SIZES OF SELMER GROUPS FOR ELLIPTIC CURVES WITH 3-TORSION

KELLY CRONE, TONY FENG, CAROLYN KIM, ERIC RAMOS

1. Introduction and Statement of Results

In this paper, we investigate a family of elliptic curves with 3-torsion given by

$$E_{a,b}/\mathbf{Q} : y^2 = x^3 + (ax + b)^2.$$

In particular, we analyze the Selmer groups associated to descent by isogeny of such elliptic curves by relating them to graphs and then apply elementary techniques from algebra and combinatorics. This method has been applied for the family of "Congruent Number" curves, possessing 2-torsion ([6], [5]), but not for curves with 3-torsion.

Mordell's Theorem [12] asserts that for a general elliptic curve, $E/\mathbf{Q}$, the group of rational points, $E(\mathbf{Q})$, is a finitely generated abelian group, i.e.

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

where $E(\mathbf{Q})_{\text{tors}}$ is a finite abelian group and r is called the *rank* of the elliptic curve. The following deep theorem due to Mazur [9] completely characterizes the possibilities for the torsion subgroup.

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

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

On the other hand, not much is known about the rank; indeed, the major open questions about elliptic curves today are concerned with computing the rank. For example, the famous Birch and Swinnerton-Dyer Conjecture (see [1] or [11]) predicts that the rank of $E/\mathbf{Q}$ equals the order of vanishing of its L-series, $L(E, s)$, at $s = 1$. The rank is, in general, very difficult to analyze. In practice, the only way to prove upper bounds for the rank of E has been to prove upper bounds for $\#\text{Sel}_m(E)$, where $\text{Sel}_m(E)$ is an effectively computable group called the m-Selmer group (see [11] for more details). More precisely, for every natural number m we have an exact sequence (see [13]Theorem 10.4.2 for details

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

where $Ш_E$ is the Tate-Shafarevich group and where $S[\phi]$ denotes the kernel of ϕ in an abelian group S. By Mordell's Theorem, we have that

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

In particular, $[E(\mathbf{Q}) : 3E(\mathbf{Q})] = 3^{r+1}$ for our family of elliptic curves since they have the 3-torsion points $T = (0, \pm b)$ and $\mathcal{O}$ (Lemma 2.1 in [3]).

In this paper we use a completely elementary combinatorial approach to compute the size of certain Selmer groups associated to the family of elliptic curves, $E/\mathbf{Q}$. Feng and Xiong [6] introduce the notion of "odd graphs" to produce certain families of congruent numbers, and Faulkner and James [5] use their ideas to compute sizes of the corresponding Selmer groups. We generalize their methods to this setting. For example, consider the family of elliptic curves

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

There is an isogeny $\phi : E_n \to \widehat{E}_n$ given by

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

We realize a concrete correspondence between the associated ϕ-Selmer group $\mathrm{Sel}^{(\phi)}(E_n)$ and the group of numbers u in $\mathbf{Q}^*/(\mathbf{Q}^*)^3$ for which the equation

$$ux^3 + \frac{1}{u}y^3 + 2bz^3 - 2axyz = 0$$

has a solution over $\mathbf{Q}_p$ for every prime p. We then cast this condition in the language of graph theory, constructing a complete digraph with vertices corresponding to the prime divisors of $2b$. Each partition of this graph into three parts that satisfies certain criteria will be called "three-balanced." (See Section 3 for the precise definitions.) We will then be able to prove the following theorem.

Theorem. *Let $E_n/\mathbf{Q} : y^2 = x^3 + n^2$. Suppose that n is odd, square-free, and divisible by 3, and define $G(E_n)$ to be the associated complete digraph. Then*

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

2. Notation and Setup

We first consider the general family of elliptic curve

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

with 3-torsion points $\{\mathcal{O}, \mathcal{T}, -\mathcal{T}\}$ where $T = (0, b\sqrt{D})$. Every elliptic curve with a rational 3-torsion subgroup can be given in such a form, where the cube-free part of b is

coprime with a and D is a fundamental discriminant [3]. We recall the notion of *isogeny* between elliptic curves.

Definition 2.1. *An* isogeny *between the elliptic curves E and $\widehat{E}$ is a morphism $\phi : E \to \widehat{E}$ satisfying $\phi(\mathcal{O}) = \widehat{\mathcal{O}}$. The* dual isogeny *to ϕ is the isogeny $\widehat{\phi} : \widehat{E} \to E$, satisfying $\phi\left(\widehat{\phi}\,(P)\right) = [deg(\phi)]P$.*

We define the dual curve to E as [3]

$$\widehat{E}/\mathbf{Q} : y^2 = x^3 - \widehat{D}\left(\widehat{a}x + \widehat{b}\right)^2,$$

where $\widehat{D} = 3D$, $\widehat{a} = a$, and $\widehat{b} = \frac{27b-4a^3}{9}$. The explicit isogeny $\phi : E \to \widehat{E}$ 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 $P \neq \pm T$, and $\phi(P) = \hat{\mathcal{O}}$ if $P = \mathcal{O}$ or $P = \pm T$. The dual isogeny $\widehat{\phi}$ is obtained by applying the same formula to $\widehat{E}/\mathbf{Q}$ 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. *(Proposition 1.4 in* [3]*) 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 $\widehat{E}$, respectively. The kernel of ϕ is $\{\mathcal{O}, \pm T\}$, and that of $\widehat{\phi}$ is $\{\widehat{\mathcal{O}}, \pm\widehat{T}\}$, where $\widehat{T} = (0, \widehat{b}\sqrt{-3D})$.*

