The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$

Manjul Bhargava, Noam Elkies, and Ari Shnidman

June 29, 2019

Abstract

The elliptic curve $E_k\colon y^2 = x^3+k$ admits a natural 3-isogeny $\phi_k\colon E_k \to E_{-27k}$. We compute the average size of the ϕ_k-Selmer group as k varies over the integers. Unlike previous results of Bhargava and Shankar on n-Selmer groups of elliptic curves, we show that this average can be very sensitive to congruence conditions on k; this sensitivity can be precisely controlled by the Tamagawa numbers of E_k and E_{-27k}. As consequences, we prove that the average rank of the curves E_k, $k \in \mathbb{Z}$, is less than 1.21 and over 23% (resp. 41%) of the curves in this family have rank 0 (resp. 3-Selmer rank 1).

1 Introduction

Let F be a field of characteristic not 2 or 3, and let $k \in F$ be nonzero. The elliptic curve

$$E_k\colon y^2 = x^3 + k \tag{1}$$

has j-invariant 0, and every elliptic curve E/F with $j(E) = 0$ is isomorphic to E_k for some $k \in F$. The curves E_k and $E_{k'}$ are isomorphic if and only if $k' = km^6$ for some $m \in F^\times$.

Over a separable closure $\overline{F}$, each E_k has complex multiplication by the Eisenstein integers $\mathbb{Z}[\zeta_3]$, and hence admits an endomorphism $\sqrt{-3}$ of degree 3. This endomorphism is not generally defined over F, but its kernel is, and consequently there is a 3-isogeny $\phi = \phi_k\colon E_k \to E_{k'}$ for some $k' \in F$. By duality, there is a 3-isogeny $\hat{\phi} = \hat{\phi}_k\colon E_{k'} \to E_k$ in the reverse direction. In fact, we may take $k' = -27k$, and then these isogenies are given explicitly by:

$$\phi_k\colon (x,y) \;\mapsto\; \left(\frac{x^3+4k}{x^2}\,,\,\frac{y(x^3-8k)}{x^3}\right), \tag{2}$$

$$\hat{\phi}_k\colon (x,y) \;\mapsto\; \left(\frac{x^3-108k}{9x^2}\,,\,\frac{y(x^3+216k)}{27x^3}\right). \tag{3}$$

After identifying E_{3^6k} and E_k, we have $\hat{\phi}_k = \phi_{-27k}$.

If F is a number field, then the *ϕ-Selmer group*

$$\mathrm{Sel}_\phi(E_k) \subset H^1(G_F, E_k[\phi])$$

associated to the isogeny ϕ consists of all "locally soluble" cohomology classes, i.e., those that are locally in the image of the connecting map

$$\partial_v\colon E_{-27k}(F_v) \longrightarrow H^1(G_{F_v}, E_k[\phi])$$

for every place v of F; here, $G_F = \mathrm{Gal}(\overline{F}/F)$.

In this paper, we take first $F = \mathbb{Q}$, and study the average size of the ϕ-Selmer group for the elliptic curves E_k as k varies. Let

$$r = \frac{103 \cdot 229}{2 \cdot 3^2 \cdot 7^2 \cdot 13} \prod_{p \equiv 5 \pmod 6} \frac{(1-p^{-1})(1+p^{-1}+\frac{5}{3}p^{-2}+p^{-3}+\frac{5}{3}p^{-4}+p^{-5})}{1-p^{-6}}. \tag{4}$$

Then we prove:

Theorem 1. *When the elliptic curves $E_k\colon y^2 = x^3 + k$, $k \in \mathbb{Z}$, are ordered by the absolute value of k, the average size of the ϕ_k-Selmer group associated to the 3-isogeny $\phi_k\colon E_k \to E_{-27k}$ is $1 + r$ if k is negative, and $1 + r/3$ if k is positive.*

We note that, in this theorem, we may take k to range over all integers or, if desired, only the sixth-power-free ones (so that we obtain each isomorphism class of elliptic curve over $\mathbb{Q}$ of j-invariant 0 exactly once). We can calculate the product in (4) efficiently by approximating it by a product of powers of the values at $s = 2, 3, 4, \ldots$ of $(1-2^{-s})(1-3^{-s})\zeta(s)$ and $(1+2^{-s})L(\chi, s)$ where χ is the Legendre symbol mod 3; we find that the product is numerically $1.03373551201736 4858\ldots$, so $r = 2.1265\ldots$, making $1 + r = 3.1265\ldots$ and $1 + r/3 = 1.7088\ldots$.

In fact, we are able to determine the average size of the ϕ_k-Selmer group of $E_k\colon y^2 = x^3 + k$ where k varies in any subset S of $\mathbb{Z}$ defined by finitely many—or, in suitable cases, infinitely many—congruence conditions. Let $S \subset \mathbb{Z}$ be any subset of integers defined by sign conditions and congruence conditions modulo a power of each prime, such that for all sufficiently large primes p, the closure S_p of S in $\mathbb{Z}_p$ contains all elements of $\mathbb{Z}_p$ not divisible by p^2. We call such a set *acceptable*. For example, the set of all sixth-power-free integers is acceptable. The set of all positive squarefree integers congruent to 1 (mod 3) is also acceptable.

For any isogeny $\phi\colon A \to A'$ of abelian varieties over a number field F, and for any place $\mathfrak{p}$ of F, we define the *local Selmer ratio of ϕ* at $\mathfrak{p}$ to be

$$c_{\mathfrak{p}}(\phi) := \frac{|A'(F_{\mathfrak{p}})/\phi(A(F_{\mathfrak{p}}))|}{|A[\phi](F_{\mathfrak{p}})|} \tag{5}$$

where $F_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of F. The following theorem gives the average size of the ϕ_k-Selmer group as k varies over the integers in $S \subset \mathbb{Z}$:

Theorem 2. *Let S be any acceptable set of integers. When the elliptic curves $E_k\colon y^2 = x^3 + k$, $k \in S$, are ordered by the absolute value of k, the average size of the ϕ-Selmer group associated to the 3-isogeny $\phi\colon E_k \to E_{-27k}$ is*

$$1 + \prod_{p \le \infty} \frac{\displaystyle\int_{k \in S_p} c_p(\phi_k)dk}{\displaystyle\int_{k \in S_p} dk}, \tag{6}$$

where for $p < \infty$, S_p denotes the p-adic closure of S in $\mathbb{Z}_p$ and dk denotes the usual Haar measure on $\mathbb{Z}_p$, and for $p = \infty$, S_p denotes the image of S in $\mathbb{R}^*/\mathbb{R}^{*2}$ and dk denotes the uniform measure.

Remark 3. The group $H^1(G_F, E_k[\phi])$ parametrizes isomorphism classes of ϕ-*coverings*, i.e., maps $f : C \to E_{-27k}$ of curves that become isomorphic to ϕ over $\overline{F}$. We can interpret the local Selmer ratio $c_p(\phi)$ as the number of soluble ϕ-coverings f over $\mathbb{Q}_p$, where each f is weighted by the inverse of the size of its automorphism group. Theorem 2 can thus be interpreted as saying that the expected (weighted) number of nontrivial locally soluble ϕ-coverings over $\mathbb{Q}$ is simply the product of the (weighted) number of soluble ϕ-coverings over $\mathbb{Q}_p$. This suggests a Selmer-group analogue of Bhargava's conjectures for number fields [4], which would include as a special case the conjecture of Bhargava and Shankar that the average size of $\mathrm{Sel}_n(E)$ over any congruence family of elliptic curves over $\mathbb{Q}$ is $\sum_{d|n} d$.

For any given set S, the p-adic integrals in Theorem 2 can be evaluated explicitly using Proposition 34 in §4.1. In particular, when $S = \mathbb{Z}$, we recover Theorem 1.

We note that unlike the results of [7, 8, 9, 10] for the 2-, 3-, 4-, and 5-Selmer groups, respectively, the average size of the ϕ-Selmer group in Theorem 2 can depend very much on the congruences defining the set S. However, we show that we may partition the set of nonzero integers into a countable union $\cup_{m=-\infty}^{\infty} T_m$ of sets T_m, where each T_m is itself the union of countably many sets defined by congruence conditions, such that if $S \subset T_m$ is an acceptable set, then the average size of the ϕ-Selmer group of $E_k\colon y^2 = x^3 + k$, as k varies in S, depends only on m.

More precisely, we define the *global Selmer ratio*

$$c(\phi_k) := \prod_p c_p(\phi_k) \tag{7}$$

to be the product of the local Selmer ratios. If ϕ is an ℓ-isogeny, for some prime ℓ, then the global Selmer ratio $c(\phi)$ is evidently a power of ℓ.

The importance of the global Selmer ratio in the study of the Selmer groups $\mathrm{Sel}_\phi(E_k)$ is clearly seen in the following theorem.

Theorem 4. *For each $m \in \mathbb{Z}$, let $T_m := \{k \in \mathbb{Z}\colon c(\phi_k) = 3^m\}$. Then:*

(i) *Each T_m has positive density;*

(ii) *If $E_k(\mathbb{Q})$ and $E_{-27k}(\mathbb{Q})$ have trivial 3-torsion, then*

$$c(\phi_k) = \frac{|\mathrm{Sel}_\phi(E_k)|}{|\mathrm{Sel}_{\hat\phi}(E_{-27k})|};$$

hence if $k \in T_m$, then $-27k \in T_{-m}$.

(ii) *If $S = T_m$, or if S is any acceptable set contained in T_m, then the average size of $\mathrm{Sel}_\phi(E_k)$ over $k \in S$ equals $1 + 3^m$, and the average size of $\mathrm{Sel}_{\hat\phi}(E_{-27k})$ over $k \in S$ equals $1 + 3^{-m}$.*

Thus the average size of $\mathrm{Sel}_\phi(E_k)$ over $k \in S$ *is* independent of congruence conditions if we also fix the global Selmer ratio. The densities of the sets T_m, to three decimal places, are tabulated in Table 1, along with the densities of the subsets T_m^+ (respectively, T_m^-) of T_m consisting of its positive (respectively, negative) elements. We describe the sets T_m via explicit congruence conditions in §6.4.

Using Theorem 4 and the rigorous computation of the densities $\mu(T_m)$, we may obtain bounds on the limsup of the average 3-ranks of the ϕ- and $\hat\phi$-Selmer groups. These immediately imply a bound on the limsup of the average 3-rank of the 3-Selmer group $\mathrm{Sel}_3(E_k)$, and hence a bound on the limsup of the average rank of $E_k(\mathbb{Q})$ as k varies in $\mathbb{Z}$ ordered by absolute value. We prove the following theorem:

m	$\mu(T_m)$	$\mu(T_m^+)$	$\mu(T_m^-)$
-4	.000	.000	.000
-3	.004	.004	.000
-2	.067	.063	.004
-1	.295	.231	.063
0	.399	.167	.231
1	.199	.031	.167
2	.032	.000	.031
3	.000	.000	.000
4	.000	.000	.000

Table 1: Densities of the sets T_m, T_m^+, and T_m^- for $|m| \leq 4$.

Theorem 5. *The (limsup of the) average rank of the elliptic curves $E_k\colon y^2 = x^3 + k$ over $k \in \mathbb{Z}$ is less than* 1.29.

