The Average Size of Selmer Groups of Elliptic Curves

Arav Karighattam

Abstract. Several statistical properties of elliptic curves over $\mathbb{Q}$ have been deduced from the average rank of their Selmer groups. In papers by Bhargava, Shankar, and others, these average ranks have been computed by associating the Selmer groups with sets of orbits of coregular representations. In this paper, we review these methods and focus in particular on the computation of the average rank of elliptic curves ordered by a height function on the coefficients, based on the parametrization of the 2-Selmer group by orbits of binary quartic forms under the natural action by $\mathrm{PGL}_2\,\mathbb{Z}$. We also discuss the parametrization of the 3-Selmer group by orbits of ternary cubic forms under the natural action by $\mathrm{GL}_3(\mathbb{Z})$, which leads to analogous results on the average size of the 3-Selmer group over all elliptic curves.

1. Introduction.

Let E be an elliptic curve defined over $\mathbb{Q}$. The Mordell-Weil Theorem states that the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. This implies that we can study the structure of this group $E(\mathbb{Q})$ by studying the rank $r := \mathrm{rk}\,E(\mathbb{Q})$ and the torsion subgroup $E(\mathbb{Q})_{tors} \subseteq E(\mathbb{Q})$.

The possibilities for the torsion subgroup of the group of rational points of an elliptic curve are quite restricted over the base field $\mathbb{Q}$. Mazur [12] proved that the torsion subgroup of any elliptic curve over $\mathbb{Q}$ is either of the form $\mathbb{Z}/k\mathbb{Z}$ where $1 \leq k \leq 12$ (but $k \neq 11$) or of the form $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where $k = 2, 3$, or 4. For any specific elliptic curve E one can determine with little effort which of these groups is the torsion subgroup $E(\mathbb{Q})_{tors}$ using local conditions, as the reduction map $E(\mathbb{Q})_{tors} \to \tilde{E}(\mathbb{F}_p)$ modulo p turns out to be an injection for any prime $p \geq 11$ at which E has good reduction (see Silverman [13], §VII.3).

The complexity in determining the structure of the group of rational points $E(\mathbb{Q})$ thus lies in determining the rank r, and in finding generators for the $\mathbb{Z}^r$ summand of $E(\mathbb{Q})$. The rank of elliptic curves is not known to be bounded in general, except in specific families [13]. However, there is a general technique known as *n-descent* that can be used to calculate the rank of any specific elliptic curve. Following [13], §X.4, if we consider the short exact sequence $0 \to E(\overline{\mathbb{Q}})[n] \hookrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{[n]} E(\overline{\mathbb{Q}}) \to 0$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, the long exact sequence in cohomology shows that the sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{coker}([n]\colon E(\mathbb{Q}) \to E(\mathbb{Q})) = E(\mathbb{Q})/nE(\mathbb{Q}) &\longrightarrow H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n]) \\ &\longrightarrow H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E)[n] = \ker(H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E) \xrightarrow{[n]} H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E)) \longrightarrow 0 \end{aligned}$$

is exact. So, the problem of determining the rank of E is now reduced to the problem of determining $E(\mathbb{Q})/nE(\mathbb{Q}) = \ker(H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n]) \to H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E)[n])$, given knowledge of the torsion subgroup $E(\mathbb{Q})_{tors}$.

The computation of this kernel can be localized to give an upper bound on the rank of $E/\mathbb{Q}$. In particular, we define the n-Selmer group to be the kernel

$$\mathrm{Sel}_n\,E/\mathbb{Q} := \ker\left(H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n]) \to \prod_{\nu \text{ place of } \mathbb{Q}} H^1(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_\nu, E(\overline{\mathbb{Q}_\nu}))\right)$$

so that there is an inclusion $E(\mathbb{Q})/nE(\mathbb{Q}) \hookrightarrow \mathrm{Sel}_n\,E/\mathbb{Q}$.

Although there is much difficulty in determining the ranks of elliptic curves, it turns out that the *average rank* of all elliptic curves is bounded. More specifically, the following theorem holds.

THEOREM 1. [1] (Bhargava, Shankar, 2015) *Consider the elliptic curves over $\mathbb{Q}$ with equations $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ such that $p^4|A$ and $p^6|B$ do not both hold for any prime p, ordered by the height function $H(A, B) = \max\{4|A|^3, 27B^2\}$.*

(a) *The average size of* $\mathrm{Sel}_2 E/\mathbb{Q}$ *is* 3.
(b) *The average size of* $\dim_{\mathbb{F}_2} \mathrm{Sel}_2 E/\mathbb{Q}$ *is at most* 3/2.
(c) *The average value of* $\mathrm{rk}\, E(\mathbb{Q})$ *is at most* 3/2.

Similarly, the average size of $\mathrm{Sel}_3 E/\mathbb{Q}$ is known, and it turns out as a (somewhat indirect) consequence that $\mathrm{rk}\, E(\mathbb{Q}) = 0$, that is, $E(\mathbb{Q})$ is finite, with positive probability.

THEOREM 2. [2] (Bhargava, Shankar, 2015) *Consider the elliptic curves over $\mathbb{Q}$ with equations $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ such that $p^4|A$ and $p^6|B$ do not both hold for any prime p, ordered as before.*

(a) *The average size of* $\mathrm{Sel}_3 E/\mathbb{Q}$ *is* 4.
(b) *The average size of* $\dim_{\mathbb{F}_3} \mathrm{Sel}_3 E/\mathbb{Q}$ *is at most* 7/6.
(c) *The average value of* $\mathrm{rk}\, E(\mathbb{Q})$ *is at most* 7/6.
(d) *The probability that a randomly chosen elliptic curve E has rank* 0 *is positive.*

We note that there are similar results for the 4-Selmer and 5-Selmer groups [3, 4], the latter of which results in stricter upper bounds on the average rank of elliptic curves.