According to [13], we have the following exact sequence:

$$0 \to \frac{\widehat{E}(\mathbf{Q})[\widehat{\phi}]}{\phi(E(\mathbf{Q})[3])} \to \frac{\widehat{E}(\mathbf{Q})}{\phi(E(\mathbf{Q}))} \to \frac{E(\mathbf{Q})}{3E(\mathbf{Q})} \to \frac{E(\mathbf{Q})}{\widehat{\phi}(\widehat{E}(\mathbf{Q}))} \to 0,$$

which, by the above lemma, simplifies in our case to the short exact sequence

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

showing that

$$[E(\mathbf{Q}) : 3E(\mathbf{Q})] = [E(\mathbf{Q}) : \widehat{\phi}(\widehat{E}(\mathbf{Q}))][\widehat{E}(\mathbf{Q}) : \phi(E(\mathbf{Q}))].$$

In general, given a rational isogeny $\psi : E \to \widehat{E}$ such that $E[\psi] \subset E(\mathbf{Q})$, we have the exact sequence

$$0 \to \frac{\widehat{E}(\mathbf{Q})}{\psi(E(\mathbf{Q}))} \to \mathrm{Sel}^{(\phi)}(E) \to Ш_E[\psi] \to 0.$$

Combining this with the definition of the Selmer group earlier gives the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \frac{\widehat{E}(\mathbf{Q})}{\phi(E(\mathbf{Q}))} & \longrightarrow & \mathrm{Sel}^{(\phi)}(E) & \longrightarrow & Ш_E[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{E(\mathbf{Q})}{3E(\mathbf{Q})} & \longrightarrow & \mathrm{Sel}^{(3)}(E) & \longrightarrow & Ш_{\widehat{E}}[3] & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{E(\mathbf{Q})}{\widehat{\phi}(\widehat{E}(\mathbf{Q}))} & \longrightarrow & \mathrm{Sel}^{(\widehat{\phi})}(\widehat{E}) & \longrightarrow & Ш_{\widehat{E}}[\widehat{\phi}] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Let r be the rank of $E/\mathbf{Q}$ and let $\#\mathrm{Sel}^{(\phi)} = 3^{s(\phi)}$ and $\#\mathrm{Sel}^{(\widehat{\phi})} = 3^{s(\widehat{\phi})}$. Then the fundamental inequality relating $\mathrm{Sel}^{(\phi)}$ and $\mathrm{Sel}^{(\widehat{\phi})}$ is

$$r \leq s(\phi) + s(\widehat{\phi}).$$

Now define the 3-descent map $\alpha : E(\mathbf{Q}) \to \mathbf{Q}^*/(\mathbf{Q}^*)^3$ by

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

We define $\widehat{\alpha} : E(\mathbf{Q}) \to K^*/(K^*)^3$ analogously, where $K = \mathbf{Q}[\sqrt{-3D}]$. This α map is in fact a group homomorphism [3] from $E(\mathbf{Q})$ to $\mathbf{Q}^*/(\mathbf{Q}^*)^3$, and the kernel of α is precisely the image of $\widehat{\phi}$. Likewise, the kernel of $\widehat{\alpha}$ is the image of ϕ. (Prop. 1.4 in [3]). Therefore,

$$\frac{E(\mathbf{Q})}{\widehat{\phi}(\widehat{E}(\mathbf{Q}))} \cong \mathrm{Im}\ \alpha \subset \mathbf{Q}^*/(\mathbf{Q}^*)^3,$$
$$\frac{\widehat{E}(\mathbf{Q})}{\phi(E(\mathbf{Q}))} \cong \mathrm{Im}\ \widehat{\alpha} \subset K^*/(K^*)^3.$$

In particular,

$$3^{r+1} = [E(\mathbf{Q}) : 3E(\mathbf{Q})] = |\mathrm{Im}\ \alpha||\mathrm{Im}\ \widehat{\alpha}|.$$

For $D = 1$, i.e. elliptic curves of the form $E/\mathbf{Q} : y^2 = x^3 + (ax+b)^2$, Cohen and Pazuki [3] prove the following theorem describing the group Im α.

Theorem 2.3. *Let $\bar{u} \in \mathbf{Q}^*/(\mathbf{Q}^*)^3$. Write $\bar{u} = u_1u_2^2$ where u_1 and u_2 are square-free, coprime integers in $\mathbf{Z}$. Then $u_1u_2 \mid 2b$ and $\bar{u} \in Im\ \alpha$ if and only if the homogeneous cubic equation $F_u(x, y, z) = 0$ has a solution, where*

$$F_u(x, y, z) = u_1x^3 + u_2y^3 + \frac{2b}{u_1u_2}z^3 - 2axyz. \tag{2.1}$$

Remark. *When we speak of a solution to a homogenenous equation, we mean a non-trivial solution.*

Let

$$C_E(F) = \{u \in \mathbf{Q}^*/(\mathbf{Q}^*)^3 \mid F_u(x, y, z) = 0 \text{ has a solution in } F\}$$

The Selmer group $\mathrm{Sel}^{(\phi)}$ can then be represented as

$$\mathrm{Sel}^{(\phi)}(E) = \{u \in \mathbf{Q}^*/(\mathbf{Q}^*)^3 \mid C_E(\mathbf{Q}_p) \neq \emptyset \text{ for every prime } p \in \mathbf{Z}.\}$$

For $n \in \mathbf{N}$, let $v_p(n)$ be the largest power of p that divides n, i.e. $v_p(n) = -\log_p |n|_p$. We set $v_p(0) = \infty$. Clearly equations with coefficients of the form (ap, bp^3) are equivalent to those with (a, b), so we can assume that $v_p(b) \leq 2$ or $v_p(a) = 0$. Using the work in [3], Section 5, we have:

Proposition 2.4. *Let*

$$F_u(x, y, z) = u_1x^3 + u_2y^3 + u_3z^3 - 2axyz,$$

where u_1 and u_2 are square-free and coprime, $u_3 = \frac{2b}{u_1u_2}$ and $p^3 \nmid b$ for every prime p dividing a.