Theorem 5 immediately implies that a positive proportion of elliptic curves $E_k\colon y^2 = x^3 + k$ have rank 0 or 1. To produce positive proportions of curves having the individual ranks 0 or 1, we may make use of the fact in Theorem 4(ii) that for 100% of $k \in T_m$, the 3-rank of the ϕ-Selmer group of E_k is m more than that of its $\hat{\phi}$-Selmer group. This means, in particular, that 100% of the curves in T_0 have even 3-Selmer rank (Proposition 49(ii)). Since the average sizes of both the ϕ- and $\hat{\phi}$-Selmer groups are equal to 2, we conclude that at least 1/2 of all curves in T_0 must in fact have 3-Selmer rank 0. Hence we obtain the following theorem.

Theorem 6. *At least* 19.9% *of all elliptic curves $E_k\colon y^2 = x^3 + k$ with $k \in \mathbb{Z}$ have rank* 0.

Conditionally on the finiteness of the 3-primary part of the Shafarevich–Tate group, we may obtain a similar result for rank 1 elliptic curves by using instead the set $T_1 \cup T_{-1}$, for which the 3-Selmer parity is always odd.

Theorem 7. *Assume for all $k \in T_1 \cup T_{-1}$ that the* 3*-primary part of $\text{Ш}(E_k)$ is finite. Then at least* 41.1% *of all elliptic curves $E_k\colon y^2 = x^3 + k$ with $k \in \mathbb{Z}$ have rank* 1.

Combining Theorems 6 and 7, we obtain:

Corollary 8. *At least* 61% *of all elliptic curves $E_k\colon y^2 = x^3 + k$ with $k \in \mathbb{Z}$ have rank* 0 *or* 1.

Thus the majority of curves $E_k\colon y^2 = x^3 + k$ have rank 0 or 1.

Remark 9. Theorems 5, 6, and 7 and Corollary 8 can be improved slightly if we combine our results with those in Alpoge's thesis [1], where it is shown that the average size of $\mathrm{Sel}_2(E_k)$ over $k \in S$ is at most 3 (generalizing and streamlining earlier results of Ruth [37]). Indeed, this gives an average rank bound of 4/3 on any T_m, giving a better bound than ours for $m > 1$. The improvements are small since even T_2 has very small density: incorporating Alpoge's result, we can show that the average rank of E_k is at most 1.21, and the proportion of rank 0 curves is at least 23.2%.

Theorem 4 implies the following result concerning curves with fixed 3-Selmer rank:

Theorem 10. *For each $m \geq 0$, a positive proportion of elliptic curves $E_k\colon y^2 = x^3 + k$ with $k \in \mathbb{Z}$ have 3-Selmer rank m.*

Indeed, the average size of $\mathrm{Sel}_{\hat{\phi}}(E_k)$ is $1 + 3^{-m}$ for $k \in T_m$ and, therefore, a positive proportion of $k \in T_m$ satisfy $|\mathrm{Sel}_{\hat{\phi}}(E_k)| = 1$. By Theorem 4(ii), we then have $|\mathrm{Sel}_\phi(E_k)| = 3^m$ and thus $|\mathrm{Sel}_3(E_k)| = 3^m$ for most of these k. Taking into account Remark 9 and Selmer parity [21] we see that, for even m, Theorem 10 holds not just for $\mathrm{Sel}_3(E_k)$, but for $Ш(E_k)[3]$ as well.

Finally, using the methods of [12, 13], we can extend Theorem 2 to the case where the ground field is any number field F. To order the curves E_k, we think of k as an element of F^*/F^{*6}. There is a natural height function on F^*/F^{*6} defined as follows: if $\tilde{k} \in F^*$ is a representative for $k \in F^*/F^{*6}$, and $I(\tilde{k})$ denotes the $\mathcal{O}_F$-ideal

$$I(\tilde{k}) = \{a \in F\colon a^6\tilde{k} \in \mathcal{O}_F\},$$

then the *height* $H(k)$ of k is defined by

$$H(k) := N(I(\tilde{k}))^6 \prod_{\mathfrak{p} \in M_\infty} |\tilde{k}|_{\mathfrak{p}}$$

where M_∞ denotes the set of infinite places of F; this definition is evidently independent of the lift $\tilde{k}$ of k. Alternatively, $H(k)$ gives the norm of the unique sixth-power-free integral ideal representative of $k\mathcal{O}_F$ in the group of fractional $\mathcal{O}_F$-ideals modulo sixth powers. Then we have the following analogue of Theorem 2 over a general number field F:

Theorem 11. *When the elliptic curves E_k, $k \in F^*/F^{*6}$, are ordered by the height $H(k)$ of k, the average size of $\mathrm{Sel}_{\phi_k}(E_k)$ is*

$$1 + \prod_{\mathfrak{p}} \frac{\displaystyle\int_{k \in \mathcal{O}_{\mathfrak{p}}(6)} c_{\mathfrak{p}}(\phi_k)dk}{\displaystyle\int_{k \in \mathcal{O}_{\mathfrak{p}}(6)} dk},$$

where if $\mathfrak{p}$ is a finite place of F, then $\mathcal{O}_{\mathfrak{p}}(6) = \{k \in \mathcal{O}_{\mathfrak{p}}\colon v_{\mathfrak{p}}(k) < 6\}$ and dk denotes the Haar measure on $\mathcal{O}_{\mathfrak{p}}$, normalized so that $\mathcal{O}_{\mathfrak{p}}$ has volume 1, and if $\mathfrak{p}$ is an infinite place, then $\mathcal{O}_{\mathfrak{p}}(6) = F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*6}$ and dk is the uniform measure.

As over $\mathbb{Q}$, we actually prove a more general result (Theorem 51) that allows for subfamilies of sextic twists defined by finite (and indeed suitable infinite) sets of congruence conditions. In particular, this lets us prove the analogue of Theorem 4 over a general number field. To state the result, we define again the global Selmer ratio $c(\phi_k)$ of the isogeny ϕ_k by $c(\phi_k) = \prod_{\mathfrak{p}} c_{\mathfrak{p}}(\phi_k)$, where the product is over all places $\mathfrak{p}$ of F.

Theorem 12. *Let F be a number field, and for $m \in \mathbb{Z}$, let $T_m(F) := \{k \in F^*/F^{*6}\colon c(\phi_k) = 3^m\}$. Then:*

(i) *If $k \in T_m(F)$, and $E_k(F)$ and $E_{-27k}(F)$ have trivial 3-torsion, then $|\mathrm{Sel}_\phi(E_k)| = 3^m|\mathrm{Sel}_{\hat{\phi}}(E_{-27k})|$;*

(ii) *If $T_m(F)$ is nonempty, then the average size of $\mathrm{Sel}_\phi(E_k)$ over $k \in T_m(F)$ equals $1 + 3^m$, and the average size of $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ over $k \in T_m(F)$ equals $1 + 3^{-m}$.*

If $\sqrt{-3} \notin F$, then each $T_m(F)$ has positive density. However, if $\sqrt{-3} \in F$, then $F^*/F^{*6} = T_0(F)$, and $T_m(F)$ is empty for each $m \neq 0$.

Thus, if $\sqrt{-3} \notin F$, then the exact analogue of Theorem 4 holds over F. However, if $\sqrt{-3} \in F$, then each of $\mathrm{Sel}_\phi(E_k)$ and $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ has average size 2 as k varies over F^*/F^{*6}.

The dichotomy in Theorem 12 comes from the fact that the CM curve E_k obtains extra endomorphisms over F when $\sqrt{-3} \in F$. In fact, in this case, $E_k \simeq E_{-27k}$ and ϕ is multiplication by $\sqrt{-3}$, up to an automorphism. As corollaries of Theorem 12, we prove the following results on the ranks of the elliptic curves E_k over F:

Theorem 13. *Suppose F is a number field with $\sqrt{-3} \notin F$, and let the elliptic curves E_k, $k \in F^*/F^{*6}$, be ordered by the height of k. Then the average rank of the elliptic curves E_k over F is bounded. Moreover, a positive proportion of curves E_k have 3-Selmer rank 0 over F, and thus also Mordell-Weil rank 0; and a positive proportion of curves E_k have 3-Selmer rank 1 over F.*

Theorem 14. *Suppose F is a number field with $\sqrt{-3} \in F$, and let the elliptic curves E_k, $k \in F^*/F^{*6}$, be ordered by the height of k. Then each of the Selmer groups $\mathrm{Sel}_{\phi_k}(E_k)$ and $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ over F has average size 2. Furthermore, the average rank of the elliptic curves E_k is at most 1, and at least 50% of E_k have rank 0 over F.*

Remark 15. If $\sqrt{-3} \in F$, then $\mathbb{Z}[\sqrt{-3}]$ acts faithfully on each $E_k(F)$, and hence the ranks of the elliptic curves E_k over F are all even. It might thus be natural to expect that, in this case, the true proportion of elliptic curves E_k having rank 0 over F is 100%.

Theorems 13 and 14 give the first example (to our knowledge) of an algebraic family of elliptic curves with a positive proportion of rank 0 members, over a general number field F:

Corollary 16. *Over any number field F, there exists a non-trivial algebraic family of elliptic curves with a positive proportion of specializations having rank 0.*

Our methods in obtaining the above results involve the connection between ϕ-Selmer groups and binary cubic forms. This connection was first studied by Selmer himself [41], and later by Cassels [17]. The rational theory was thoroughly treated by Satgé [38], where he studied the ϕ-Selmer group from the point of view of cubic fields. Later, Liverance [30] studied these Selmer groups using the classical invariant theory of binary cubics.

The boundedness of the average size of the ϕ- and $\hat{\phi}$-Selmer groups—and thus the rank—of the elliptic curves $E_k\colon y^2 = x^3+k$ over $\mathbb{Q}$ was first demonstrated by Fouvry [25], who used Satgé's results to reduce the boundedness of the average rank to the theorem of Davenport and Heilbronn [20] on the boundedness of the average size of the 3-torsion subgroups of the class groups of quadratic fields. Fouvry's method thus implicitly used binary cubic forms, as Davenport and Heilbronn's proof on the mean size of the 3-torsion of the class groups of quadratic fields used a count of integral binary cubic forms to count cubic fields of bounded discriminant, together with class field theory to transform this count to one about 3-torsion elements in class groups of quadratic fields.

Recently, in [15] a more direct proof of Davenport and Heilbronn's theorem on 3-torsion elements in class groups of quadratic fields was given. This proof used a count of *integer-matrix* binary cubic forms $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ $(a, b, c, d \in \mathbb{Z})$, together with a direct correspondence between 3-torsion ideal classes in quadratic fields and integer-matrix binary cubic forms as studied in [24, 3] (see Section 2 for a description of this correspondence over any Dedekind domain). This suggested to us that perhaps a direct and natural discriminant-preserving map from ϕ-Selmer groups $\mathrm{Sel}_\phi(E_k)$ over $\mathbb{Q}$ to orbits of integer-matrix binary cubic forms could be constructed.

We say a binary cubic form $f(x, y)$ over $\mathbb{Q}$ is *locally soluble* if the curve $C_f : z^3 = f(x, y)$ has a solution over $\mathbb{Q}_p$ for every prime p. The curve C_f has Jacobian E_k, where $4k = \mathrm{Disc}(f)$, and there is a degree 3 map $C_f \to E_{-27k}$ which is a twist of $\phi_k : E_k \to E_{-27k}$. This correspondence between ϕ-coverings and binary cubic forms is the key to our method, and is the subject of Sections 3–6.

