5.5. (1) *If* $v_3(a) = 0$, *the number of three-balanced partitions of* G *is* 3^{n-s} *where* s *is the rank of the* $(r' + m) \times n$ *matrix* $L(G)$.

(2) *If* $v_3(a) > 0$, *then the number of three-quasi-balanced partitions at* 3 *of* G *is between* 3^{n-s_1} *and* 3^{n-s} *where* s *is the rank of the* $(r' + m) \times n$ *matrix* $L(G)$ *and* s_1 *is the rank of the* $(r' + m - 1) \times n$ *matrix* $L_3(G)$.

As a result of Lemma 5.4 and Corollary 5.5, we can construct an element of $\mathrm{Sel}^{(\phi)}(E_{ab})$ for the family of elliptic curves $\mathcal{E}_2$.

Corollary 5.6. (1) *If* $v_3(a) = 0$, *then* $\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| = 3^{n-s}$ *where* s *is the rank of the* $(r' + m) \times n$ *matrix* $L(G)$.

(2) *If* $v_3(a) > 0$, *then* $3^{n-s_1} \leq \left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \leq 3^{n-s}$ *where* s *is the rank of the* $(r' + m) \times n$ *matrix* $L(G)$ *and* s_1 *is the rank of the* $(r' + m - 1) \times n$ *matrix* $L_3(G)$, *with possible equality on the right.*

5.2. **The Isogenous Curve $E'_{ab'}$.** Consider a graph G'' with vertex set $V(G'')$ and subgraphs G' and G with vertex sets $V(G')$ and $V(G)$ respectively, as defined in the previous section. Once again, we want to construct a characteristic matrix to relate the graph theory problem to a linear algebra problem.

We will index the rows and columns of the characteristic matrix by primes and we begin by ordering the primes which will correspond to the columns of the characteristic matrix. Let $p_1, \ldots, p_n$ be the distinct primes equivalent to 1 mod 3 which divide $2b'$. Let $p_{n+1}, \ldots, p_l$ be the second copy of primes equivalent to 1 mod 3 which divide $2b'$. Next, let $p_{l+1}, \ldots, p_t$ be all copies of primes not equivalent to 1 mod 3 which divide $2b'$. Finally, we will also need $p_{t+1} = \sqrt{-3}$.

Next, we will order the primes which will correspond to the rows of the characteristic matrix. Let $q_1, \ldots, q_\nu$ be the distinct primes equivalent to 1 mod 3 which divide $2b'$ exactly once and divide $\Delta' = 27b' + 12a^3$. Let $q_{\nu+1}, \ldots, q_m$ be the distinct primes equivalent to 1 mod 3 which divide $2b'$ exactly twice and divide Δ'. Next, let $q_{m+1}, \ldots, q_l$ be the distinct primes equivalent to 1 mod 3 which divide Δ', but do not divide $2b'$. Finally, let $q_{l+1}, \ldots, q_r$ be the distinct primes equivalent to 2 mod 3, not including 2, which divide Δ'.

Now we are ready to define the $r \times (t+1)$ matrix, $A(G'')$. Define the entries of $A(G'')$ by

$$a_{ij} = \begin{cases} \log_\omega(\ell(q_i, p_j)) & 1 \leq i \leq m, 1 \leq j \leq t+1, q_i \neq p_j \\ \log_\omega(\ell(q_i, p_j)) & m+1 \leq i \leq r, 1 \leq j \leq l, q_i \neq p_j \\ 0 & \text{otherwise} \end{cases}.$$

Let $D(G'')$ be the $r \times (t+1)$ diagonal matrix with entries

$$d_{ij} = \begin{cases} \sum_{k=0}^{t+1} a_{ik} & 1 \leq i \leq \nu, i = j \\ -\sum_{k=0}^{t+1} a_{ik} & \nu + 1 \leq i \leq m, i = j \\ 0 & \text{otherwise} \end{cases}.$$

Let

$$L'(G'') = A(G'') - D(G'')$$

and define $L(G'')$ to be the $r \times n$ submatrix of $L'(G'')$ with the $n+1$ through $t+1$ columns removed.

Remark 5. *Notice that* $\ker L(G'') = \left\{\vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G'')\right\}$.

Let $\vec{w} = (w_1, \ldots, w_n)^T \in F_3^n$. Recall $p_1, \ldots, p_n$ are the distinct prime equivalent to 1 mod 3 which divide $2b'$. For $1 \leq i \leq n$, let

$$S_1 = \{p_i : w_i = 1\}$$

$$S_2 = \{p_i : w_i = 2\}$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t+1}\}.$$

Define the labeling $\mathcal{L}$ on $V(G)$ by $\mathcal{L}(p_i) = w_i$. Then we have the following lemma.

Lemma 5.7. *The labeling* $\mathcal{L}$ *of* $V(G)$ *corresponding to* $\vec{w}$ *is good if and only if* $\vec{w} \in \ker L(G'')$.