1. *If $p \neq 2$, $p \neq 3$, $p \nmid b$, and $p \nmid (27b - 4a^3)$, then $F_u(x, y, z) = 0$ has a solution in $\mathbf{Q}_p$.*
2. *If $p \neq 2$, $p \neq 3$, and $p \mid b$, then $F_u(x, y, z) = 0$ has a solution in $\mathbf{Q}_p$ 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 $\mathbf{F}_p^*$.*
   (c) *$v_p(a) > 0$ and exactly two of $\{u_1, u_2, u_3\}$ is divisible by p and their ratio is a cube in $\mathbf{F}_p^*$.*
3. *If $p = 2$, then $F_u(x, y, z) = 0$ has a solution in $\mathbf{Q}_p$ if and only if $2 \nmid u_1u_2$ or $2 \mid u_1u_2$ and $4 \nmid b$.*
4. *If $p \neq 2$, $p \neq 3$, $p \nmid b$, and $p \mid 27b - 4a^3$, then $F_u(x, y, z) = 0$ has a solution in $\mathbf{Q}_p$ if and only if u_i/u_j is a cube in $\mathbf{F}_p^*$ for some $i \neq j$.*
5. *If $p = 3$ and $v_p(a) \neq 1$, then $F_u(x, y, z) = 0$ has a solution in $\mathbf{Q}_p$ if and only if one of the following is fulfilled.*
   (a) *$v_p(a) = 0$.*
   (b) *$v_p(a) \geq 2$ and $v_p(b) = 0$ and $u_i \equiv \pm u_j \pmod 9$ for some $i \neq j$.*
   (c) *$v_p(a) \geq 2$ and exactly one of $\{u_1, u_2, u_3\}$ is divisible by p and the ratio of the other two is $\pm 1 \pmod 9$.*

(d) $v_p(a) \geq 2$ *and exactly two of* $\{u_1, u_2, u_3\}$ *are divisible by* 9 *and their ratio is* $\pm 1 \pmod 9$.

Remark. We can also give criteria in the case $D = -3$, i.e. elliptic curves of the form $E/K : y^2 = x^3 - 3(ax+b)^2$. As usual, $\mathcal{O}_K$ denotes the ring of integers of K.

Theorem. *Let* $\bar{u} \in K^*/(K^*)^3$. *Write* $\bar{u} = u_1 u_2^2$ *where* u_1 *and* u_2 *are square-free, coprime integers in* $\mathcal{O}_K$. *Then* $u_1 u_2 \mid 2b$ *and* $\bar{u} \in Im\, \widehat{\alpha}$ *if and only if the homogenous cubic equation* $F'_u(x,y,z) = 0$ *has a solution, where*

$$F'_u(x,y,z) = u_1 x^3 + u_2 y^3 + \sqrt{-3}\frac{2b}{u_1 u_2} z^3 - 2\sqrt{-3} axyz \tag{2.2}$$

We can then similarly define

$$C'_E(F) = \{u \in K^*/(K^*)^3 \mid F'_u(x,y,z) = 0 \text{ has a solution in } F\},$$

$$\text{Sel}^{(\widehat{\phi})}(E) = \{u \in K^*/(K^*)^3 \mid C'_E(K_p) \neq \emptyset \text{ for every prime } p \in \mathcal{O}_K.$$

We have not been able to cast the criteria for solvability in a form conducive to our graphical approach, as we were able to do above. If this is possible, though, it would provide us with bounds on the rank by the formulas exhibited above.

3. Graphical Representations

Generalizing the ideas of Feng [6], we can use Proposition 2.4 to give a characterization of the Selmer group in terms of graphs. For each elliptic curve, we construct a complete directed graph whose directed edges are labeled by cubic roots of unity. If we define a "three-balanced" partition in terms of the following labelings, then the size of Sel^{ϕ} corresponds to the number of "three-balanced" partitions of the graph. We will make this notion more precise below.

Let ω be a primitive cubic root of unity. If $p \equiv 1 \pmod 3$ is a rational prime (i.e. p splits in $\mathbf{Z}[\omega]$), then write $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ is in the upper-half plane. Using these conventions, we define the following:

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

The following properties of χ_p are immediate:

(1) $\chi_p(q) = 1 \iff q$ is a cube in $\mathbf{F}_p^*$.
(2) $\chi_p(ab) = \chi_p(a)\chi_p(b)$.

Since $(\mathbf{Z}/9\mathbf{Z})^*$ is cyclic, in particular generated by 2, we may define χ_3 on $(\mathbf{Z}/9\mathbf{Z})^*$ in the same way. If $q = 2^t \in (\mathbf{Z}/9\mathbf{Z})^*$, then set

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

Throughout the rest of this paper, all integers are in $\mathbf{Z}$.