Theorem 17. *For any non-zero $k \in \mathbb{Z}$, the elements of $\mathrm{Sel}_\phi(E_k)$ correspond bijectively to the orbits of $\mathrm{SL}_2(\mathbb{Q})$ on locally soluble binary cubic forms over $\mathbb{Q}$ of discriminant $4k$. If $81 \mid k$, then every such orbit has an integral representative.*

With this direct map in hand, the problem of determining the average size of the ϕ-Selmer group is reduced to counting the appropriate set of integer-matrix binary cubic forms of bounded discriminant. For this, the counting method of Davenport [19] and a suitable adaptation of the sieve methods of [20] and [7] may be applied to obtain the optimal upper and lower bounds, and this is carried out in Section 6. This sieve renders the final answer as a product of local densities, and we prove that the density at the p-adic place for a given elliptic curve $E_k : y^2 = x^3 + k$ is given precisely by the local Selmer ratio $c_p(\phi)$ as defined by (5). For k varying over an acceptable set S, this yields Theorem 2 (see §6.3).

We evaluate the local Selmer ratios by relating them to Tamagawa numbers and using Tate's algorithm (Proposition 34). Setting $S = \mathbb{Z}$ then yields Theorem 1, while setting $S = T_m$, and applying a formula of Cassels [16] on the global Selmer ratio, yields Theorem 4 (see §§6.3–6.4). The results on average rank and on positive proportions of rank 0 and 3-Selmer rank 1 curves, as in Theorems 5–7 and Corollary 8, are then deduced in Section 7. Finally, we use the work of [13] to extend these results to any number field, as in Theorems 11–14, in Section 8.

We note that the connection between binary cubic forms and Selmer groups also has an interpretation in terms of Lie groups. In the language of Vinberg theory, the representation of SL_2 on binary cubic forms arises from a $\mathbb{Z}/3\mathbb{Z}$-grading of the Lie algebra of G_2. This paper is one example of recent work connecting representations arising from Vinberg's theory to Selmer groups of Jacobians of algebraic curves. In this context, we believe that our theorems above give the first results for the exact and finite average size of a Selmer group associated to an isogeny that is not the multiplication-by-n isogeny. For results and conjectures about the latter see, e.g., [5, 44, 45, 7, 27, 31, 33, 36, 42]. A beautiful treatment of the connection between algebraic curves and Vinberg theory, using versal deformations, has been given by Thorne [44].

The parametrization and methods introduced here have a number of other applications as well. For example, they can be used to obtain an improved upper bound on the average number of *integral* points on the curves E_k [2]. The finiteness of the number of integral points on such curves was first proven by Mordell [29], which is why these curves are sometimes called *Mordell curves*. Another application of our parameterization and methods is the existence of rational points on cubic surfaces: Tim Browning [14] has recently used our results, along with [35], to prove that a positive proportion of cubic surfaces of the form $f(x, y) = g(z, w)$ have a rational point.

One may ask about the ϕ-Selmer group in families of quadratic twists $E_{km^3} : y^2 = x^3 + km^3$, for fixed k and m varying, as well as in families of cubic twists $E_{km^2} : y^2 = x^3 + km^2$. These are very sparse subsets of all curves E_k, and so our results in Theorem 2 do not apply. Nevertheless, in a forthcoming paper [6], it is shown that the analogue of Theorem 2 continues to hold even in these families of quadratic twists; in fact, the formula (6) for the average size of the ϕ-Selmer group holds more generally in any family of quadratic twists of an abelian variety having a rational 3-isogeny. When the abelian variety is an elliptic curve, this leads to a proof of the boundedness of the average rank in such quadratic twist families, over any number field. The analogue of the formula in Theorem 2 is expected to hold also for the above cubic twist families, although in most such cases the product in (6) goes to infinity and the average ϕ-Selmer group sizes for curves in these families will correspondingly be infinite. The exception is when k is a square, in which case the Euler product (6) goes to 0, and we expect that the average size of the ϕ-Selmer group is equal to 1 in that case.

Finally, in recent work, Kriz and Li [35] prove that (over $\mathbb{Q}$) at least 10% of the curves $y^2 = x^3+k$ have rank 0 (resp. 1). Their p-adic methods are completely different from ours, and while their rank 0 and 1 proportions are lower, their rank 1 results over $\mathbb{Q}$ are unconditional.

2 Integer-matrix binary cubic forms over a Dedekind domain

Let $V^*(\mathbb{Z}) = \mathrm{Sym}^3\mathbb{Z}^2$ be the lattice of integer-coefficient binary cubic forms, i.e., forms $f(u, v) = au^3 + bv^2y + cuv^2 + dv^3$ with $a, b, c, d \in \mathbb{Z}$. To ease notation, we write $f(u, v) = [a, b, c, d]$. The group $\mathrm{GL}_2(\mathbb{Z})$ acts naturally on $V^*(\mathbb{Z})$ by linear change of variable, and the *discriminant*

$$\mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

is $\mathrm{SL}_2(\mathbb{Z})$-invariant.

In this paper, the more fundamental object will be the dual lattice $V(\mathbb{Z}) = \mathrm{Sym}_3\mathbb{Z}^2$ consisting of *integer-matrix* binary cubic forms, i.e., forms $f(u, v) = [a, 3b, 3c, d]$ with $a, b, c, d \in \mathbb{Z}$. The lattice $V(\mathbb{Z})$ has its own (*reduced*) *discriminant*

$$\mathrm{disc}(f) = -\frac{1}{27}\mathrm{Disc}(f).$$

We note that the action of $\mathrm{GL}_2(F)$ on the space $V(F) := V(\mathbb{Z}) \otimes F$ of binary cubic forms with coefficients in F satisfies

$$\mathrm{disc}(g \cdot f) = \det(g)^6\mathrm{disc}(f)$$

for all $g \in \mathrm{GL}_2(F)$ and $f \in V(F)$. For any ring R and $d \in R$, we write $V(R)_d$ for the set of $f \in V(R) := V(\mathbb{Z}) \otimes R$ with $\mathrm{disc}(f) = d$.

In this section, we classify the orbits of $V(D)$, under the action of $\mathrm{SL}_2(D)$, for an arbitrary Dedekind domain D of characteristic not 2 or 3. In later sections we will apply our classification to the case where D is a field, $\mathbb{Z}_p$, or $\mathbb{Z}$. Our result is a generalization of [3, Theorem 13], and is proved in the same way.

Theorem 18. *Let D be a Dedekind domain of characteristic not 2 or 3, and let $k \in D$ be any nonzero element. Let F be the fraction field of D, and let $S := D[z]/(z^2-k)$ and $K := F[z]/(z^2-k)$. Then there is a bijection between the orbits of $\mathrm{SL}_2(D)$ on $V(D)_{4k}$ and equivalence classes of triples (I, δ, s), where I is a fractional S-ideal, $\delta \in K^*$, and $s \in F^*$, satisfying the relations $I^3 \subset \delta S$, $N(I)$ is the principal fractional ideal sD in F, and $N(\delta) = s^3$ in F^*. Two triples (I, δ, s) and (I', δ', s') are equivalent if there exists $\kappa \in K^*$ such that $I' = \kappa I$, $\delta' = \kappa^3\delta$, and $s' = N(\kappa)s$. Under this correspondence, the stabilizer in $\mathrm{SL}_2(D)$ of $f \in V(D)_{4k}$ is isomorphic to $S(I)^*[3]_{N=1}$, where $S(I)$ is the ring of endomorphisms of I.*

Remark 19. We call triples (I, δ, s) satisfying the relations above *valid triples.*

Proof. We describe here the explicit bijection, but refer readers to [3] for the details of the proof. First, note that $S = D + D\tau$, with τ the image of x in S. Given a valid triple (I, δ, s), since $N(I)$ is the principal D-ideal sD, the projective D-module I of rank 2 is free, and so we may write $I = D\alpha + D\beta$ for some $\alpha, \beta \in I$. Because $I^3 \subset \delta S$, we have

$$\begin{array}{rcl} \alpha^3 & = & \delta(e_0 + \tau a) \\ \alpha^2\beta & = & \delta(e_1 + \tau b) \\ \alpha\beta^2 & = & \delta(e_2 + \tau c) \\ \beta^3 & = & \delta(e_3 + \tau d), \end{array} \tag{8}$$

for some a, b, c, $d, e_i \in D$. Then corresponding to (I, δ, s) is the binary cubic form $f = [a, 3b, 3c, d]$, which has discriminant $\operatorname{disc}(f) = 4k$. In more coordinate-free terms, f is the symmetric trilinear form

$$\frac{1}{\delta}\times : I \times I \times I \to S/D \cong D\tau. \tag{9}$$

We obtain an $\mathrm{SL}_2(D)$-orbit of symmetric trilinear forms (integer-matrix binary cubic forms) over D by taking the symmetric $2 \times 2 \times 2$ matrix representation of this form with respect to any ordered basis $\langle \alpha, \beta \rangle$ of I that gives rise to the basis element $s(1 \wedge \tau)$ of the top exterior power of I over D. This normalization deals with the difference between $\mathrm{SL}_2(D)$- and $\mathrm{GL}_2(D)$-orbits. The stabilizer statement follows because elements in $S(I)^*[3]_{N=1}$ are precisely the elements of $K^*_{N=1}$ that preserve the map (9). $\square$

When D is a field, so that $D = F$, the previous result simplifies quite a bit. Let us write $(K^*/K^{*3})_{N=1}$ to denote the kernel of the norm map $K^*/K^{*3} \to F^*/F^{*3}$, and $(\mathrm{Res}^K_F \mu_3)_{N=1}$ for the kernel of the norm map $\mathrm{Res}^K_F\, \mu_3 \to \mu_3$.

Corollary 20. *There is a natural bijection between the set of* $\mathrm{SL}_2(F)$*-orbits on* $V(F)_{4k}$ *and the group* $\left(K^*/K^{*3}\right)_{N=1}$*. Moreover, the stabilizer of any* $f \in V(F)_{4k}$ *in* $\mathrm{SL}_2(F)$ *is isomorphic to* $(\mathrm{Res}^K_F\, \mu_3)_{N=1}$*.*

Proof. Both statements follow from taking $D = F$ in the previous theorem. The bijection sends $\delta \in (K^*/K^{*3})_{N=1}$ to the orbit of binary cubic forms corresponding to the triple (K, δ, s), where s is any choice of cube root of $N(\delta)$. $\square$

Remark 21. Explicitly, if $\delta = a + b\tau \in K^*$, then the corresponding cubic form is $f = [ak, 3bk, 3a, b]$. In particular, $\delta = 1$ corresponds to the form $kx^3 + 3xy^2$, the Kostant section in Vinberg's theory.