How are results on the average size of the n-Selmer group proved? The key ingredient in the proof is a parametrization by what is known as a *coregular representation* [1], that is, a parametrization of the n-Selmer group by a certain class of orbits of a vector space V over $\mathbb{Q}$ under the action of a matrix group with the property that the set of polynomials on V fixed by G forms a polynomial ring (isomorphic to $\mathbb{Q}[x_1, x_2, \ldots, x_\ell]$ for some ℓ). For the 2-Selmer group, it turns out that the correct group action is the action of $\mathrm{PGL}_2\mathbb{Q}$ on the vector space of binary quartic forms over $\mathbb{Q}$, on which we will elaborate in the subsequent sections.

2. Selmer Groups and Soluble Coverings.

In this section we describe an alternative description of the elements of the n-Selmer group of an elliptic curve E, in terms of what are known as the locally soluble n-coverings of E. Following the notational conventions of [13], for any field K and any curve C/K, we will let $K(C)$ denote the function field of C over K.

As defined by Birch and Swinnerton-Dyer [5], for any integer $n \geq 2$, an *n-covering* of an elliptic curve $E/\mathbb{Q}$ consists of a curve $C/\mathbb{Q}$ and an isomorphism $\varphi_C \colon C \xrightarrow{\cong} E$ over $\overline{\mathbb{Q}}$ such that $[n] \circ \varphi_C$ is a morphism (of degree n^2) defined over $\mathbb{Q}$. We say that two n-coverings of E are isomorphic if they only differ by the addition of an n-torsion point of E. More precisely, (C, φ_C) and $(C', \varphi_{C'})$ are isomorphic n-coverings if there is an isomorphism $\psi \colon C \to C'$ defined over $\mathbb{Q}$ and a point $P \in E[n]$ such that $P + \varphi_C = \varphi_{C'} \circ \psi$. The following result, adapted from Silverman [13], Theorem X.2.2, and utilized by Bhargava and Shankar [1, 2, 3, 4], relates n-coverings of elliptic curves to cocycles in the Galois cohomology of $E[n]$.

THEOREM 3. [1, 13] *There exists a canonical bijection between the set of n-coverings of E up to isomorphism and $H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n])$, which sends a covering (C, φ_C) to the cocycle ξ_C with $\xi_C(\sigma) = \sigma(\varphi_C)(Q) - \varphi_C(Q)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where $Q \in C(\overline{\mathbb{Q}})$ is any point.*

Proof. We follow the proof method of Silverman [13], Theorem X.2.2. First, to show that ξ_C is independent of the choice of $Q \in C(\overline{\mathbb{Q}})$ (and is valued in $E[n]$), note that the morphism $\sigma(\varphi_C) - \varphi_C \colon C \to E$ has image contained in $E[n]$ as $[n] \circ \varphi_C$ is a morphism defined over $\mathbb{Q}$ and $[n] \circ (\sigma(\varphi_C) - \varphi_C) = \sigma([n] \circ \varphi_C) - [n] \circ \varphi_C = O$ is the constant map sending C to the identity $O \in E$. As $\sigma(\varphi_C) - \varphi_C$ is a morphism of (irreducible) projective varieties with finite image ($E[n]$ has n^2 elements), it must be constant. The fact that the cochain ξ_C

associated to a covering (C, φ_C) is indeed a cocycle follows from the fact that

$$\begin{aligned}\xi_C(\sigma\tau) &= (\sigma(\varphi_C)(Q) - \varphi_C(Q)) + \sigma(\tau(\varphi_C)(\sigma^{-1}(Q)) - \varphi_C(\sigma^{-1}(Q))) \\ &= \xi_C(\sigma) + \sigma(\xi_C(\tau)),\end{aligned}$$

for any $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Next, to show that the correspondence is well-defined, we must show that isomorphic n-coverings (C, φ_C) and $(C', \varphi_{C'})$ of E give rise to the same element $[\xi_C] = [\xi_{C'}] \in H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n])$. If $\psi\colon C \to C'$ is an isomorphism over $\mathbb{Q}$ and $P \in E[n]$ such that $P + \varphi_C = \varphi_{C'} \circ \psi$,

$$\xi_{C'}(\sigma) - \xi_C(\sigma) = (\sigma(\varphi_{C'} \circ \psi))(Q) - (\varphi_{C'} \circ \psi)(Q) - (\sigma(\varphi_C)(Q) - \varphi_C(Q)) = \sigma(P) - P,$$

which is a coboundary for $E[n]$, as desired.

To see that the correspondence is injective, one notes that if for two n-coverings (C, φ_C) and $(C', \varphi_{C'}$, $\xi_{C'}(\sigma) - \xi_C(\sigma) = \sigma(P) - P$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and some $P \in E[n]$, the map $\psi\colon C \to C'$ with $\psi(Q) = \varphi_{C'}^{-1}(P + \varphi_C(Q))$ is an isomorphism of varieties over $\mathbb{Q}$ which, together with the point $P \in E[n]$, forms an isomorphism of n-coverings. (To check that ψ is defined over $\mathbb{Q}$, we may use the relation $\xi_{C'}(\sigma) - \xi_C(\sigma) = \sigma(P) - P$ to find that $\sigma(P) = (\sigma(\varphi_{C'}))(\psi(Q)) - (\sigma(\varphi_C))(Q)$ for any $Q \in C(\overline{\mathbb{Q}})$ and solve for $\sigma^{-1}(\psi(Q))$.)