Case 1. Consider the family $\mathcal{E}_1$ of elliptic curves given by

$$E/\mathbf{Q} : y^2 = x^3 + b^2$$

and suppose that $2b$ is square-free and divisible by 3. Write $2b = p_1 p_2 \dots p_n$ where the p_i are primes and $p_n = 3$. Let us define a complete directed graph G_E associated to $E/\mathbf{Q}$ as follows: the vertex set, $V(G_E)$, is

$$V(G_E) = \{p_1, p_2, \dots, p_n\}.$$

Label the directed edge from p_i to p_j with e_{ij} according to the following rule:

$$e_{ij} = \begin{cases} \chi_{p_i}(p_j) & p_i \neq 3, \\ \chi_9(p_j) & p_i = 3. \end{cases}$$

A *partition* of $V(G_E)$ into three parts is an ordered triple of subsets (V_1, V_2, V_3) such that $V_1 \cup V_2 \cup V_3 = V(G_E)$ and $V_1 \cap V_2 = V_2 \cap V_3 = V_3 \cap V_1 = \emptyset$.

Definition 3.1. *Call the partition* (V_1, V_2, V_3) three-balanced *if for each* $p_i \in V_\nu$, *we have*

$$\left(\prod_{p_j \in V_{\nu+1}} e_{ij} \right) \left(\prod_{p_k \in V_{\nu+2}} e_{ik}^2 \right) = 1,$$

where we cycle the indices of the partitions (i.e. $V_1 = V_4$, *etc.).*

Lemma 3.2. *Suppose that* (V_1, V_2, V_3) *is a partition of* $V(G_E)$. *Let*

$$u_1 = \prod_{p_i \in V_1} p_i, \quad \textit{and} \quad u_2 = \prod_{p_j \in V_2} p_j.$$

Then the homogeneous equation

$$u_1 x^3 + u_2 y^3 + \frac{2b}{u_1 u_2} z^3 = 0 \tag{3.1}$$

has a solution in every local field $\mathbf{Q}_p$ *if and only if* (V_1, V_2, V_3) *is three-balanced.*

Proof. Let $u_3 = 2b/(u_1 u_2)$. First suppose that (V_1, V_2, V_3) is a three-balanced partition. By Proposition 2.4, we need to check that $\chi_{p_i}(u_{\nu+1}/u_{\nu+2}) = 1$ if $p_i \mid u_\nu$, where we cycle

the indices. But note that

$$\begin{aligned}\chi_{p_i}(u_{\nu+1}/u_{\nu+2}) &= \chi_{p_i}(u_{\nu+1})\chi_{p_i}(u_{\nu+2})^2 \\ &= \left(\prod_{p_j \in V_{\nu+1}} \chi_{p_i}(p_j)\right)\left(\prod_{p_k \in V_{\nu+2}} \chi_{p_i}(p_k)^2\right) \\ &= \left(\prod_{p_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{p_k \in V_{\nu+1}} e_{ik}^2\right) = 1\end{aligned}$$

since (V_1, V_2, V_3) is three-balanced.
Conversely, suppose that (V_1, V_2, V_3) is not three-balanced. Then by reversing the above equations there is some p_i such that $\chi_{p_i}(u_{\nu+1}/u_{\nu+2}) \neq 1$, so by Proposition 2.4, (3.1) has no solution in $\mathbf{Q}_{p_i}$. □

Theorem 3.3. *Let $E/\mathbf{Q} : y^2 = x^3 + b^2$. Suppose that $2b$ is square-free and divisible by 3, and define G_E as above. Then we have*

$$|\mathrm{Sel}^{(\phi)}| = \#\{\textit{three-balanced partitions of } V(G_E)\}.$$

Proof. By Lemma 3.2, each three-balanced partition corresponds to a homogeneous equation (3.1) which is solvable over each local field $\mathbf{Q}_p$. □

Case 2. Consider the family $\mathcal{E}_2$ of elliptic curves given by

$$E/\mathbf{Q} : y^2 = x^3 + (ax + b)^2$$

where $v_3(a) \geq 2$ and $2b$ is square-free and divisible by 3. Write

$$d := \frac{4a^3 - 27b}{\gcd(4a^3 - 27b, 2b)} = q_1 q_2 \dots q_m,$$

and

$$b = p_1 p_2 \dots p_n,$$

where the q_i and p_i are primes and $p_n = 3$. Let us define a complete directed graph G_E associated to $E\mathbf{Q}$ as follows: the vertex set $V(G_E)$ is

$$V(G_E) = \{q_1, q_2, \dots, q_m, p_1, p_2, \dots, p_n\}.$$

Label the directed edge from v_i to v_j with $e(\overrightarrow{v_i v_j})$ according to the following rule:

$$e(\overrightarrow{v_i v_j}) = \begin{cases} \chi_{v_i}(v_j) & v_i \neq 3 \text{ and } v_j \mid b, \\ \chi_9(v_j) & v_i = 3 \text{ and } v_j \mid b, \\ 1 & \text{otherwise.} \end{cases}$$

Definition 3.4. *Call the partition* (V_1, V_2, V_3) three-balanced *if for each vertex* p_i *and* $q_i \in V_\nu$*, we have*

$$\left(\prod_{p_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{p_k \in V_{\nu+2}} e_{ik}^2\right) = 1,$$

where we cycle the indices of the partitions (i.e. $V_1 = V_4$*, etc.).*

Lemma 3.5. *Suppose that* (V_1, V_2, V_3) *is a partition of* $V(G_E)$*. Let*

$$u_1 = \prod_{p_i \in V_1} p_i, \quad \text{and} \quad u_2 = \prod_{p_j \in V_2} p_j.$$

Then the homogeneous equation

$$u_1 x^3 + u_2 y^3 + \frac{2b}{u_1 u_2} z^3 - 2axyz = 0 \tag{3.2}$$

has a solution in every local field $\mathbf{Q}_p$ *if and only if* (V_1, V_2, V_3) *is three-balanced.*