Another case of interest is when $D = \mathbb{Z}_p$ and S is the maximal order in K:

Proposition 22. *Let p be a prime and assume $S = \mathbb{Z}_p[z]/(z^2 - k)$ is the maximal order in $K = \mathbb{Q}_p[z]/(z^2 - k)$. Then the set of* $\mathrm{SL}_2(\mathbb{Z}_p)$*-orbits on* $V(\mathbb{Z}_p)_{4k}$ *is in bijection with the unit subgroup* $(S^*/S^{*3})_{N=1} \subset (K^*/K^{*3})_{N=1}$*. Every rational* $\mathrm{SL}_2(\mathbb{Q}_p)$*-orbit of discriminant $4k$ whose class lies in this unit subgroup contains a unique integral* $\mathrm{SL}_2(\mathbb{Z}_p)$*-orbit. The stabilizer in* $\mathrm{SL}_2(\mathbb{Q}_p)$ *of an element in* $V(\mathbb{Z}_p)_{4k}$ *is equal to its stabilizer in* $\mathrm{SL}_2(\mathbb{Z}_p)$*.*

Proof. Indeed, every S-ideal I is principal in this case. From the $\mathbb{Z}_p$-version of Theorem 18, it follows that any integral orbit corresponds to a triple (S, δ, s) with $\delta \in S^*$. The stabilizer statement follows because $K^*[3]_{N=1} = S^*[3]_{N=1}$ when S is the maximal order in K. $\square$

Finally, we will need the following result on stabilizers of integer-matrix binary cubic forms over $\mathbb{Z}$. Let $G = \mathrm{SL}_2$ and for any ring R and $f \in V(R)$, write $\mathrm{Aut}_R(f)$ for $\mathrm{Stab}_{G(R)}(f)$.

Proposition 23. *Suppose $f \in V(\mathbb{Z})_{4k}$ is an integer-matrix binary cubic form of discriminant $4k$. Then*

$$|\mathrm{Aut}_{\mathbb{Q}}(f)| \sum_{f' \in O(f)} |\mathrm{Aut}_{\mathbb{Z}}(f')|^{-1} = \prod_p |\mathrm{Aut}_{\mathbb{Q}_p}(f)| \sum_{f'_p \in O_p(f)} |\mathrm{Aut}_{\mathbb{Z}_p}(f'_p)|^{-1},$$

where $O(f)$ is a set of representatives for the $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})_{4k}$ contained in the $G(\mathbb{Q})$-orbit of f, and similarly $O_p(f)$ is a set of representatives for the $G(\mathbb{Z}_p)$-orbits on $V(\mathbb{Z}_p)_{4k}$ contained in the $G(\mathbb{Q}_p)$-orbit of f.

Proof. We follow the proof of [5, Proposition 8.9]. Let $K = \mathbb{Q}[z]/(z^2 - k)$, and fix a representative $\delta \in K^*$ of the class in $(K^*/K^{*3})_{N=1}$ corresponding to f. Let $m(\delta)$ be the number of ideals I of $S = \mathbb{Z}[z]/(z^2 - k)$ satisfying $I^3 \subset \delta S$ and the ideal equality $N(I)^3 = N(\delta)$. Similarly, let $m_p(\delta)$ be the number of ideals I_p of $S_p := S \otimes \mathbb{Z}_p$ with $I_p^3 \subset \delta S_p$ and $N(I_p)^3 = N(\delta)$. Note that for all but finitely many p, S_p is the maximal order and δ is a unit, so $m_p(\delta) = 1$ for all but finitely many p.

Since a lattice is determined by its local completions, and since a collection of local ideals produces a global ideal with the desired properties, we have

$$m(\delta) = \prod_p m_p(\delta). \tag{10}$$

Let s be any cube root of $N(\delta)$. Then the triple (I, δ, s) is valid and hence corresponds to an integer-matrix binary cubic form $f_I \in V(\mathbb{Z})_{4k}$ mapping to the rational orbit of δ. If s' is another choice of cube root, then $s' = s\zeta_3$ and (I, δ, s) is equivalent to (I, δ, s'). A triple (I, α, s) is in the same integral orbit as (cI, α, s), for some $c \in K^\times$, exactly when $c^3 = 1$ and $N(c) = 1$. On the other hand, the ideals I and cI are equal if c is a unit in the ring of endomorphisms $S(I)$ of I. Thus, the number of distinct ideals giving the same integral orbit is the size of the group $K^*[3]_{N=1}/S(I)^*[3]_{N=1}$.

We have $K^*[3]_{N=1} \cong \mathrm{Aut}_{\mathbb{Q}}(f)$ and $S(I)^*[3]_{N=1} \cong \mathrm{Aut}_{\mathbb{Z}}(f_I)$ by Theorem 18. Thus, the number of distinct ideals associated to the integral orbit of f_I is $|\mathrm{Aut}_{\mathbb{Q}}(f)|/|\mathrm{Aut}_{\mathbb{Z}}(f_I)|$. We conclude that

$$m(\delta) = \sum_{f_I \in O(f)} |\mathrm{Aut}_{\mathbb{Q}}(f)|/|\mathrm{Aut}_{\mathbb{Z}}(f_I)|.$$

The same reasoning implies an analogous formula for $m_p(\delta)$, with global stabilizers replaced by local stabilizers. The proposition now follows from (10). □

3 The elliptic curves E_k and orbits of binary cubic forms over a field

Let F be a field of characteristic not 2 or 3, and let $k \in F$ be nonzero. Recall that the elliptic curve

$$E_k \colon y^2 = x^3 + k \tag{11}$$

admits a 3-isogeny $\phi \colon E_k \to E_{-27k}$ defined over F, and a dual 3-isogeny $\hat{\phi} \colon E_{-27k} \to E_k$.

In this section, we describe the connection between the isogenies ϕ and $\hat{\phi}$ and binary cubic forms (i.e., symmetric trilinear forms) over F.

3.1 Galois cohomology of the 3-isogeny kernel and field arithmetic

Important in the study of ϕ- and $\hat{\phi}$-descents on the curves E_k and E_{-27k} is the pair of "mirror" quadratic étale F-algebras

$$K = F[z]/(z^2 - k) \quad \text{and} \quad \hat{K} = F[z]/(z^2 + 27k).$$

The following result connects the arithmetic of the elliptic curves E_{-27k} and E_k to the arithmetic of K and $\hat{K}$:

Proposition 24. *There is an isomorphism of group schemes*

$$E_{-27k}[\hat{\phi}] \cong \ker\left(\mathrm{Res}_F^K \mu_3 \to \mu_3\right),$$

and an induced isomorphism

$$H^1(G_F, E_{-27k}[\hat{\phi}]) \cong \left(K^*/K^{*3}\right)_{N=1},$$

where $\left(K^*/K^{*3}\right)_{N=1}$ *denotes the kernel of the norm* $N\colon K^*/K^{*3} \to F^*/F^{*3}$.

Proof. Duality gives a non-degenerate pairing

$$\langle\ ,\ \rangle\colon E_{-27k}[\hat{\phi}] \times E_k[\phi] \to \mu_3.$$

Since $E_k[\phi](\overline{F})$ becomes a trivial Galois module when restricted to G_K, this induces an injective homomorphism of group schemes $\iota\colon E_{-27k}[\hat{\phi}] \to \mathrm{Res}_F^K \mu_3$, given on points by

$$P \mapsto (\langle P, Q_1\rangle, \langle P, Q_2\rangle),$$

where Q_1 and Q_2 are the non-trivial points of $E_k[\phi]$. The image of ι is precisely the kernel of the norm map $\mathrm{Res}_F^K \mu_3 \to \mu_3$, giving the desired isomorphism.

From Kummer theory and the long exact sequence attached to

$$0 \to E_{-27k}[\hat{\phi}] \to \mathrm{Res}_F^K \mu_3 \to \mu_3 \to 0,$$

we obtain the isomorphism $H^1(G_F, E_{-27k}[\hat{\phi}]) \cong \left(K^*/K^{*3}\right)_{N=1}$. □

Remark 25. The sequence $0 \to E_{-27k}[\hat{\phi}] \to E_{-27k} \to E_k \to 0$ induces a Kummer map

$$\partial\colon E_k(F) \to H^1(G_F, E_{-27k}[\hat{\phi}]) \cong \left(K^*/K^{*3}\right)_{N=1},$$

which can be described explicitly as follows. If $(x, y) \notin E_k[\phi](F)$, then $\partial((x, y)) = y - \tau$, where τ is the image of x in $K = F[z]/(z^2 - k)$. If $P = (0, \pm\sqrt{k}) \in E_k[\phi]$, then $\partial(P) = \pm 1/2\tau$. See [16, §15].

Remark 26. Of course, the analogues of all these results hold also when $\hat{\phi}$ is replaced with ϕ and K is replaced with $\hat{K}$; these analogues are obtained simply via the change of variable $k \mapsto -27k$.

3.2 Connection to binary cubic forms

We may now compare Corollary 20 and Proposition 24. This immediately yields the following canonical bijection:

Theorem 27. *There is a bijection between* $H^1(G_F, E_{-27k}[\hat{\phi}])$ *and the* $\mathrm{SL}_2(F)$*-orbits on* $V(F)_{4k}$*. Moroever, the stabilizer in* $\mathrm{SL}_2(F)$ *of any* $f \in V(F)_{4k}$ *is isomorphic to* $E_{-27k}[\hat{\phi}](F)$*.*

Let $V(F)^{\mathrm{sol}}$ denote the set of binary cubic forms $f(x, y) \in V(F)$ that correspond under the bijection of Theorem 27 to classes in the image of the Kummer map $\partial\colon E_k(F) \to H^1(G_F, E_{-27k}[\hat{\phi}])$ for some $k \in F$. If $f \in V(F)^{\mathrm{sol}}$, then we also say that f is *soluble*. We write $V(F)^{\mathrm{sol}}_D$ for the elements of $V(F)^{\mathrm{sol}}$ having discriminant D.

Corollary 28. *There is a natural bijection between the* $\mathrm{SL}_2(F)$*-orbits on* $V(F)^{\mathrm{sol}}_{4k}$ *and the elements of the group* $E_k(F)/\hat{\phi}(E_{-27k}(F))$*. Under this bijection, the identity element of* $E_k(F)/\hat{\phi}(E_{-27k}(F))$ *corresponds to the unique* $\mathrm{SL}_2(F)$*-orbit of reducible binary cubic forms in* $V(F)^{\mathrm{sol}}_{4k}$*, namely the orbit of* $f = [k, 0, 3, 0]$*.*

Proof. The second part follows from Remark 21, by taking $\delta = 1$. Indeed, if the cubic form corresponding to δ is reducible, then $\mathrm{Tr}(x^3\sqrt{k}\delta^{-1}) = 0$, for some $x \in K$; hence $x^3 = \delta t$ for some $t \in F^{\times}$. As $N(\delta)$ is a cube, we see that t is a cube in $F^{\times}$, and hence δ is a cube in $K^{\times}$. So we may as well take $\delta = 1$. □

The use of the term "soluble" comes from the following fact:

Proposition 29. *A binary cubic form* $f(x, y) \in V(F)_{4k}$ *corresponds to an element* δ *in the image of* $\partial\colon E_k(F) \to H^1(G_F, E_{-27k}[\hat{\phi}]) \cong \big(K/K^{*3}\big)_{N=1}$ *if and only if the curve* $C_f\colon z^3 = f(x, y)$ *in* $\mathbb{P}^2$ *has an* F*-rational point.*

Proof. Suppose $f \in V(F)_{4k}$, and let $\delta \in K^*$ be a representative element in $\big(K/K^{*3}\big)_{N=1}$ corresponding to the $\mathrm{SL}_2(F)$-orbit of f under the bijection of Corollary 20.

If δ represents the image of a point $(x, y) \in E_k(F)$ under ∂, then, by Remarks 21 and 25, the form f is $\mathrm{SL}_2(F)$-equivalent to $[1, 3y, 3k, yk]$, which represents a cube (namely, 1).