Finally, we show that the correspondence is surjective. To each cocycle we will exhibit an n-covering of E mapping to that cocycle by constructing its function field. Suppose that $\xi \in H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E[n])$. Let $\overline{\mathbb{Q}}(E)_\xi$ denote the field $\overline{\mathbb{Q}}(E)$ endowed with the twisted Galois action $\sigma \star f = \sigma(f) \circ T_{\xi(\sigma)}$, where T_P denotes the translation-by-P isomorphism of E. Then we may choose a curve $C/\mathbb{Q}$ such that the function field $\mathbb{Q}(C)$ of C over $\mathbb{Q}$ is the fixed field $K := (\overline{\mathbb{Q}}(E)_\xi)^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$, with an isomorphism $\varphi_C\colon C \to E$ corresponding to the function field isomorphism $\overline{\mathbb{Q}}(E) \xrightarrow{\cong} \overline{\mathbb{Q}}(E)_\xi$. Such a curve $C/\mathbb{Q}$ exists as K is an extension of $\mathbb{Q}$ of transcendence degree 1 containing no nontrivial algebraic extensions of $\mathbb{Q}$ (see for example [13], Remark II.2.5). The pair (C, φ_C) forms an n-covering of E as $[n] \circ \varphi_C$ corresponds to the homomorphism of function fields $\overline{\mathbb{Q}}(E) \xrightarrow{\circ[n]} \overline{\mathbb{Q}}(E) \xrightarrow{\cong} \overline{\mathbb{Q}}(E)_\xi$, which restricts to a homomorphism $\mathbb{Q}(E) \to K$ (so that $[n] \circ \varphi_C$ is defined over $\mathbb{Q}$) since $[n]\xi(\sigma) = O$ and hence $\sigma \star (f \circ [n]) = \sigma(f) \circ ([n] \circ T_{\xi(\sigma)}) = \sigma(f) \circ [n] = f \circ [n]$ for any $f \in \mathbb{Q}(E)$. It is straightforward to check that (C, φ_C) indeed does correspond to the cocycle ξ, concluding the proof. □

To describe elements of the n-Selmer group of E, we must determine the inverse image of $\mathrm{Sel}_n E/\mathbb{Q}$ under the bijection of Theorem 3. In order to do so, as in [1], we will make the following definitions. A *soluble n-covering* of E is an n-covering (C, φ_C) such that $C(\mathbb{Q}) \neq \emptyset$. A *locally soluble n-covering* of E is an n-covering (C, φ_C) satisfying the local conditions $C(\mathbb{Q}_\nu) \neq \emptyset$ for all places ν of $\mathbb{Q}$.

Then if C has a rational point Q, $\xi_C(\sigma) = \sigma(\phi_C(Q)) - \phi_C(Q)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $[\xi_C] = 0 \in H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E)$ as it is the coboundary of $\phi_C(Q) \in E(\overline{\mathbb{Q}})$. Similarly, if C has a point Q defined over $\mathbb{Q}_\nu$ for some place ν of $\mathbb{Q}$, we find that ξ_C has trivial image in $H^1(\mathrm{Gal}(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_\nu), E(\overline{\mathbb{Q}_\nu}))$ (it is the coboundary of the point $\varphi_C(Q) \in E(\overline{\mathbb{Q}}) \subseteq E(\overline{\mathbb{Q}_\nu})$). Moreover, the converse to both of these statements holds: If ξ_C has trivial image in $H^1(\overline{K}/K, E(\overline{K}))$ (for $K = \mathbb{Q}$ or $\mathbb{Q}_\nu$ for some place ν of $\mathbb{Q}$), then it is the coboundary of some $P \in E(\overline{K})$, and we can verify that $\varphi_C^{-1}(P) \in C(K)$ as $\sigma(P) - P = \sigma(\varphi_C)(\varphi_C^{-1}(P)) - P$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We may summarize these observations using the exact sequences in Section 1 in the following corollary.

Corollary 4. [1] *The bijection of Theorem 3 induces a canonical bijection between the set of soluble n-coverings of E up to isomorphism and $E(\mathbb{Q})/nE(\mathbb{Q})$, and a canonical bijection between the set of locally soluble n-coverings of E up to isomorphism and* $\mathrm{Sel}_n E/\mathbb{Q}$.

In order to construct parametrizations for 2-Selmer groups in terms of orbits of a vector space under the action of a matrix group, we will need the following result due to Cassels [6] on the existence of certain divisors on n-coverings, which will prove in full generality. As we will see in Section 3, this result will enable us to use the Riemann-Roch Theorem to find a polynomial relation between appropriately chosen linearly independent functions in the function field of C. This theorem can also be used to construct the similar parametrization of 3-Selmer groups by orbits of ternary cubic forms.

THEOREM 5. [6] (Cassels, 1962) *If (C, φ_C) is a locally soluble n-covering of E, there is a positive divisor D on C, defined over $\mathbb{Q}$, such that* $\deg D = n$.

Proof. We follow the proof method in [6]. As $\operatorname{Pic} E(\overline{\mathbb{Q}}) \cong E(\overline{\mathbb{Q}})$ via the map $[P - O] \mapsto P$, we see that if $P, P' \in E[n]$, $nP - nP' = n(P-O) - n(P'-O)$ is linearly equivalent to the divisor 0, so that nP and nP' are linearly equivalent divisors. Thus, if we define the divisor $D' := nQ$ for $Q \in C(\overline{\mathbb{Q}})$ such that $[n]\varphi_C(Q) = O$, the linear equivalence class of D' does not depend on the choice of Q, and D' is linearly equivalent to its Galois conjugates. In other words, for each $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we may choose a function $f_\sigma \in \overline{\mathbb{Q}}(C)$ for which $\sigma(D') - D' = \operatorname{div} f_\sigma$. As $\deg D' = n$, it suffices to show that D' is linearly equivalent to a divisor D on C defined over $\mathbb{Q}$.