Proof. Let $u_3 = 2b/(u_1 u_2)$. First suppose that (V_1, V_2, V_3) is a three-balanced partition. By Proposition 2.4, we need to check that

$$\begin{cases} \chi_{p_i}(u_{\nu+1}/u_{\nu+2}) = 1 & p_i \mid u_\nu,\ p_i \mid b, \\ \chi_{q_i}(u_{\nu+1}/u_{\nu+2}) = 1 & q_i \mid d, \end{cases}$$

where we cycle the indices. But note that

$$\begin{aligned} \chi_{p_i}(u_{\nu+1}/u_{\nu+2}) &= \chi_{p_i}(u_{\nu+1})\chi_{p_i}(u_{\nu+2})^2 \\ &= \left(\prod_{p_j \in V_{\nu+1}} \chi_{p_i}(p_j)\right)\left(\prod_{p_k \in V_{\nu+2}} \chi_{p_i}(p_k)^2\right) \\ &= \left(\prod_{p_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{p_k \in V_{\nu+2}} e_{ik}^2\right) = 1 \end{aligned}$$

since (V_1, V_2, V_3) is three-balanced. Similarly, $\chi_{q_i}(u_{\nu+1}/u_{\nu+2}) = 1$.
Conversely, suppose that (V_1, V_2, V_3) is not three-balanced. Then by reversing the above equations there is some $p \in V_\nu$ such that $\chi_p(u_{\nu+1}/u_{\nu+2}) \neq 1$, so by Proposition 2.4, (3.1) has no solution in $\mathbf{Q}_p$. □

Theorem 3.6. *Let* $E/\mathbf{Q} : y^2 = x^3 + (ax+b)^2$ *where* $v_3(a) \geq 1$ *and* $2b$ *is square-free and divisible by* 3*. Define* G_E *as above. Then we have*

$$|\mathrm{Sel}^{(\phi)}| = \frac{1}{3^m} \#\{\textit{three-balanced partitions of } V(G_E)\}.$$

Proof. By Lemma 3.5, each three-balanced partition corresponds to a homogeneous equation (3.2) which is solvable over each local field $\mathbf{Q}_p$. We overcount by a factor of 3 for each vertex q_i since which partition it is in is irrelevant. □

Remark. Case 1 above is in fact a special case of Case 2, but we chose to separate them for clarity.

Case 3. Consider the family $\mathcal{E}_3$ of elliptic curves given by

$$E/\mathbf{Q} : y^2 = x^3 + (ax + b)^2$$

where $3 \nmid a$ and $2b$ is square-free. Write

$$d := \frac{4a^3 - 27b}{\gcd(4a^3 - 27b, 2b)} = q_1 \dots q_m$$

and

$$b = p_1 p_2 \dots p_n,$$

where the q_i and p_i are primes. Let us define a complete directed graph G_E associated to $E/\mathbf{Q}$ as follows: the vertex set $V(G_E)$ is

$$V(G_E) = \{q_1, q_2, \dots, q_m, p_1, p_2, \dots, p_n\}.$$

Label the directed edge from v_i to v_j with $e(\overrightarrow{v_i v_j})$ according to the following rule:

$$e(\overrightarrow{v_i v_j}) = \begin{cases} \chi_{v_i}(v_j) & v_i \neq 3 \text{ and } v_j \mid b, \\ 1 & \text{otherwise.} \end{cases}$$

Definition 3.7. *Call the partition* (V_1, V_2, V_3) three-balanced *if for each vertex* p_i *and* $q_i \in V_\nu$*, we have*

$$\left(\prod_{p_j \in V_{\nu+1}} e_{ij} \right) \left(\prod_{p_k \in V_{\nu+2}} e_{ik}^2 \right) = 1,$$

where we cycle the indices of the partitions (i.e. $V_1 = V_4$*, etc.).*

Lemma 3.8. *Suppose that* (V_1, V_2, V_3) *is a partition of* $V(G_E)$*. Let*

$$u_1 = \prod_{p_i \in V_1} p_i, \quad \text{and} \quad u_2 = \prod_{p_j \in V_2} p_j.$$

Then the homogeneous equation

$$u_1 x^3 + u_2 y^3 + \frac{2b}{u_1 u_2} z^3 - 2axyz = 0 \tag{3.3}$$

has a solution in every local field $\mathbf{Q}_p$ *if and only if* (V_1, V_2, V_3) *is three-balanced.*

Proof. Let $u_3 = 2b/(u_1u_2)$. First suppose that (V_1, V_2, V_3) is a three-balanced partition. By Proposition 2.4, we need to check that

$$\begin{cases} \chi_{p_i}(u_{\nu+1}/u_{\nu+2}) = 1 & p_i \mid u_\nu,\ p_i \mid b,\ p_i \neq 3 \\ \chi_{q_i}(u_{\nu+1}/u_{\nu+2}) = 1 & q_i \mid d, \end{cases}$$

where we cycle the indices. But note that

$$\begin{aligned} \chi_{p_i}(u_{\nu+1}/u_{\nu+2}) &= \chi_{p_i}(u_{\nu+1})\chi_{p_i}(u_{\nu+2})^2 \\ &= \left(\prod_{p_j \in V_{\nu+1}} \chi_{p_i}(p_j)\right)\left(\prod_{p_k \in V_{\nu+2}} \chi_{p_i}(p_k)^2\right) \\ &= \left(\prod_{p_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{p_k \in V_{\nu+2}} e_{ik}^2\right) = 1 \end{aligned}$$

since (V_1, V_2, V_3) is three-balanced.
Conversely, suppose that (V_1, V_2, V_3) is not three-balanced. Then by reversing the above equations there is some $p_i \in V_\nu$ such that $\chi_p(u_{\nu+1}/u_{\nu+2}) \neq 1$, so by Proposition 2.4, (3.3) has no solution in $\mathbf{Q}_p$. □