Conversely, if there exist $u, v, z \in F$ such that $z^3 = f(u, v)$, then by scaling u and v if necessary we may assume that $z = 1$. Therefore, we have by (8) or (9) that

$$(u + v\tau)^3 = \delta(g(u, v) + f(u, v)\tau) = \delta(g(u, v) + \tau) \tag{12}$$

where g is a binary cubic form over F, and so $g(u, v) \in F$. Writing $N(\delta) = s^3$, and then taking norms of both sides of (12), we obtain $N(u + v\tau)^3 = s^3(g(u, v)^2 - k)$. Thus the point $(x, y) = (N(u + v\tau)/s, g(u, v))$ lies on E_k, and this point (x, y) then maps to the class of δ in $\big(K/K^{*3}\big)_{N=1}$ under ∂. □

Remark 30. Recall that a $\hat{\phi}$-covering is a map of curves $C \to E_k$ over F which is a twist of $\hat{\phi}$. By descent, the group $H^1(G_F, E_{-27k}[\hat{\phi}])$ is in bijection with isomorphism classes of $\hat{\phi}$-coverings. To construct the $\hat{\phi}$-covering corresponding to $\delta \in \big(K/K^{*3}\big)_{N=1}$, take any $s \in F^*$ such that $N(\delta) = s^3$, and let f be the corresponding binary cubic form over F under the bijection of Corollary 20. Then we take C_f to be the curve $z^3 = f(x, y)$ in $\mathbb{P}^2$ (whose Jacobian is easily computed to be E_k), and the $\hat{\phi}$-covering map $C_f \to E_k$ corresponding to the class δ is given explicitly by

$$(u\colon v\colon z) \mapsto ((u^2 - kv^2)/s, g(u, v)),$$

where $g(u, v)$ is the cubic polynomial in the preceding proof.

Remark 31. One can also construct the $\hat{\phi}$-covering using the invariant theory of binary cubics. If $f = [a, 3b, 3c, d] \in V(F)$, then the covariants of f are generated by the discriminant disc, the scaled Hessian

$$h(x,y) = \frac{1}{36}(f_{xx}f_{yy} - f_{xy}^2) = (ac - b^2)x^2 + (ad - bc)xy + (bd - c^2), \tag{13}$$

and the Jacobian derivative of f and h,

$$g(x,y) = \frac{\partial(f,h)}{\partial(x,y)} = f_x h_y - f_y h_x, \tag{14}$$

which is a cubic polynomial in x, y whose coefficients are cubic polynomials in a, b, c, d. The cubic f and its covariants g, h are related by the syzygy[1]

$$(g/3)^2 - \mathrm{disc}(f) f^2 + 4h^3 = 0. \tag{15}$$

This gives us a degree-3 map from the genus-1 curve

$$C_f \colon z^3 = f(x,y)$$

to E_k with $k = \mathrm{disc}/4$: divide both sides of (15) by $4z^6$ and solve for $(g/2z^3)^2$ to obtain

$$\left(\frac{1}{6}\frac{g}{z^3}\right)^2 = \left(-\frac{h}{z^2}\right)^3 + \frac{\mathrm{disc}(f)}{4}. \tag{16}$$

Our curve E_{-27k} is the special case of C_f where $f(x,y) = kx^3 + 3xy^2$; we then see that $\mathrm{disc}(f) = 4k$, and the map $(z, y/x) \mapsto (-h/z^2, g/6z^3)$ to E_k recovers our formula (3) for the 3-isogeny $\hat{\phi}$.

4 Soluble orbits over local and global fields

When F is a local field, we can give explicit formulas for the number of soluble $\mathrm{SL}_2(F)$-orbits of binary cubic forms of discriminant $4k$, i.e., the size of the group $E_k(F)/\hat{\phi}(E_{-27k}(F))$. Since $|E_{-27k}[\hat{\phi}](F)|$ is 3 or 1 depending on whether $-3k$ is a square in F, it is equivalent to give formulas for the (local) Selmer ratios

$$c(\hat{\phi}_k) = \frac{|\mathrm{coker}(E_{-27k}(F) \to E_k(F))|}{|\ker(E_{-27k}(F) \to E_k(F))|}.$$

We do this below for the local fields $\mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{C}$, though there are similar formulas for any finite extension of $\mathbb{Q}_p$ and for equicharacteristic local fields such as $\mathbb{F}_p((t))$. If $F = \mathbb{Q}_p$, $\mathbb{R}$, or $\mathbb{C}$, we use the notation $c_p(\hat{\phi}_k)$, with $p \leq \infty$, to match with the introduction. We state the result for $c_p(\phi_k)$, the Selmer ratio of the original isogeny $\phi_k \colon E_k \to E_{-27k}$.

[1] These results are classical, at least for $F = \mathbb{C}$, and they go back at least to Hilbert [28, pp.68–69]; see also Schur's treatment [40, II, §8, Satz 2.24 on p. 77]. The syzygy (15) can be verified by direct computation, though it is easier to check it for one choice of f without repeated factors and then use the fact that $\mathrm{SL}_2(\overline{F})$ acts transitively on such f. For example, $f = x^3 - y^3$ gives disc $= 1$, $h = -xy$ and $g = -3(x^3 + y^3)$, reducing the syzygy (15) to the identity $(x^3 + y^3)^2 - (x^3 - y^3)^2 = 4(xy)^3$.

4.1 Orbits over $\mathbb{Q}_p$

Suppose $F = \mathbb{Q}_p$. We first determine when $E_k/\mathbb{Q}_p$ has good reduction.

Lemma 32. *Assume $k \in \mathbb{Z}_p$ is sixth-power-free. If $p > 3$, then $E_k/\mathbb{Q}_p$ has good reduction if and only if $p \nmid k$. If $p = 3$, then $E_k/\mathbb{Q}_3$ has bad reduction. If $p = 2$, then $E_k/\mathbb{Q}_2$ has good reduction if and only if $k \equiv 16 \pmod{64}$.*

Proof. This follows from Tate's algorithm. If $k \equiv 16 \pmod{64}$, a model with good reduction at 2 is $y'^2 + y' = x'^3 + a_6$ where $k = 64a_6 + 16$ and $(x, y) = (4x', 8y' + 4)$. □

Next, we express $c_p(\phi_k)$ in terms of the Tamagawa numbers of E_k and E_{-27k} (cf. [39, Lemma 3.8]).

Proposition 33. *If $k \in \mathbb{Z}_p$ is sixth-power-free, then*

$$c_p(\phi_k) = \frac{c_p(E_{-27k})}{c_p(E_k)} \times \begin{cases} 3 & \text{if } p = 3 \text{ and } 27 \mid k; \text{ and} \\ 1 & \text{otherwise,} \end{cases}$$

where $c_p(E) = |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$ denotes the Tamagawa number of E.

Proof. Let ω_k and ω_{-27k} denote Néron differentials on E_k and E_{-27k}, respectively. Then for some $b, b' \in \mathbb{Q}$, we have $\omega = b \cdot \frac{dx}{y}$ and $\omega_{-27k} = b' \cdot \frac{dX}{Y}$ on $E_k \colon y^2 = x^3 + k$ and $E_{-27k} \colon Y^2 = X^3 - 27k$, respectively. The model $y^2 = x^3 + k$ is minimal except if $k \equiv 16 \pmod{64}$, in which case the model given in the proof of Lemma 32 is minimal. In either case, we compute that $b = b'$ when $27 \nmid k$ and $b' = 3b$ when $27 \mid k$. Since

$$\phi^* \left(b \cdot \frac{dX}{Y} \right) = \frac{b \cdot d\left(\dfrac{x^3 + 4k}{x^2} \right)}{\dfrac{y(x^3 - 8k)}{x^3}} = \frac{b \cdot \left(1 - \dfrac{8k}{x^3} \right) dx}{\dfrac{y(x^3 - 8k)}{x^3}} = b \cdot \frac{dx}{y},$$

we have $\phi^* \omega_{-27k} = a\omega_k$, where $a = 1$ if $27 \nmid k$ and $a = 3$ if $27 \mid k$.

We then compute

$$\int_{\hat{\phi}(E_k(\mathbb{Q}_p))} |\omega_{-27k}|_p \;=\; \frac{1}{|E_k[\phi](\mathbb{Q}_p)|} \cdot \int_{E_k(\mathbb{Q}_p)} |\phi^* \omega_{-27k}|_p \;=\; \frac{1}{|E_k[\phi](\mathbb{Q}_p)|} \cdot |a|_p \cdot \int_{E_k(\mathbb{Q}_p)} |\omega_k|_p.$$

Therefore,

$$c_p(\phi_k) = \frac{|(E_{-27k}(\mathbb{Q}_p)/\phi(E_k(\mathbb{Q}_p)))|}{|E_k[\phi](\mathbb{Q}_p)|} \;=\; \frac{\int_{E_{-27k}(\mathbb{Q}_p)} |\omega_{-27k}|_p}{|a|_p \int_{E_k(\mathbb{Q}_p)} |\omega_k|_p} \;=\; \frac{1}{|a|_p} \cdot \frac{c_p(E_{-27k})}{c_p(E_k)}$$

as desired. □

We use Tate's algorithm [43] to compute the ratios of Tamagawa numbers in Proposition 33, and hence the local Selmer ratios $c_p(\phi_k)$. In particular, we find that the $c_p(\phi_k)$ are determined by congruence conditions on k:

Proposition 34. *Let $k \in \mathbb{Z}$ be sixth-power-free, and let χ_K denote the quadratic character attached to $K = \mathbb{Q}(\sqrt{k})$. If $p \neq 3$, then*

$$c_p(\phi_k) = \begin{cases} 3^{-\chi_K(p)} & \text{if } p \equiv 2 \pmod 3 \text{ and } v_p(4k) \in \{2,4\}; \\ 1 & \text{otherwise.} \end{cases}$$

If $p = 3$, write $k = 3^{v_3(k)} k_3$. Then

$$c_p(\phi_k) \;=\; \begin{cases} 9 & \text{if } v_3(k) = 5, \text{ and } k_3 \equiv 2 \pmod 3; \\[1ex] 3 & \text{if } v_3(k) = 0, \text{ and } k_3 \equiv 5 \text{ or } 7 \pmod 9; \text{ or} \\ & \quad v_3(k) \in \{1,4\}, \text{ and } k_3 \equiv 2 \pmod 3; \text{ or} \\ & \quad v_3(k) = 3, \text{ and } k_3 \not\equiv 2 \text{ or } 4 \pmod 9; \text{ or} \\ & \quad v_3(k) = 5, \text{ and } k_3 \equiv 1 \pmod 3; \\[1ex] \frac{1}{3} & \text{if } v_3(k) = 2, \text{ and } k_3 \equiv 1 \pmod 3; \\[1ex] 1 & \text{otherwise.} \end{cases} \tag{17}$$

From Proposition 34, we may easily deduce explicit formulas for the number of soluble $\mathrm{SL}_2(\mathbb{Q}_p)$-orbits on $V(\mathbb{Q}_p)_{4k}$ (see also Corollary 37 below). One may go further and describe the soluble classes as a subgroup of $(K^*/K^{*3})_{N=1}$. We describe this below in the cases where $p \neq 3$.