To accomplish this, we will construct a function $g \in \overline{\mathbb{Q}}(C)$ such that $\operatorname{div} \sigma(g)/g = \sigma(D') - D'$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so that $\sigma(D' - \operatorname{div} g) = D' - \operatorname{div} g$. For such a function g, we see that f_σ and $\sigma(g)/g$ have the same divisor, from which we can conclude that $f_\sigma/(\sigma(g)/g)$ would be a constant in $\overline{\mathbb{Q}}^\times$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In order to construct the function g, we will first construct a cochain $\xi \in C^1(\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{Q}}^\times)$ such that $\sigma \mapsto f_\sigma/\xi(\sigma)$ is a cocycle, and then show that $\sigma \mapsto f_\sigma/\xi(\sigma)$ is also a coboundary.

First, we will use the Brauer-Hasse-Noether theorem (see for example [11], Theorem 14.11) – in particular, that the map $H^2(\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{Q}}^\times) \to \prod_\nu H^2(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_\nu, \overline{\mathbb{Q}_\nu}^\times)$ is an injection – to make use of the condition that (C, φ_C) is locally soluble. For any $\sigma, \tau \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let $\alpha(\sigma, \tau) := \sigma(f_\tau) f_\sigma / f_{\sigma\tau}$. Then

$$\operatorname{div} \alpha(\sigma, \tau) = \sigma(\tau(D') - D') + (\sigma(D') - D') - (\sigma\tau(D') - D') = 0,$$

hence $\alpha(\sigma, \tau)$ corresponds to a non-surjective morphism $C \to \mathbb{P}^1$ (as it has no zeroes or poles), so is a constant in $\overline{\mathbb{Q}}^\times$. By a quick calculation, we can show that α is a cocycle and consequently $[\alpha] \in H^2(\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{Q}}^\times)$. But, as (C, φ_C) is locally soluble, we may choose a point $P_\nu \in C(\mathbb{Q}_\nu)$ for any place ν of $\mathbb{Q}$. Since $\sigma(P) = P$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_\nu)$, we find that $\alpha(\sigma, \tau) = \sigma(f_\tau(P_\nu)) f_\sigma(P_\nu)/f_{\sigma\tau}(P_\nu) \in Z^2(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_\nu, \overline{\mathbb{Q}_\nu}^\times)$ is the coboundary of the cochain $\sigma \mapsto f_\sigma(P_\nu)$, and $[\alpha]$ is locally trivial. Thus, by the Brauer-Hasse-Noether theorem, α is the coboundary of some cochain $\xi \in C^1(\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{Q}}^\times)$.

Next, by a generalization of Hilbert's Theorem 90, $H^1(\overline{\mathbb{Q}}/\mathbb{Q}, \overline{\mathbb{Q}}(C)^\times) = 1$ (this can be proved in the same manner as Hilbert's Theorem 90). Then as ξ and the cochain $\sigma \mapsto f_\sigma$ have the same coboundary, the cochain $\sigma \mapsto f_\sigma/\xi(\sigma)$ is a cocycle. By the generalization of Hilbert's Theorem 90 mentioned above, $\sigma \mapsto f_\sigma/\xi(\sigma)$ is the coboundary of some function $g \in \overline{\mathbb{Q}}(C)$. It follows from the discussion earlier in the proof that the divisor $D := D' - \operatorname{div} g$ is the desired divisor of degree n defined over $\mathbb{Q}$. □

3. 2-Selmer Groups and Binary Quartic Forms.

In this section we will describe a correspondence due to Birch and Swinnerton-Dyer [5], and made explicit by Cremona [14], between the 2-Selmer group and a class of orbits of an action on the space of binary quartic forms over $\mathbb{Q}$ by the group $\mathrm{PGL}_2 \mathbb{Q}$.

First, let us describe the action and its invariant polynomials, following [1, 5, 7, 14]. Let

$$V(\mathbb{Q}) := \{ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \mid a, b, c, d, e \in \mathbb{Q}\}$$

be the 5-dimensional vector space of binary quartic forms over $\mathbb{Q}$. For any $M \in \mathrm{PGL}_2 \mathbb{Q}$ and any $f \in V(\mathbb{Q})$, we define $Mf(X, Y) := (\det M)^{-2} f(M^\top(X, Y))$. We can make analogous definitions for $V(\mathbb{Z})$ and $V(\mathbb{R})$. By making the action explicit in terms of the coefficients of the quartic form, it can be easily checked that the polynomials

$$\begin{aligned} I(f) &:= 12ae - 3bd + c^2 \\ J(f) &:= 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3 \end{aligned}$$

on $V(\mathbb{Q})$, for $f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, are invariant under the action by $\mathrm{PGL}_2 \mathbb{Q}$. With more elaborate computations due to Cremona [7], it can be shown that to any binary quartic form $f \in V(\mathbb{Q})$

with invariants I and J we can associate a projective curve C_f isomorphic to the elliptic curve $Y^2Z = X^3 - IXZ^2/3 - JZ^3/27$.