Theorem 3.9. *Let $E/\mathbf{Q} : y^2 = x^3 + (ax+b)^2$ where $v_3(a) \geq 1$ and $2b$ is square-free and divisible by 3. Define G_E as above. Then we have*

$$|\mathrm{Sel}^{(\phi)}| = \frac{1}{3^m}\#\{\textit{three-balanced partitions of } V(G_E)\}.$$

Proof. By Lemma 3.8, each three-balanced partition corresponds to a homogeneous equation (3.3) which is solvable over each local field $\mathbf{Q}_p$. We overcount by a factor of 3 for each vertex q_i since the partition it is in is irrelevant. □

Case 4. Consider the family $\mathcal{E}_4$ of elliptic curves given by

$$E/\mathbf{Q} : y^2 = x^3 + b^2$$

where $3 \mid b$ and $4 \nmid b$. Write $2b = b_1b_2^2$, with $\gcd(b_1, b_2) = 1$, and let $b_1 = p_1p_2\dots p_m$, $b_2 = q_1q_2\dots q_n$ where the p_i, q_i are primes. Let us define a complete directed graph G_E associated to $E/\mathbf{Q}$ as follows: the vertex set $V(G_E)$ is

$$V(G_E) = \{p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n, q_1', q_2', \dots, q_n'\}.$$

where $q_i = q_i'$. Label the directed edge from v_i to v_j with $e(\overrightarrow{v_iv_j})$ according to the following rule:

$$e(\overrightarrow{v_iv_j}) = \begin{cases} \chi_{v_i}(v_j) & v_i \neq 3 \text{ and } v_j \neq v_i, \\ \chi_9(v_j) & v_i = 3 \\ 1 & v_i = v_j. \end{cases}$$

Definition 3.10. *Call the partition* (V_1, V_2, V_3) three-balanced *if* $\{q'_1, q'_2, \ldots, q'_m\} \subset V_3$ *and for each vertex* $v_i = p_r \in V_\nu$ *and each* $v_i = q_s \in V_3$*, we have*

$$\left(\prod_{v_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{v_k \in V_{\nu+2}} e_{ik}^2\right) = 1,$$

where we cycle the indices of the partitions (i.e. $V_1 = V_4$*, etc.) and for each* $q_i \in V_\nu$ *for* $\nu \neq 3$

$$\left(\prod_{v_j \in V_3} e_{ij}\right)\left(\prod_{v_k \in V_\nu} e_{ik}^2\right) = 1.$$

Lemma 3.11. *Suppose that* (V_1, V_2, V_3) *is a partition of* $V(G_E)$*. Let*

$$u_1 = \prod_{v_i \in V_1} v_i, \quad \text{and} \quad u_2 = \prod_{v_j \in V_2} v_j.$$

Then the homogeneous equation

$$u_1 x^3 + u_2 y^3 + \frac{2b}{u_1 u_2} z^3 - 2axyz = 0$$

has a solution in every local field $\mathbf{Q}_p$ *if and only if* (V_1, V_2, V_3) *is three-balanced.*

Proof. Let $u_3 = 2b/(u_1 u_2)$. First suppose that (V_1, V_2, V_3) is a three-balanced partition. By Proposition 2.4, we need that $\gcd(u_1, u_2) = 1$, which is exactly when $\{q'_1, q'_2, \ldots, q'_n\} \subset V_3$ and we need to check that

$$\begin{cases} \chi_{p_i}(u_{\nu+1}/u_{\nu+2}) = 1 & p_i \in V_\nu \text{ or } q_i \in V_3 \\ \chi_{q_i}(u_3/u_\nu) = 1 & q_i \in u_\nu \text{ where } \nu \neq 3, \end{cases}$$

where we cycle the indices. But note that for $p_i \in V_\nu$ or $q_i \in V_3$,

$$\begin{aligned} \chi_{v_i}(u_{\nu+1}/u_{\nu+2}) &= \chi_{v_i}(u_{\nu+1})\chi_{v_i}(u_{\nu+2})^2 \\ &= \left(\prod_{v_j \in V_{\nu+1}} \chi_{v_i}(v_j)\right)\left(\prod_{v_k \in V_{\nu+2}} \chi_{v_i}(v_k)^2\right) \\ &= \left(\prod_{v_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{v_k \in V_{\nu+2}} e_{ik}^2\right) = 1 \end{aligned}$$

since (V_1, V_2, V_3) is three-balanced. Similarly, for $q_i \in V_\nu$ with $\nu \neq 3$,

$$\begin{aligned}\chi_{v_i}(u_3/u_\nu) &= \chi_{v_i}(u_3)\chi_{v_i}(u_\nu)^2 \\ &= \left(\prod_{v_j \in V_3} \chi_{v_i}(v_j)\right)\left(\prod_{v_k \in V_\nu} \chi_{v_i}(v_k)^2\right) \\ &= \left(\prod_{v_i \in V_3} e_{ij}\right)\left(\prod_{v_k \in V_\nu} e_{ik}^2\right) = 1.\end{aligned}$$