Proposition 35. *If $k \in \mathbb{Z}_p$ and E_k has good reduction, then the Kummer map induces an isomorphism*

$$E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p)) \cong (S_0^*/S_0^{*3})_{N=1},$$

where S_0 is the ring of integers of $K = \mathbb{Q}_p[x]/(x^2 - k)$.

Proof. See [18, Lemma 4.1] or [26, Lemma 6]. □

Proposition 36. *Assume $p \neq 3$ and that $E_k/\mathbb{Q}_p$ has bad reduction. Then the natural map*

$$j\colon E_k[\phi](\mathbb{Q}_p) \to E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p))$$

is an isomorphism.

Proof. We first claim that $E_k[3](\mathbb{Q}_p) = E_k[\phi](\mathbb{Q}_p)$. Indeed, the six other 3-torsion points on $E_k(\bar{\mathbb{Q}}_p)$ are $(\sqrt[3]{-4k}, \sqrt{-3k})$, for the six possible choices of roots in this expression. It follows from the bad reduction of E_k and Lemma 32 that these points are defined over ramified extensions of $\mathbb{Q}_p$, so they do not lie in $E_k(\mathbb{Q}_p)$, proving the claim.

Next we show that j is injective. Indeed, if $P \in E_k[\phi](\mathbb{Q}_p)$ and $Q \in E_{-27k}(\mathbb{Q}_p)$ satisfy $\hat{\phi}(Q) = P$, then $Q \in E_{-27k}[3](\mathbb{Q}_p) = E_{-27k}[\hat{\phi}](\mathbb{Q}_p)$, where the equality follows from the above claim applied to E_{-27k}. Thus, $P = 0$ and j is injective.

Finally, it suffices to show that $|E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p))| \leq |E_k[\phi](\mathbb{Q}_p)|$. Note that the group $E_k(\mathbb{Q}_p)/3E_k(\mathbb{Q}_p)$ surjects onto $E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p))$. Since $p \neq 3$, an argument using the formal group [5, Lemma 12.3] shows that $E_k(\mathbb{Q}_p)/3E_k(\mathbb{Q}_p)$ has size $|E_k[3](\mathbb{Q}_p)|$, which is equal to $|E_k[\phi](\mathbb{Q}_p)|$, again by our claim above. Therefore, we indeed have

$$|E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p))| \leq |E_k[3](\mathbb{Q}_p)| = |E_k[\phi](\mathbb{Q}_p)|,$$

as desired. □

Corollary 37. *If $p \neq 3$, then the number of soluble orbits in $V(\mathbb{Q}_p)$ of discriminant $4k$ is equal to*

$$\begin{cases} |E_{-27k}[\hat{\phi}](\mathbb{Q}_p)| & \text{if } E_k/\mathbb{Q}_p \text{ has good reduction,} \\ |E_k[\phi](\mathbb{Q}_p)| & \text{if } E_k/\mathbb{Q}_p \text{ has bad reduction.} \end{cases}$$

Remark 38. At the start of the proof of Proposition 36, we noted that $E_k[3]$ consists of the three points of $E_k[\phi]$ together with the six points (x, y) with $x^3 = -4k$ and $y^2 = -3k$. If such a point is rational then $(k, x, y) = (-432m^6, 12m^2, 36m^3)$ for some nonzero m. In this case our elliptic curve $E_k \cong E_{-432}$ is isomorphic with the Fermat cubic $X^3 + Y^3 = Z^3$ (which is also isomorphic with the modular curve $\mathrm{X}_0(27)$), and the isogenous curve $E_{27k} \cong E_{16}$ is isomorphic with $XY(X + Y) = Z^3$. These curves have good reduction at primes other than 3; in particular, they satisfy the condition of Lemma 32 for good reduction at 2, with minimal models $y'^2 + y' = x'^3 - 7$ and $y'^2 + y' = x'^3$ respectively.

4.2 Orbits over $\mathbb{R}$ or $\mathbb{C}$

If $F = \mathbb{R}$ or $\mathbb{C}$, then every binary cubic form $f \in V(F)$ is reducible, so by Corollary 28, there is a unique $\mathrm{SL}_2(F)$-orbit of binary cubic forms of discriminant $4k$. This agrees with the fact that $E_k(F)/\hat{\phi}(E_{-27k}(F))$ is always trivial. We conclude:

Proposition 39. *If $F = \mathbb{C}$, then $c_\infty(\phi_k) = 1/3$ if $F = \mathbb{C}$. If $F = \mathbb{R}$, then*

$$c_\infty(\phi_k) = \begin{cases} \frac{1}{3} & \text{if } k > 0; \\ 1 & \text{if } k < 0. \end{cases}$$

4.3 ϕ-Selmer groups and locally soluble orbits over a global field

We let F now be a global field of characteristic not 2 or 3. If $\varphi\colon A \to A'$ is an isogeny of abelian varieties over F, then the *φ-Selmer group*

$$\mathrm{Sel}_\varphi(A) \subset H^1(G_F, A[\varphi])$$

is the subgroup consisting of classes that are locally in the image of the Kummer map

$$\partial_v\colon A'(F_v) \longrightarrow H^1(G_{F_v}, A[\varphi])$$

for every place v of F. Equivalently, these are the classes locally in the kernel of the map

$$H^1(G_{F_v}, A[\varphi]) \to H^1(G_{F_v}, A)[\varphi],$$

for every place v of F, i.e., the classes corresponding to ϕ-coverings having a rational point over F_v for every place v.

Now let $V(F)^{\text{loc. sol.}} \subset V(F)$ denote the set of *locally soluble* binary cubic forms, i.e. those $f(u, v) \in V(F)$ such that the equation $z^3 = f(u, v)$ has a nonzero solution over F_v for every place v of F. Then the following result follows immediately from Corollary 28.

Theorem 40. *Let $k \in F^*$. Then there is a bijection between the $\mathrm{SL}_2(F)$-orbits on $V(F)^{\text{loc. sol.}}$ having discriminant $4k$ and the elements of $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ corresponding to the isogeny $\hat{\phi}_k\colon E_{-27k} \to E_k$. Under this bijection, the identity element of $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ corresponds to the unique $\mathrm{SL}_2(F)$-orbit of reducible binary cubic forms of discriminant $4k$, namely the orbit of $f(x, y) = kx^3 + 3xy^2$. Moroever, the stabilizer in $\mathrm{SL}_2(F)$ of any $f \in V(F)^{\text{loc. sol.}}_{4k}$ is isomorphic to $E_{-27k}[\hat{\phi}](F)$.*

5 Existence of integral orbits

We now specialize to the case where $F = \mathbb{Q}$. The main goal of this section is to prove the following theorem.

Theorem 41. *Let $k \in 3\mathbb{Z}$. Then every locally soluble orbit for the action of* $\mathrm{SL}_2(\mathbb{Q})$ *on* $V(\mathbb{Q})_{4k}$ *has an integral representative, i.e., contains an element of* $V(\mathbb{Z})_{4k}$.

Proof. By Theorem 18 applied to the cases $D = \mathbb{Z}$ and $D = \mathbb{Z}_p$, it suffices to find a representative in $V(\mathbb{Z}_p)_{4k}$ for every soluble orbit of cubic forms $f \in V(\mathbb{Q}_p)_{4k}$, for each prime p. Indeed, such integral representatives would correspond to valid triples over $\mathbb{Z}_p$, which together determine a valid triple over $\mathbb{Z}$.

Let $S = \mathbb{Z}_p[z]/(z^2 - k)$ and $K = \mathbb{Q}_p[z]/(z^2 - k)$ as before, and assume for now that $p \neq 3$. The binary cubic form $f \in V(\mathbb{Q}_p)_{4k}^{\mathrm{sol}}$ corresponds to an element $\delta \in (K^*/K^{*3})_{N=1}$ in the image of the Kummer map. Let $P = (x, y) \in E_k(\mathbb{Q}_p)$ be a rational point mapping to δ. By Remark 25, we have $\delta = y - \tau$, where τ is the image of z in $K = \mathbb{Q}_p[z]/(z^2 - k)$. If x and y have negative valuation, then P lies in the subgroup $E_{k,1}(\mathbb{Q}_p) \subset E_k(\mathbb{Q}_p)$ isomorphic to the formal group of E_k. Since the formal group is pro-p and $p \neq 3$, it follows that there is a point $Q \in E_{k,1}(\mathbb{Q}_p)$ such that $3Q = P$; hence P is in $\hat{\phi}(E_{-27k}(\mathbb{Q}_p))$ and $\delta = \partial(P) = 1$. Thus, the valid triple $(S, 1, 1)$ corresponds to an integral representative in the orbit of f under the bijection of Theorem 18.

We may thus assume that x and y are in $\mathbb{Z}_p$. Define $I = \mathbb{Z}_p x + \mathbb{Z}_p \delta \subset K$. Then

$$\tau I \;=\; \mathbb{Z}_p x\tau + \mathbb{Z}_p \delta\tau \;=\; \mathbb{Z}_p(xy - x\delta) + \mathbb{Z}_p(x^3 - y\delta) \;\subset\; I,$$

and therefore I is an S-ideal. Furthermore, we have $N(I) = x\mathbb{Z}_p$, and $N(\delta) = N(y-\tau) = y^2 - k = x^3$. Finally, we note that the elements

$$\begin{array}{rcl} \delta^{-1}(x^3) & = & y + \tau \\ \delta^{-1}(x^2\delta) & = & x^2 \\ \delta^{-1}(x\delta^2) & = & xy - x\tau \\ \delta^{-1}(\delta^3) & = & y^2 + k - 2y\tau, \end{array}$$

are each contained in $S = \mathbb{Z}_p + \mathbb{Z}_p\tau$, implying that $I^3 \subset \delta S$. Thus (I, δ, x) is a valid triple for S in the sense of Theorem 18 and Remark 19, and yields the desired integral representative in $V(\mathbb{Z}_p)_{4k}$.

Remark 42. One can even *characterize* the integral classes in terms of solubility conditions, at least if $p \neq 3$. Specifically, if $k \in \mathbb{Z}_p$ is sixth-power-free, then an $\mathrm{SL}_2(\mathbb{Q}_p)$-orbit of forms $f \in V(\mathbb{Q}_p)_{4k}$ contains an integral form $f_0 \in V(\mathbb{Z}_p)_{4k}$ if and only if f is soluble over $\mathbb{Q}_p^{\mathrm{ur}}$, the maximal unramified extension of $\mathbb{Q}_p$.

Before considering the case $p = 3$, we state a general lemma. For any prime p, and for any $i \geq 0$, let S_i be the order of index p^i in the maximal order S_0 of $K = \mathbb{Q}_p[z]/(z^2 - k)$.