PROPOSITION 6. [7] (Cremona, 2001) *Let $f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be a binary quartic form in $V(\mathbb{Q})$, and let C_f be a projective curve with affine part defined by the equation $y^2 = f(x, 1)$. (We will define C_f as the blow-up of the (singular) projective curve $Y^2Z^2 = f(X, Y)$ in $\mathbb{P}^2$ at the point $[X : Y : Z] = [0 : 0 : 1]$.) Then there is an isomorphism φ_{C_f}, defined over $\overline{\mathbb{Q}}$, from C_f to the elliptic curve E defined by the equation $Y^2Z = X^3 - I(f)XZ^2/3 - J(f)Z^3/27$, making (C_f, φ_{C_f}) into a 2-covering of E, that is, where $[2] \circ \varphi_{C_f}$ is a morphism of degree 4 defined over $\mathbb{Q}$. This isomorphism can be chosen to have the property that the inverse image of the identity $O \in E$ is the set of points in C_f with y-coordinate 0.*

Now, we must consider the converse – for any given elliptic curve $E/\mathbb{Q}$, is every locally soluble 2-covering of the form prescribed by Lemma 6? This question turns out to have a positive answer, and an equation of the desired form for any locally soluble 2-covering may be obtained by applying the Riemann-Roch theorem to the divisor of Theorem 5, as described below.

THEOREM 7. [5] (Birch, Swinnerton-Dyer, 1963) *Let E be an elliptic curve over $\mathbb{Q}$ and let (C, φ_C) be a locally soluble 2-covering of $E/\mathbb{Q}$. Then there exists a binary quartic form $f(x, y) \in V(\mathbb{Q})$ such that $C \cong C_f$ over $\mathbb{Q}$, where C_f is the projective curve defined in Proposition 6.*

Proof. We follow the proof method in [5]. As (c, φ_C) is a locally soluble 2-covering of E, we may apply Theorem 5 to construct a divisor D on C defined over $\mathbb{Q}$ and of degree 2. Following the notation in [13], §II.5, for any divisor D_0 on C, let $\mathcal{L}(D_0)$ be the $\overline{\mathbb{Q}}$-vector space of all functions $f \in \overline{\mathbb{Q}}(C)$ whose divisor is at least $-D_0$, and let $\ell(D_0) := \dim_{\overline{\mathbb{Q}}} \mathcal{L}(D_0)$. The Riemann-Roch Theorem then implies that $\ell(nD) = 2n$ for all $n \in \mathbb{N}$, for C has genus 1, and that $\ell(\widetilde{D}) = 1$ for all divisors $\widetilde{D}$ of degree 1. In addition (see [13], Proposition II.5.8), as nD is defined over $\mathbb{Q}$, $\mathcal{L}(nD)$ has a basis contained in $\mathbb{Q}(C)$. In particular, we see that $\mathcal{L}(\widetilde{D}) = \overline{\mathbb{Q}}$ for any divisor $\widetilde{D}$ of degree 1, and that $\ell(D) = 2$, $\ell(2D) = 4$, and $\ell(4D) = 8$ – the utility of these particular dimensions will be apparent shortly.

Choose functions $w, x \in \mathbb{Q}(C)$ such that $\{1, x\}$ is a basis for $\mathcal{L}(D)$ and $\{1, w, x, x^2\}$ is a basis for $\mathcal{L}(2D)$. Then $S := \{1, x, x^2, x^3, x^4, w, w^2, wx, wx^2\}$ cannot be a linearly independent subset of $\mathcal{L}(4D)$, as the latter is an 8-dimensional vector space, and S has 9 elements. It follows that there is a linear relation between the 9 elements of S, say of the form

$$g(w, x) := u_0w^2 + u_1wx^2 + u_2wx + u_3w - (v_0x^4 + v_1x^3 + v_2x^2 + v_3x + v_4) = 0$$

for some constants $u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3, v_4 \in \mathbb{Q}$.

Let us try to simplify this relation to the desired form. As we know that $\mathcal{L}(\widetilde{D}) = \overline{\mathbb{Q}}$ for any divisor $\widetilde{D}$ of degree 1, and $x \notin \overline{\mathbb{Q}}$, we see that $(\operatorname{div} x)|_{\operatorname{supp} D} = -D$ as the divisor of poles of x must have degree 2. First, we claim that $u_0 \neq 0$. If $u_0 = 0$, we find that

$$w = \frac{v_0x^4 + v_1x^3 + v_2x^2 + v_3x + v_4}{u_1x^2 + u_2x + u_3},$$

which either will have poles outside of $\operatorname{supp} D$ or will have the incorrect order on $\operatorname{supp} D$, unless $u_1 = u_2 = u_3 = v_0 = v_1 = 0$. However, this contradicts the fact that $\{1, w, x, x^2\}$ forms a basis for $\mathcal{L}(2D)$.

Now consider the binary quadratic form

$$f(X, Y) := \frac{v_0}{u_0}X^4 + \frac{v_1}{u_0}X^3Y + \frac{v_2}{u_0}X^2Y^2 + \frac{v_3}{u_0}XY^3 + \frac{v_4}{u_0}Y^4 + \frac{1}{4u_0^2}(u_1X^2 + u_2XY + u_3Y^2)^2.$$

If we define $z := w + \frac{1}{2u_0}(u_1x^2 + u_2x + u_3)$, it follows from the relation $g(w, x) = 0$ that $z^2 = f(x, 1)$. This results in a homomorphism of function fields $\mathbb{Q}(C_f) = \operatorname{Frac} \mathbb{Q}[x, z]/(z^2 - f(x, 1)) \to \mathbb{Q}(C)$. To see that this homomorphism is injective, note that if $h(x, z) = 0$ for some polynomial $h \notin (z^2 - f(x, 1)) \subseteq \mathbb{Q}[x, z]$, we may substitute the relation $z^2 = f(x, 1)$ into the equation $h(x, z) = 0$ to find that $z \in \mathbb{Q}(x)$. This is impossible

by the same argument we used to show that $u_0 \neq 0$. To see that this homomorphism is surjective, note that $x\colon C \to \mathbb{P}^1$ is a function with exactly 2 poles (counting multiplicity), x has degree 2, so that $\mathbb{Q}(C)$ is an extension of $\mathbb{Q}(x)$ of degree 2. As $\mathbb{Q}(C_f)$ is already an extension of $\mathbb{Q}(x)$ of degree 2, the map $\mathbb{Q}(C) \to \mathbb{Q}(C_f)$ is an isomorphism.