Conversely, suppose that (V_1, V_2, V_3) is not three-balanced. Then by reversing the above equations there is some $p_i \in V_\nu$ or $q_i \in V_3$ such that $\chi_p(u_{\nu+1}/u_{\nu+2}) \neq 1$ or some $q_i \in V_\nu$ where $\nu \neq 3$ such that $\chi_q(u_3/u_\nu) \neq 1$, so by Proposition 2.4, (3.1) has no solution in $\mathbf{Q}_p$. □

Theorem 3.12. *Let $E/\mathbf{Q} : y^2 = x^3 + b^2$ where $3|b$ and and $4 \nmid b$.. Define G_E as above. Then we have*

$$|\mathrm{Sel}^{(\phi)}| = \#\{\textit{three-balanced partitions of } V(G_E)\}.$$

Proof. By Lemma 3.11, each three-balanced partition corresponds to a homogeneous equation (3.11) which is solvable over each local field $\mathbf{Q}_p$. □

Case 5. Consider the family $\mathcal{E}_5$ of elliptic curves given by

$$E/\mathbf{Q} : y^2 = x^3 + b^2$$

where $2b$ is not square-free and $4|b$, write $b/4 = b_1 b_2^2$, with $\gcd(b_1, b_2) = 1$, and let $b_1 = p_1 p_2 \dots p_m$, $b_2 = q_1 q_2 \dots q_n$ where the p_i, q_i are primes. Let us define a complete directed graph G_E associated to $E/\mathbf{Q}$ as follows: the vertex set $V(G_E)$ is

$$V(G_E) = \{p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n, q_1', q_2', \dots, q_n', 2, 2, 2\}.$$

where $q_i = q_i'$. Label the directed edge from v_i to v_j with $e(\overrightarrow{v_i v_j})$ according to the following rule:

$$e(\overrightarrow{v_i v_j}) = \begin{cases} \chi_{v_i}(v_j) & v_i \neq 3 \text{ and } v_j \neq v_i, \\ \chi_9(v_j) & v_i = 3 \\ 1 & v_i = v_j. \end{cases}$$

Definition 3.13. *Call the partition (V_1, V_2, V_3)* three-balanced *if $\{q_1', q_2', \dots, q_m', 2, 2, 2\} \subset V_3$ and for each vertex $v_i = p_r \in V_\nu$ and each $v_i = q_s \in V_3$, we have*

$$\left(\prod_{v_j \in V_{\nu+1}} e_{ij}\right)\left(\prod_{v_k \in V_{\nu+2}} e_{ik}^2\right) = 1,$$

where we cycle the indices of the partitions (i.e. $V_1 = V_4$, etc.) and for each $q_i \in V_\nu$ for $\nu \neq 3$

$$\left(\prod_{v_j \in V_3} e_{ij}\right)\left(\prod_{v_k \in V_\nu} e_{ik}^2\right) = 1$$

Lemma 3.14. *Suppose that (V_1, V_2, V_3) is a partition of $V(G_E)$. Let*

$$u_1 = \prod_{v_i \in V_1} v_i, \quad \text{and} \quad v_2 = \prod_{v_j \in V_2} v_j.$$

Then the homogeneous equation

$$u_1 x^3 + u_2 y^3 + \frac{2b}{u_1 u_2} z^3 - 2axyz = 0 \tag{3.4}$$

has a solution in every local field $\mathbf{Q}_p$ if and only if (V_1, V_2, V_3) is three-balanced.

Proof. The case for every prime except 2 is the same as above. By Proposition 2.4, we need $2 \nmid u_1 u_2$, which happens exactly when all the copies of 2 are in V_3. □

Theorem 3.15. *Let $E/\mathbf{Q} : y^2 = x^3 + b^2$ where $v_3(a) \geq 1$ and $2b$ is not square-free and divisible by 3. Define G_E as above. Then we have*

$$|\mathrm{Sel}^{(\phi)}| = \#\{\textit{three-balanced partitions of } V(G_E)\}.$$

Proof. By Lemma 3.14, each three-balanced partition corresponds to a homogeneous equation (3.4) which is solvable over each local field $\mathbf{Q}_p$. □

4. Linear Algebra Perspective.

Given a graph G as defined in the previous section, we construct a characteristic matrix as follows.

Case 1. If G has no repeated vertices, define the n-by-n matrix $A(G)$, where n is the number of vertices in G, such that

$$A(G)_{ij} = \begin{cases} \log_\omega e_{ij} & i \neq j, \\ 0 & i = j, \end{cases}$$

with the usual choice of the principal branch so that $\log_\omega 1 = 0$. Let $d_i = \sum_j A(G)_{ij}$, i.e. the sum of the entries in the ith row of $A(G)$. Now let

$$L(G) = A(G) - \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix}.$$

Note that there is a bijection between partitions of $V(G)$ into three possibly empty parts and $\mathbf{F}_3^n$ vectors v. Specifically, let $v = (v_1, \ldots, v_n)$ and set

$$v_i = \begin{cases} 0 & p_i \in V_1, \\ 1 & p_i \in V_2, \\ 2 & p_i \in V_3. \end{cases}.$$

Lemma 4.1. *We have $v \in \ker L(G)$ if and only if the partition corresponding to v is three-balanced.*

Proof. Let $v = (v_1, \ldots, v_n)$. Suppose $p_i \in V_1$. Then we have

$$(L(G)v)_i = \sum_j a_{ij}v_j - d_i v_i = \sum_j a_{ij}(v_j - v_i) = \sum_{v_j=1} a_{ij} + \sum_{v_j=2} 2a_{ij},$$

which is congruent to $0 \pmod 3$ if and only if

$$\left(\prod_{p_j \in V_2} e_{ij}\right)\left(\prod_{p_k \in V_3} e_{ik}^2\right) = 1.$$

The other two cases are completely analogous.