Lemma 43. *If (I, δ, s) is a valid triple for the ring S_i, with $i \geq 1$, then there exists an S_{i+1}-ideal J such that (J, δ, s) is a valid triple for the ring S_{i+1}. If $p = 3$, then this is true even if $i = 0$.*

Proof. This follows from the explicit bijection given in the proof of Theorem 18. If $f = [a, 3b, 3c, d]$ is a binary cubic form corresponding to the valid triple (I, δ, s), then f has a root over $\mathbb{F}_p$, since

$$\mathrm{Disc}(f) = -27\mathrm{disc}(f) = -27 \cdot \mathrm{Disc}(S_i)$$

is divisible by p. So via a change of variables we may assume that $p \mid d$. If $\alpha\mathbb{Z}_p + \beta\mathbb{Z}_p$ is the corresponding basis of I, then $[p^2a, 3pb, 3c, d/p]$ is an integer-matrix binary cubic form corresponding to the triple $(p\alpha\mathbb{Z}_p + \beta\mathbb{Z}_p, \delta, s)$ for the ring S_{i+1}. If $p = 3$, then $\mathrm{Disc}(f) = -27\mathrm{disc}(f)$ is divisible by p, even if $i = 0$. $\square$

Now let $p = 3$ and let $f \in V(\mathbb{Q}_3)_{4k}^{\mathrm{sol}}$ correspond to $\delta \in (K^*/K^{*3})_{N=1}$, with K and S as before. If the class of δ lies in the unit subgroup $(S_0^*/S_0^{*3})_{N=1}$, then (S_0, δ, s) is a valid triple for the ring S_0, and so by Lemma 43, there exists J such that (J, δ, s) is valid for the ring S. This triple corresponds to the desired $f \in V(\mathbb{Z}_3)_{4k}$ in the orbit corresponding to δ.

If δ is not represented by a unit, then we must be in the case $K = \mathbb{Q}_3 \times \mathbb{Q}_3$, as this is the only étale $\mathbb{Q}_3$-algebra where there exist δ's not represented by units. Since $k \in 3\mathbb{Z}$, we must have $S = S_i$ for some $i \geq 1$. We may choose δ to be of the form $(3\pi, 3u)$, for some uniformizer $\pi \in 3\mathbb{Z}_3$ and unit $u \in \mathbb{Z}_3^*$. Then the triple $(3S_0, \delta, s)$ is valid for the ring S_1, so by Lemma 43, there exist valid triples (J, δ, s) for S_i, for all $i \geq 1$, and in particular for S. This gives the desired $f \in V(\mathbb{Z}_3)_{4k}$ in the orbit corresponding to δ, and completes the proof of Theorem 41. $\square$

6 The average size of $\mathrm{Sel}_\phi(E_k)$

In this section, for acceptable subsets $S \subset \mathbb{Z}$, we asymptotically count the number of $\mathrm{SL}_2(\mathbb{Q})$-classes of locally soluble integer-matrix binary cubic forms $f \in V(\mathbb{Z})$ of discriminant $3^6 4k$ for $|k| < X$, $k \in S$, as $X \to \infty$. By the work of Section 5, this will then allow us to deduce Theorems 1, 2, and 4.

6.1 The asymptotic number of binary cubic forms of bounded discriminant with weighted congruence conditions

Let $V(\mathbb{R})$ denote the vector space of binary cubic forms over $\mathbb{R}$. Let $V^{(0)}(\mathbb{R})$ denote the subset of elements in $V(\mathbb{R})$ having positive discriminant, and $V^{(1)}(\mathbb{R})$ the subset of elements having negative discriminant. We use $V^{(i)}(\mathbb{Z})$ to denote $V(\mathbb{Z}) \cap V^{(i)}(\mathbb{R})$.

Now let T be any set of integral binary cubic forms that is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Let $N(T; X)$ denote the number of *irreducible* binary cubic forms contained in T, up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence, having absolute discriminant at most X. Then we have the following theorem counting $\mathrm{SL}_2(\mathbb{Z})$-classes of integer-matrix binary cubic forms of bounded reduced discriminant, which easily follows from the work of Davenport [19] and Davenport–Heilbronn [20] (see [15, Theorem 19] for this deduction):

Theorem 44. *Let T be any set of integer-matrix binary cubic forms that is defined by finitely many congruence conditions modulo prime powers and that is invariant under the action of* $\mathrm{SL}_2(\mathbb{Z})$*. For each prime p, let $\mu_p(T)$ denote the p-adic density of the p-adic closure of T in $V(\mathbb{Z}_p)$, where $V(\mathbb{Z}_p)$ is equipped with the usual additive p-adic measure normalized so that $\mu_p(V(\mathbb{Z}_p)) = 1$. Then*

(a) $N(T \cap V^{(0)}(\mathbb{Z}); X) = \dfrac{\pi^2}{12} \cdot \prod_p \mu_p(T) \cdot X + o(X)$;

(b) $N(T \cap V^{(1)}(\mathbb{Z}); X) = \dfrac{\pi^2}{4} \cdot \prod_p \mu_p(T) \cdot X + o(X)$.

For our particular application, we require a more general congruence version of our counting theorem for binary cubic forms, namely, one which not only allows appropriate infinite sets of congruence conditions to be imposed but which also permits weighted counts of lattice points (where weights are also assigned by congruence conditions). More precisely, we say that a function $\phi\colon V(\mathbb{Z}) \to [0,1] \subset \mathbb{R}$ is *defined by congruence conditions* if, for all primes p, there exist functions $\phi_p\colon V(\mathbb{Z}_p) \to [0,1]$ such that:

(1) For all $f \in V(\mathbb{Z})$, we have $\phi(f) = \prod_p \phi_p(f)$.

(2) For each prime p, the function ϕ_p is locally constant outside some set $Z_p \subset V(\mathbb{Z}_p)$ of measure zero.

Such a function ϕ is called *acceptable* if it is $\mathrm{SL}_2(\mathbb{Z})$-invariant and, for sufficiently large primes p, we have $\phi_p(f) = 1$ whenever $p^2 \nmid \mathrm{disc}(f)$. For such an acceptable function ϕ, we let $N_\phi(V^{(i)}(\mathbb{Z}); X)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of elements in $V^{(i)}(\mathbb{Z})$ having absolute discriminant at most X, where the equivalence class of $f \in V^{(i)}(\mathbb{Z})$ is weighted by $\phi(f)$.

We then have the following generalization of Theorem 44:

Theorem 45. *Let $\phi\colon V(\mathbb{Z}) \to [0,1]$ be an acceptable function that is defined by congruence conditions via the local functions $\phi_p\colon V(\mathbb{Z}_p) \to [0,1]$. Then*

$$N_\phi(V^{(i)}(\mathbb{Z}); X) = N(V^{(i)}(\mathbb{Z}); X) \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f)\, df + o(X). \tag{18}$$

Proof. The proof is exactly as in [7, Theorem 2.21], though we use the uniformity estimate

$$N(\mathcal{Z}_p; X) = O(X/p^2)$$

of [11, Proposition 29] in place of the uniformity estimate [7, Theorem 2.13]. Here, $\mathcal{Z}_p$ is the set of integral cubic forms of non-fundamental discriminant at p. $\square$

6.2 Weighted counts of binary cubic forms corresponding to Selmer elements

We wish to apply Theorem 45 to the set T of all integral binary cubic forms that lie in the correspondence of Theorems 40 and 41, with appropriately assigned weights. Namely, we need to count each $\mathrm{SL}_2(\mathbb{Z})$ orbit, $\mathrm{SL}_2(\mathbb{Z}) \cdot f$, weighted by $1/n(f)$, where $n(f)$ is number of $\mathrm{SL}_2(\mathbb{Z})$-orbits inside the $\mathrm{SL}_2(\mathbb{Q})$-equivalence class of f in $V(\mathbb{Z})$. For this purpose, it suffices to count the number of $\mathrm{SL}_2(\mathbb{Z})$-orbits of locally soluble integral binary cubic forms having bounded discriminant and no rational linear factor with each orbit $\mathrm{SL}_2(\mathbb{Z}) \cdot f$ weighted by $1/m(f)$, where

$$m(f) := \sum_{f' \in O(f)} \frac{|\mathrm{Aut}_{\mathbb{Q}}(f')|}{|\mathrm{Aut}_{\mathbb{Z}}(f')|} = \sum_{f' \in O(f)} \frac{|\mathrm{Aut}_{\mathbb{Q}}(f)|}{|\mathrm{Aut}_{\mathbb{Z}}(f')|};$$

here $O(f)$ is a set of representatives for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the $\mathrm{SL}_2(\mathbb{Q})$-equivalence class of f in $V(\mathbb{Z})$ and $\mathrm{Aut}_{\mathbb{Q}}(f)$ (resp. $\mathrm{Aut}_{\mathbb{Z}}(f)$) denotes the stabilizer of f in $\mathrm{SL}_2(\mathbb{Q})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$). The reason it suffices to weight by $1/m(f)$ instead of $1/n(f)$ is that, by the proof of [11, Lemma 22], all but a negligible number of $\mathrm{SL}_2(\mathbb{Z})$-orbits of integral irreducible binary cubic forms with bounded discriminant have trivial stabilizer in $\mathrm{SL}_2(\mathbb{Q})$; thus all but a negligible number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms of bounded discriminant satisfy $m(f) = n(f)$. In the remainder of this subsection, we compute this weighted p-adic density of locally soluble integral binary cubic forms.

For a prime p and a binary cubic form $f \in V(\mathbb{Z}_p)$, define $m_p(f)$ by

$$m_p(f) := \sum_{f' \in O_p(f)} \frac{|\mathrm{Aut}_{\mathbb{Q}_p}(f')|}{|\mathrm{Aut}_{\mathbb{Z}_p}(f')|} = \sum_{f' \in O_p(f)} \frac{|\mathrm{Aut}_{\mathbb{Q}_p}(f)|}{|\mathrm{Aut}_{\mathbb{Z}_p}(f')|},$$

where $O_p(f)$ is a set of representatives for the action of $\mathrm{SL}_2(\mathbb{Z}_p)$ on the $\mathrm{SL}_2(\mathbb{Q}_p)$-equivalence class of f in $V(\mathbb{Z}_p)$ and $\mathrm{Aut}_{\mathbb{Q}_p}(f)$ (resp. $\mathrm{Aut}_{\mathbb{Z}_p}(f)$) denotes the stabilizer of f in $\mathrm{SL}_2(\mathbb{Q}_p)$ (resp. $\mathrm{SL}_2(\mathbb{Z}_p)$). By Proposition 23, we have the factorization

$$m(f) = \prod_p m_p(f),$$

and so we have put ourselves in position to use Theorem 45.

Let S be an acceptable subset of $\mathbb{Z}$, and for each prime p, let S_p denote the closure of S in $\mathbb{Z}_p$. Let $B(S)$ denote the set of all locally soluble integral binary cubic forms having discriminant $3^6 4k$ for $k \in S$, and let $B_p(S)$ denote the p-adic closure of $B(S)$ in $V(\mathbb{Z}_p)$.

We now determine the p-adic density of $B_p(S)$, where each element $f \in B_p(S)$ is weighted by $1/m_p(f)$, in terms of the p-adic integral over S_p of the local Selmer ratio and the volume $\mathrm{Vol}(\mathrm{SL}_2(\mathbb{Z}_p))$ of the group $\mathrm{SL}_2(\mathbb{Z}_p)$, which is computed with respect to a fixed generator ω of the rank 1 module of top-degree differentials of SL_2 over $\mathbb{Z}$, so that ω is well-determined up to sign.