In conclusion, we find that there is an isomorphism of curves $C \cong C_f$ defined over $\mathbb{Q}$ ([13], Remark II.2.5), so that we may identify C with the curve in $\mathbb{P}^2$ cut out by the equation $y^2z^2 = f(x, y)$, as desired. □

Following [1], let us say that a binary quartic form $f \in V(\mathbb{Q})$ is *soluble* if the curve C_f in P^2 defined by the equation $y^2z^2 = f(x, y)$ has a point defined over $\mathbb{Q}$, and that a binary quartic form $f \in V(\mathbb{Q})$ is *locally soluble* if the curve C_f has a point defined over $\mathbb{Q}_\nu$ for all places ν of $\mathbb{Q}$. Combining Corollary 4, Proposition 6, and Theorem 7, we obtain the following result.

THEOREM 8. [1, 5, 7, 14] *Fix $I, J \in \mathbb{Q}$. Then there is a canonical bijection between $\mathrm{PGL}_2\mathbb{Q}$-orbits of locally soluble binary quartic forms $f \in V$ with $I(f) = I$ and $J(f) = J$, and elements of the 2-Selmer group $\mathrm{Sel}_2 E/\mathbb{Q}$ for E the elliptic curve over $\mathbb{Q}$ defined by the equation $Y^2 = X^3 - IX/3 - J/27$.*

Proof. By applying Corollary 4, Proposition 6, and Theorem 7, we see that the theorem follows from the following two facts. First, if (C, φ_C) is a locally soluble 2-covering of the elliptic curve E with equation $Y^2 = X^3 - IX/3 - J/27$, then we claim that $C \cong C_f$ over $\mathbb{Q}$ for some $f \in V(\mathbb{Q})$ with invariants $I(f) = I$ and $J(f) = J$. By Proposition 6, this follows from the fact that if C is a 2-covering of two elliptic curves E and E' defined over $\mathbb{Q}$, then $E \cong E'$ over $\mathbb{Q}$. This fact can be justified as follows. If (C, φ_C) is a 2-covering of E and (C, φ'_C) is a 2-covering of E', we see that $(\varphi'_C \circ \varphi_C^{-1}) \circ ([2] \circ \varphi_C) = [2] \circ \varphi'_C$, so that the composition of the morphism $[2] \circ \varphi_C\colon C \to E$ defined over $\mathbb{Q}$ with the isomorphism $\phi := \varphi'_C \circ \varphi_C^{-1}\colon E \to E'$ is a morphism defined over $\mathbb{Q}$. Checking Galois actions, we see that $\phi\colon E \to E'$ is an isomorphism defined over $\mathbb{Q}$.

Second, we claim that for any binary quartic forms $f, g \in V(\mathbb{Q})$ with common invariants, that is, $I := I(f) = I(g)$ and $J := J(f) = J(g)$, the 2-coverings (C_f, φ_{C_f}) and (C_g, φ_{C_g}) of the elliptic curve with equation $Y^2 = X^3 - IX/3 - J/27$ are isomorphic if and only if f and g are in the same $\mathrm{PGL}_2\mathbb{Q}$-orbit. First, if $g = Mf$ for some $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2\mathbb{Q}$ (and hence $M \in \mathrm{SL}_2\mathbb{Q}$), the map of function fields $\mathbb{Q}(C_f) = \mathrm{Frac}\,\mathbb{Q}[x, y]/(y^2 - f(x, 1)) \to \mathrm{Frac}\,\mathbb{Q}[x, y]/(y^2 - g(x, 1)) = \mathbb{Q}(C_g)$ defined by $x \mapsto \frac{ax+b}{cx+d}$ and $y \mapsto \frac{y}{(cx+d)^2}$ is an isomorphism, and by [13], Theorem II.2.4, this isomorphism induces an isomorphism of curves $C_f \cong C_g$ over $\mathbb{Q}$. The fact that this isomorphism of curves corresponds to an isomorphism of 2-covering spaces follows from the $\mathrm{PGL}_2\mathbb{Q}$-invariance properties of the maps $C_f \to E$ and $C_g \to E$, as outlined in [7]. On the other hand, if (C_f, φ_{C_f}) and (C_g, φ_{C_g}) are isomorphic 2-coverings of E, following [5], we note that there is an isomorphism $\psi\colon C_f \to C_g$ defined over $\mathbb{Q}$ with the points on C_f with y-coordinate 0 sent to the points on C_g with y-coordinate 0, by Proposition 6. The corresponding isomorphism of function fields $\psi^*\colon \mathbb{Q}(C_g) \to \mathbb{Q}(C_f)$ has $\psi(y)$ to be a function whose zeros are precisely the zeroes of y. Since the poles of y have double the order of the poles of x, we deduce that $\psi^*(y) = y/h_1(x)$, $\psi^*(y/x) = y/h_2(x)$, and $\psi^*(y/x^2) = y/h_3(x)$ for nonzero quadratic polynomials h_1, h_2, and h_3, so that ψ^* restricts to an automorphism of $\mathbb{Q}(x)$. Now the automorphisms of $\mathbb{P}^1_{\mathbb{Q}}$ are linear fractional transformations, hence we see that $\psi^*(x) = \frac{ax+b}{cx+d}$ for some $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2\mathbb{Q}$. By the construction of h_3, we see that h_1 is a quadratic polynomial divisible by $(cx+d)^2$, and hence that f and g are in the same $\mathrm{PGL}_2\mathbb{Q}$-orbit (as can be seen by comparing invariants). □

In order to count binary quartic forms via a method estimating a lattice by a volume, it would be helpful to make the space of binary quartic forms in question discrete, by for instance restricting to integer binary quartic forms. We refer the reader to [5] for proofs, but the integral version of Theorem 8 is stated below.