Proof. Without loss of generality, assume $w_i = 1$ for $1 \leq i \leq \nu$. So there is only one copy of p_i which divides $2b'$. It is enough to show that $L'(G'')\vec{w}' = \vec{0}$ with $\vec{w}' =$

$(w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$. Then

$$\begin{aligned} L'(G'')\vec{w} &= \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i, p_j\right)\right) w_j - \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i, p_j\right)\right) w_i \\ &= \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i, p_j\right)\right)\left(w_j - w_i\right) \\ &= \sum_{w_j=2} \log_\omega\left(\ell\left(q_i, p_j\right)\right) + \sum_{w_j=0} 2\log_\omega\left(\ell\left(q_i, p_j\right)\right). \end{aligned}$$

This is equivalent to zero mod 3 if and only if

$$\left(\prod_{\substack{p \in S_1 \\ p=\eta\overline{\eta}}} \ell(q_i, \overline{\eta})\right)\left(\prod_{\substack{p \in S_2 \\ p=\eta\overline{\eta}}} \ell(q_i, \eta)\right)\left(\prod_{\substack{p \in V(G'') \setminus (S_1 \cup S_2) \\ p \mid 2b'\sqrt{-3}}} \ell(p, q)^2\right) = 1.$$

The cases that $w_i = 2$ and $w_i = 0$ are identical.

Similar arguments can be used to verify the remainder of the proof. □

Corollary 5.8. *The number of good labellings of $V(G)$ is 3^{n-s} where s is the rank of the $r \times n$ matrix $L(G)$.*

Therefore, as a result of Lemma 5.7 and Corollary 5.8, we can construct an element in the modified Selmer group, $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$.

Corollary 5.9. $\left|\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})\right| \leq \left|\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)\right| = 3^{n-s}$, *where s is the rank of the $r \times n$ matrix $L(G)$ and $\mathcal{S} = \{2, 3\}$.*

6. Conclusion

Let $L_1(G)$ and $L_{3_1}(G')$ be the matrices defined in Section 5.1.1. Similarly, let $L_2(G)$ and $L_{3_2}(G)$ be the matrices defined in Section 5.1.2. Finally, let $L(G)$ be the matrix defined in Section 5.2. Then combining Corollaries 5.3, 5.6 and 5.9 we obtain the following results:

Theorem 6.1. (1) *If $3 \nmid b$ and $v_3(a) = 0$, then*

$$r \leq n_1 + n_2 - s_1 - s - 1$$

where s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_1(G)$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

(2) *If $3 \nmid b$ and $v_3(a) > 0$, then*

$$r \leq R_1 + R_2 - 1$$

where

$$n_1 + n_2 - s_2 - s \leq R_1 + R_2 \leq n_1 + n_2 - s_1 - s$$

and s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_1(G)$, s_2 is the rank of the $(r_1' + m_1 - 1) \times n_2$ matrix $L_{3_1}(G')$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

(3) *If $3 \mid b$ and $v_3(a) = 1$, then*

$$r \leq n_1 + n_2 - s_1 - s - 1$$

where s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_2(G)$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

(4) *If* $3 \mid b$ *and* $v_3(a) \neq 1$, *then*

$$r \leq R_1 + R_2 - 1$$

where

$$n_1 + n_2 - s_2 - s \leq R_1 + R_2 \leq n_1 + n_2 - s_1 - s$$

where s_1 *is the rank of the* $(r_1' + m_1) \times n_1$ *matrix* $L_2(G)$, s_2 *is the rank of the* $(r_1' + m_1 - 1) \times n$ *matrix* $L_{3_2}(G)$, s *is the rank of the* $r_2 \times n_2$ *matrix* $L(G)$ *and* r *is the rank of* E_{ab}.

Remark 6. *Once one has computed* $\mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$ *using linear algebra, applying Propositions 3.7 and 3.8 to the elements of* $\mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$, *one can compute* $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[2] Henri Cohen and Fabien Pazuki. Elementary 3-descent with a 3-isogeny. *Acta Arith.*, 140(4):369–404, 2009.

[3] Bryan Faulkner and Kevin James. A graphical approach to computing Selmer groups of congruent number curves. *Ramanujan J.*, 14(1):107–129, 2007.

[4] Keqin Feng and Maosheng Xiong. On elliptic curves $y^2 = x^3 - n^2x$ with rank zero. *J. Number Theory*, 109(1):1–26, 2004.

[5] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

[6] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[7] Kevin James and Ken Ono. Selmer groups of quadratic twists of elliptic curves. *Math. Ann.*, 314(1):1–17, 1999.

[8] Robert C. Rhoades. 2-Selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves. *J. Number Theory*, 129(6):1379–1391, 2009.

[9] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474 (electronic), 2002.

[10] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[11] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[12] Gang Yu. Average size of 2-Selmer groups of elliptic curves. II. *Acta Arith.*, 117(1):1–33, 2005.

(Tony Feng) Department of Mathematics, Harvard University, One Oxford Street Cambridge MA 02138

E-mail address: tfeng@college.harvard.edu

(Kevin James) Department of Mathematical Sciences, Clemson University, Box 340975 Clemson, SC 29634-0975

E-mail address: kevja@clemson.edu

URL: www.math.clemson.edu/∼kevja

(Carolyn Kim) Department of Mathematics, Harvard University, One Oxford Street Cambridge MA 02138

E-mail address: carolynkim@college.harvard.edu

(Eric Ramos) Department of Mathematical Sciences, Carnegie Mellon University, Wean Hall 6113, Pittsburgh, PA 15213

E-mail address: eramos@cmu.edu

(Catherine Trentacoste) Department of Mathematical Sciences, Clemson University, Box 340975 Clemson, SC 29634-0975

E-mail address: trentac@clemson.edu

(Hui Xue) Department of Mathematical Sciences, Clemson University, Box 340975 Clemson, SC 29634-0975

E-mail address: huixue@clemson.edu