□

Case 2. If G has repeated vertices and at most 2 copies of 2, let the vertices, in order, be $\{p_1, p_2, \ldots, p_m, q_1, q_2, \ldots q_n, q_1', q_2', \ldots, q_n'\}$, where $q_i = q_i'$ and all other vertices are distinct. Otherwise, if G has 3 copies of 2, let the vertices, in order, be $\{p_1, p_2, \ldots, p_m, q_1, q_2, \ldots q_n, q_1', q_2', \ldots, q_{n+3}'\}$, where $q_i = q_i'$ and all other vertices are distinct except for $q_{n+1}' = q_{n+2}' = q_{n+3}' = 2$.

If $4 \nmid b$, let $n' = (m + 2n)$. Otherwise if $4|b$, let $n' = (m + 2n + 3)$. Define the n'-by-n' matrix $A'(G)$ such that

$$A'(G)_{ij} = \begin{cases} \log_\omega e_{ij} & i \neq j, \\ 0 & i = j, \end{cases}$$

with the usual choice of the principal branch so that $\log_\omega 1 = 0$. Next, let

$$d_i = \begin{cases} \sum_j A'(G)_{ij} & i \leq m, \\ -\sum_j A'(G)_{ij} & m < i \leq n', \end{cases}$$

Now let

$$L'(G) = A'(G) - \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_{n'} \end{pmatrix}.$$

Let $L(G)$ be the upper left $(m+n)$-by-$(m+n)$ submatrix of $L'(G)$.

Note that there is a bijection between valid partitions of $V(G)$ into three possibly empty parts and $\mathbf{F}_3^{n'}$ vectors w. Specifically, let $w = (w_1, \ldots, w_{n'})$ and set

$$w_i = \begin{cases} 1 & v_i \in V_1 \\ 2 & v_i \in V_2 \\ 0 & v_i \in V_3 \end{cases}.$$

Remark. *Note that* $\ker L(G) = \{w \in \ker L'(G) \mid w_i = 0 \quad i > m+n\}$

Lemma 4.2. *We have $w \in \ker L(G)$ if and only if the partition corresponding to w is three-balanced.*

Proof. It suffices to show that $v \in \{w \in \ker L'(G) \mid w_i = 0 \quad i > m+n\}$ if and only if the partition corresponding to w' is three-balanced, where $w' = \{w_1, \ldots, w_{m+n}\}$. We see that $w_i = 0$ for $i > m+n$ if and only if all the q_i' are in V_3, which is one condition for the partition to be three-balanced.

For $p_i \in V_1$ we have

$$(L'(G)w)_i = \sum_j a_{ij}w_j - d_i w_i = \sum_j a_{ij}(w_j - w_i) = \sum_{w_j=2} a_{ij} + \sum_{w_j=0} 2a_{ij},$$

which is congruent to $0 \pmod 3$ if and only if

$$\prod_{p_j \in V_2} e_{ij} \prod_{p_k \in V_3} e_{ik}^2 = 1.$$

The cases for when $p_i \in V_2$ or V_3 or when $q_i, q_i' \in V_3$ are completely analogous.

For $q_i \in V_1$ we have

$$(L'(G)w)_i = \sum_j a_{ij}w_j - d_i w_i = \sum_j a_{ij}(w_j + w_i) = \sum_{w_j=0} a_{ij} + \sum_{w_j=1} 2a_{ij},$$

which is congruent to $0 \pmod 3$ if and only if

$$\prod_{v_j \in V_3} e_{ij} \prod_{v_k \in V_1} e_{ik}^2 = 1$$

The case for when $q_i \in V_2$ is completely analogous.

□

Corollary 4.3. *The number of three-balanced partitions of G is 3^{l-s}, where s is the rank of the l-by-l matrix $L(G)$.*

Corollary 4.4. $|\mathrm{Sel}^\phi| = 3^{l-s}$*, where s is the rank of the l-by-l matrix $L(G)$.*

References

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

[2] Brent, R. P. and McKay, B. D. *Determinants of and rank of random matrices over* $\mathbf{Z}_m$. Discrete Math., **66** (1987) 35-49.

[3] Cohen, H. and Pazuki, F., *Elementary 3-descent with a 3-isogeny*. Acta Arith. **140** (2009), no. 4, 369–404.

[4] Cremona, J. E. and Odoni, R. W. K., *Some Density Results For Negative Pell Equations; An Application of Graph Theory*. J. London Math. Soc. (2) **39** (1989) 16-28.

[5] Faulker, B. and James, K., *A graphical approach to computing selmer groups of congruent number curves*. Ramanujan Journal **14** (2007) no. 1, 107–129.

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

[7] Garcia, A. *Curves over Finite Fields Attaining the Hasse-Weil Upper Bound*. Progr. Math. **202**, pp. 199-205. Birkhauser, Basel (2001).

[8] Heath-Brown, D. R. *The size of Selmer groups for the congruent number problem, II*. Invent. Math. **118** (2) (1994) 331-370.

[9] Mazur, B. *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (2) (1978) 129-162.

[10] Rhodes, Robert C. *2-Selmer groups and the Birch-Swinnerton-Dyer Conjecture for the congruent number curves*, J. Number Theory **129** (2009), 1379-1391.

[11] Rubin, K. and Silverberg, S. *Ranks of Elliptic Curves*. Bulletin of the AMS **39** (2002), 455-474.

[12] Silverman, J. H. and Tate, J. *Rational Points on Elliptic Curves*, Springer, New York, 1992.

[13] Silverman, J. H. *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.