THEOREM 9. [1, 5, 7, 14] *Fix $A, B \in \mathbb{Z}$. Then there is a canonical bijection between $\mathrm{PGL}_2\mathbb{Z}$-orbits of locally soluble binary quartic forms $f \in V(\mathbb{Z})$ with $I(f) = -(2^4 \cdot 3)I$ and $J(f) = -(2^6 \cdot 3^3)J$, and elements of the 2-Selmer group $\mathrm{Sel}_2 E/\mathbb{Q}$ for E the elliptic curve over $\mathbb{Q}$ defined by the equation $Y^2 = X^3 + AX + B$.*

4. Counting Binary Quartic Forms.

Recall from Section 3 that there is a bijective correspondence between the elements of the 2-Selmer group of an elliptic curve E defined by the equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, and $\mathrm{PGL}_2\mathbb{Z}$-orbits of binary

quartic forms $f \in V(\mathbb{Z})$ with invariants $I(f) = -3A$ and $J(f) = -27B$. Then one of the key ingredients in the proof of Theorem 1 is the following result on counting binary quartic forms satisfying a finite number of congruence conditions whose invariants (I, J) have bounded height. To determine the average size of the 2-Selmer group, Bhargava and Shankar [1] use this theorem, and perform a sieve to account for the infinitely many congruence conditions that arise from local solubility of the binary quartic forms to be counted.

THEOREM 10. [1] (Bhargava, Shankar, 2015) *Let $X > 0$ and let $H(I, J) := \max\{|I|^3, J^2/4\}$ (note that this is $27/4$ times the height of the corresponding elliptic curve as defined in Theorem 1). For $i \in \{0, 1, 2+, 2-\}$, let $V^{(i)}(\mathbb{Z})$ be the set of irreducible binary quartic forms $f \in V(\mathbb{Z})$ with exactly $2i$ complex roots (which is positive definite for $i = 2+$ and is negative definite for $i = 2-$). In addition, let $S \subseteq V(\mathbb{Z})$ be a set defined by a finite set of congruence conditions with p-adic volume $\mu_p(S)$ for each prime p, and let*

$$\mathcal{N}(V^{(i)}(\mathbb{Z}) \cap S, X) := |\{f \in V^{(i)}(\mathbb{Z}) \cap S \mid H(I(f), J(f)) \leq X\}|.$$

Then

$$\mathcal{N}(V^{(i)}(\mathbb{Z}) \cap S, X) = C_i \zeta(2) \left(\prod_{p \text{ prime}} \mu_p(S) \right) X^{5/6} + O(X^{3/4+\varepsilon})$$

as $X \to \infty$ for any $\varepsilon > 0$, where

$$C_i = \begin{cases} 4/135 & i = 0, 2+, 2- \\ 32/135 & i = 1 \ . \end{cases}$$

The proof [1] of this theorem involves several steps. First, one splits the theorem into computing the volume of the space of orbits of $\{f \in V^{(i)}(\mathbb{R}) \mid H(I(f), J(f)) \leq X\}$ under the action of $\mathrm{PGL}_2 \mathbb{Z}$ by using an appropriate fundamental domain, and using the volume of this region to estimate the number of irreducible lattice points contained in the region. The latter problem is subdivided into further steps – first applying Davenport's Lemma [10] to an appropriate subset of the fundamental domain (avoiding cusps), and then estimating the number of reducible binary quartic forms in $V^{(i)}(\mathbb{Z}) \cap S$ and the number of binary quartic forms in $V^{(i)}(\mathbb{Z}) \cap S$ with large $\mathrm{PGL}_2 \mathbb{Z}$-stabilizer, in order to compute the error term.

LEMMA 11. [1] *For any $X > 0$, defined $V^{(i)}(\mathbb{R}, X) := \{f \in V^{(i)}(\mathbb{R}) \mid H(I(f), J(f)) \leq X\}$. Then the volume $\mathrm{Vol}\, \mathrm{PGL}_2 \mathbb{Z} \backslash V^{(i)}(\mathbb{R}, X)$ of the set of $\mathrm{PGL}_2 \mathbb{Z}$-orbits of real binary quartic forms with height at most X is $\frac{4\zeta(2)}{135} X^{5/6}$ if $i = 0, 2+$, or $2-$, and is $\frac{32\zeta(2)}{135} X^{5/6}$ if $i = 1$.*

Proof. We follow the proof in [1]. For simplicity, we will just consider the case $i = 0$, the results for other values of i can be obtained by similar methods. We will compute this volume by taking a fundamental domain for the action of $\mathrm{PGL}_2 \mathbb{R}$ on $V^{(i)}(\mathbb{R})$. We will choose a fundamental domain for this action which contains one form in $V^{(0)}(\mathbb{R})$ with invariants I and J for each choice of (I, J) with $H(I, J) = 1$ and $I = 1$; in particular, we will let

$$R := \{f_{c,j} := c(x^3 y - xy^3/3 - jy^4/27) \mid j \in (-2, 2), c > 0\} \subseteq V^{(0)}(\mathbb{R}).$$

This set R is a fundamental domain as every polynomial $f \in V^{(0)}(\mathbb{R})$ satisfies the relation $\Delta(f) := \frac{1}{27}(4I(f)^3 - J(f)^2) > 0$, and for every pair (I, J) of invariants with this property, there is exactly one $\mathrm{PGL}_2 \mathbb{R}$-orbit of $V^{(0)}(\mathbb{R})$ with invariants I and J (see Cremona [8]).

As $I(f_{c,j}) = c^2$ and $J(f_{c,j}) = c^3 j$, we see that for any fundamental domain $\phi : \mathrm{PGL}_2 \mathbb{R} \to \mathbb{R}_{\geq 0}$ for the action on $\mathrm{PGL}_2 \mathbb{R}$ by $\mathrm{PGL}_2 \mathbb{Z}$,

$$\mathrm{Vol}\, \mathrm{PGL}_2 \mathbb{Z} \backslash V^{(0)}(\mathbb{R}, X) = \int_{\mathrm{PGL}_2 \mathbb{R}} \int_R \frac{1}{\mathrm{Stab}_{\mathrm{PGL}_2 \mathbb{R}} f_{c,j}} \phi(g) \cdot 1_{c < X^{1/6}}(f_{c,j}) d(g f_{c,j}).$$

We will now use the result ([1], Proposition 2.8) that the Jacobian of the change-of-basis transformation sending $d(g f_{c,j})$ to $dg dI dJ$ is $1/27$, and the result due to Cremona and Fisher [9] that the stabilizer of any

element of $V^{(0)}(\mathbb{R})$ under the action of $\mathrm{PGL}_2\mathbb{R}$ has size 4. This implies that

$$\mathrm{Vol}\,\mathrm{PGL}_2\mathbb{Z}\backslash V^{(0)}(\mathbb{R},X) = \frac{1}{108}(\mathrm{Vol}\,\mathrm{PGL}_2\mathbb{Z}\backslash\mathrm{PGL}_2\mathbb{R})\int_{\substack{0<I<X^{1/3}\\ 0\leq|J|<2I^{3/2}}} dIdJ = \frac{1}{108}\cdot 2\zeta(2)\cdot\frac{8}{5}X^{5/6},$$

as desired. □

Now, we outline how to approximate the number of orbits of integer binary quartic forms by this volume, as done by Bhargava and Shankar [1]. By Davenport's Lemma [10], we can estimate $\mathcal{N}(V^{(i)}(\mathbb{Z}),X)$ by the volume computed in Lemma 11, but with error term given by the maximum volume of a projection to a 4-dimensional subspace of $V(\mathbb{R})$ of a fundamental domain for the action of $\mathrm{PGL}_2\mathbb{Z}$ on $V^{(i)}(\mathbb{R},X)$.

Some of the technicalities are as follows. To remove problems in counting points on the cusps (and to only need to compute 5-dimensional volumes), we will average over an appropriately chosen compact set $K\subseteq\mathrm{PGL}_2\mathbb{R}$. Then we use a bounded fundamental domain Ω for the action of $\mathrm{PGL}_2\mathbb{Z}$ on $\mathrm{PGL}_2\mathbb{R}$ associated to the Iwasawa decomposition, and count using Davenport's Lemma the number of points in $V^{(0)}(\mathbb{Z})$ that are contained within the product of a given translate of the compact set K with the set of binary quartic forms in R with height bounded by X. The conditions in Davenport's Lemma turn out to give a error bound of order $O_\varepsilon(X^{3/4+\varepsilon})$ for any $\varepsilon>0$, after integrating over all translates of K (which corresponds to an integral over the fundamental domain Ω); see [1] for details. Via working with the explicit fundamental domain Ω, Bhargava and Shankar [1] prove that the volume of the space of orbits of reducible binary quartic forms has order $O(X^{2/3})<O(X^{3/4})$ (in [1], Lemma 2.3), so that this volume is insignificant. To add congruence conditions modulo q (with k allowable congruence classes) for some q, we simply scale the problem by q and sum over k translates. Combining these methods, Theorem 10 follows.

References

[1] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Math. **181** (2015), pp. 191–242

[2] M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Annals of Math. **181** (2015), pp. 587–621

[3] M. Bhargava, A. Shankar, *The average number of elements in the 4-Selmer groups of elliptic curves is 7*, arxiv: 1312.7333 (2013)

[4] M. Bhargava, A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, arxiv: 1312.7859 (2013)

[5] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves I*, J. fur Reine Angew. Math. **212** (1963), pp. 7–25

[6] J. W. S. Cassels, *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung*, J. fur Reine Angew. Math. **211** (1962), pp. 95–112

[7] J. E. Cremona, *Classical Invariants and 2-descent on Elliptic Curves*, J. Symbolic Computation **31** (2001), pp. 71–87

[8] J. E. Cremona, *Reduction of Binary Cubic and Quartic Forms*, LMS J. Comput. Math. **2** (1999), pp. 62–92

[9] J. E. Cremona, T. A. Fisher, *On the equivalence of binary quartics*, J. Symbolic Computation **44** (2009), pp. 673–682

[10] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), pp. 179–183

[11] D. Harari, *Galois Cohomology and Class Field Theory*, Springer-Verlag–EDP Sciences (2020)

[12] B. Mazur, *Modular Curves and the Eisenstein Ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), pp. 33–186

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag GTM **106** (2009)

[14] M. Stoll, J. E. Cremona, *Minimal Models for* 2*-coverings of Elliptic Curves*, LMS J. Comput. Math. **5** (2002), pp. 220–243