Proposition 46. *There is a rational number $\mathcal{J} \in \mathbb{Q}^\times$, independent of S and p, such that*

$$\int_{B_p(S)} \frac{1}{m_p(f)} df = |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathrm{SL}_2(\mathbb{Z}_p)) \cdot \int_{k \in S} \frac{|E_k(\mathbb{Q}_p)/\hat{\phi}(E_{-27k}(\mathbb{Q}_p))|}{|E_{-27k}(\mathbb{Q}_p)[\hat{\phi}]|} dk.$$

Proof. We make use of the facts that the number of $\mathrm{SL}_2(\mathbb{Q}_p)$-orbits of soluble binary cubic forms of discriminant $4k$ is equal to the cardinality of $E_{-27k}(\mathbb{Q}_p)/\hat{\phi}(E_k(\mathbb{Q}_p))$ (by Theorem 40), and the cardinality of $\mathrm{Aut}_{\mathbb{Q}_p}(f)$ is equal to the cardinality of $E_k(\mathbb{Q}_p)[\hat{\phi}]$ (by Corollary 27); otherwise, the proof is identical to [7, Proposition 3.9]. □

We note that the rational number $\mathcal{J}$ also shows up in the archimedean factor of Theorem 45, since

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\mathrm{Vol}(\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R}))|\mathcal{J}|_\infty}{n_i} X + o(X), \tag{19}$$

where $n_0 = 3$ and $n_1 = 1$; see [7, Proposition 3.11, Remark 3.14]. (In fact, it turns out that $\mathcal{J} = 3/2$, although we shall not need this fact.)

6.3 Proof of Theorems 1 and 2

Theorem 47. *Let $S \subset \mathbb{Z}$ be any acceptable subset of integers. Then when all elliptic curves $E_k\colon y^2 = x^3 + k$, $k \in S$, are ordered by the absolute value of k, the average size of the $\hat{\phi}$-Selmer* *group associated to the* 3*-isogeny* $\hat{\phi}\colon E_{-27k} \to E_k$ *is*

$$1 + \prod_{p \leq \infty} \frac{\displaystyle\int_{k \in S_p} c_p(\hat{\phi}_k) dk}{\displaystyle\int_{k \in S_p} dk}, \tag{20}$$

where S_p *denotes the* p*-adic closure of* S *in* $\mathbb{Z}_p$ *for* $p < \infty$*, and* S_∞ *is the image of* S *in* $\mathbb{R}^*/\mathbb{R}^{*2}$*.*

Proof. Let $X = 3^6 4Y$, and $G = \mathrm{SL}_2$ and define $E'_k = E_{-27k}$. By the discussion in §6.2, to count the total number of non-identity elements in the groups $\mathrm{Sel}_{\hat{\phi}_k}(E'_k)$ with $k < Y$, it suffices to count the number of locally soluble irreducible $\mathrm{SL}_2(\mathbb{Z})$-orbits of binary cubic forms $f \in V(\mathbb{Z})$ having discriminant in the set $3^6 4S$ and also bounded by X, and where each orbit is weighed by $1/m(f)$. This weighting function is acceptable by Proposition 22. Thus, by Theorem 45, Propositions 46 and 39, and (19), the number of such weighted orbits divided by the total number of $k \in S$ with $k < Y$ approaches

$$\mathrm{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))|\mathcal{J}|_\infty \frac{\displaystyle\sum_{\substack{k \in S \\ |k| < Y}} \frac{1}{|E'_k[\hat{\phi}](\mathbb{R})|}}{\displaystyle\sum_{\substack{k \in S \\ |k| < Y}} 1} \prod_p |\mathcal{J}|_p \mathrm{Vol}(G(\mathbb{Z}_p)) \frac{\displaystyle\prod_p \int_{k \in S_p} \frac{|E_k(\mathbb{Q}_p)/\hat{\phi}(E'_k(\mathbb{Q}_p))|}{|E'_k[\hat{\phi}](\mathbb{Q}_p)|} dk}{\displaystyle\prod_p \int_{k \in S_p} dk}$$

$$= \frac{\displaystyle\sum_{\substack{k \in S \\ |k| < Y}} \frac{1}{|E'_k[\hat{\phi}](\mathbb{R})|}}{\displaystyle\sum_{\substack{k \in S \\ |k| < Y}} 1} \prod_p \frac{\displaystyle\int_{k \in S_p} \frac{|E_k(\mathbb{Q}_p)/\hat{\phi}(E'_k(\mathbb{Q}_p))|}{|E'_k[\hat{\phi}](\mathbb{Q}_p)|} dk}{\displaystyle\int_{k \in S_p} dk}$$

$$= \prod_{p \leq \infty} \frac{\displaystyle\int_{k \in S_p} c_p(\hat{\phi}_k) dk}{\displaystyle\int_{k \in S_p} dk}$$

as $Y \to \infty$. The first equality is due to the product formula $\prod_{p \leq \infty} |\mathcal{J}|_p = 1$, and the fact that the Tamagawa number $\mathrm{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R})) \prod_p \mathrm{Vol}(G(\mathbb{Z}_p))$ of G equals 1. This proves formula (20) of Theorem 47, after taking into account the identity element of each $\hat{\phi}$-Selmer group. $\square$

Proof of Theorem 2. The formula comes from the change of variables $k \mapsto -27k$ in the result of Theorem 47, and the fact that $\hat{\phi}_k = \phi_{-27k}$. $\square$

Proof of Theorem 1. We use Proposition 34 to compute the p-adic integrals in Theorem 2 for the set $S = \mathbb{Z}$. The result is that the product of the local densities at finite primes equals

$$\begin{aligned} r \quad = \quad & \left[\frac{(1-2^{-1})(\frac{4}{3}+2^{-1}+\frac{4}{3}2^{-2}+2^{-3}+2^{-4}+2^{-5})}{1-2^{-6}}\right] \\ & \cdot \left[\frac{(1-3^{-1})(\frac{5}{3}+2\cdot 3^{-1}+\frac{2}{3}\cdot 3^{-2}+\frac{7}{3}\cdot 3^{-3}+2\cdot 3^{-4}+6\cdot 3^{-5})}{1-3^{-6}}\right] \\ & \cdot \prod_{p\equiv 5 \pmod 6} \left[\frac{(1-p^{-1})(1+p^{-1}+\frac{5}{3}p^{-2}+p^{-3}+\frac{5}{3}p^{-4}+p^{-5})}{1-p^{-6}}\right]. \end{aligned}$$

In each Euler factor, the six-term sum records the weighted average value of $c_p(\phi)$ on $p^i\mathbb{Z}_p - p^{i+1}\mathbb{Z}_p$ for $i = 0, \dots, 5$. Since $E_{km^6} \cong E_k$, these averages cyclically repeat themselves for $i \geq 6$, which explains the factor $1 - p^{-6}$ in the denominator. $\square$

6.4 Proof of Theorem 4

Claim (i) follows immediately from Proposition 34. Claim (ii) follows from Cassels' formula [18],

$$c(\phi) = \frac{|E_{-27k}(\mathbb{Q})[\hat{\phi}]| \cdot |\mathrm{Sel}_\phi(E_k)|}{|E_k(\mathbb{Q})[\phi]| \cdot |\mathrm{Sel}_{\hat{\phi}}(E_{-27k})|}. \tag{21}$$

To prove (iii), we use Proposition 34 to express T_m as a disjoint union

$$T_m = \bigcup_{n\in\mathbb{Z}} T_{m,n},$$

where $T_{m,n}$ is the set of all $k \in T_m$ for which there are exactly $m+n$ primes p (possibly including $p = \infty$) satisfying $c_p(\phi_k) \geq 3$, with the caveat that if $c_3(\phi_k) = 9$ then $p = 3$ is counted twice. Each $T_{m,n}$ can itself be expressed as a disjoint union

$$T_{m,n} = \bigcup_{(\Pi_1,\Pi_2)} T_{\Pi_1,\Pi_2},$$

where the union is over all pairs (Π_1, Π_2), where Π_1 is a multiset of $m+n$ primes, with each prime having multiplicity at most 1, except for $p = 3$ which may have multiplicity at most 2, and Π_2 is a set of n primes, disjoint from Π_1. The set T_{Π_1,Π_2} consists of those integers $k \in T_m$ such that $c_p(\phi_k) \geq 3$ if and only if $p \in \Pi_1$ (and having multiplicity 2 if and only if $p = 3$ and $c_3(\phi_k) = 9$), and such that $c_p(\phi_k) = 1/3$ if and only if $p \in \Pi_2$.

Note that each set $T_{\Pi_1,\Pi_2} \subset \mathbb{Z}$ is acceptable, by the explicit congruence conditions of Proposition 34. Moreover, for each prime p, the function $c_p(\phi_k)$ is constant on T_{Π_1,Π_2}. Thus by Theorem 2, for any acceptable set $S \subset T_{\Pi_1,\Pi_2}$, the average size of $\mathrm{Sel}_\phi(E_k)$ for $k \in S$ is

$$1 + \prod_p c_p(\phi_k) = 1 + c(\phi_k) = 1 + 3^m.$$

Since $c(\hat{\phi}) = c(\phi)^{-1}$, a similar argument shows that the average size of $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ for $k \in S$ is $1 + 3^{-m}$. Note that any acceptable set S contained in T_m is necessarily contained in some T_{Π_1,Π_2}, so this proves Theorem 4(iii) in the case that $S \subset T_m$ is an acceptable set.

If $S = T_m$, then since

$$T_m = \bigcup_n \bigcup_{(\Pi_1,\Pi_2)} T_{\Pi_1,\Pi_2},$$

we may write T_m as an ascending union $T_m = \bigcup_{i\geq 1} S_i$, where each S_i is the union of all T_{Π_1,Π_2} such that each prime $p \in \Pi_1 \cup \Pi_2$ is less than the i-th prime number p_i. Thus, each S_i is a finite union of acceptable sets, and so the average size of $\mathrm{Sel}_\phi(E_k)$ for $k \in S_i$ is $1 + 3^m$. Moreover, by Proposition 34, the binary cubic forms $f \in V(\mathbb{Z})$ having discriminant in the complement $T_m - S_i$ have discriminant divisible by p_j^2 for some $j \geq i$. By the uniformity estimate in [11, Proposition 29], we have $\sum_{k\in T_m\setminus S;|k|<X} \mathrm{Sel}_\phi(E_k)$ is $\sum_{j\geq i} O(X/p_j^2) = O(X/p_i)$, where the implied constant is independent of i. That is, the total number of Selmer elements of E_k over all $k \in T_m \setminus S_i$, $|k| < X$, is $O(X/p_i)$, while the total number of Selmer elements of E_k over all $|k| < X$ is of course $\gg X$. Letting i tend to infinity, we conclude that the average size of $\mathrm{Sel}_\phi(E_k)$ for $k \in T_m$ is also equal to $1 + 3^m$. The same argument shows that the average size of $\mathrm{Sel}_{\hat\phi}(E_k)$ for $k \in T_m$ is again equal to $1 + 3^{-m}$. This completes the proof of Theorem 4.

Remark 48. If $S \subset \mathbb{Z}$ is any acceptable set, then the average size of $\mathrm{Sel}_\phi(E_k)$ for $k \in S$ equals $\sum_{m\in\mathbb{Z}} \mu(S \cap T_m)(1 + 3^m)$, and the average size of $\mathrm{Sel}_{\hat\phi}(E_{-27k})$ equals $\sum_{m\in\mathbb{Z}} \mu(S \cap T_m)(1 + 3^{-m})$. Indeed, even though the sets $S \cap T_m$ are not in general acceptable, the sets of the form $S \cap T_{\Pi_1,\Pi_2}$ are, so we can argue as above.

7 Ranks of elliptic curves

In the previous section, we computed the average size of the ϕ-Selmer and $\hat\phi$-Selmer groups in any acceptable family of elliptic curves with j-invariant 0. In this section, we deduce an upper bound on the average rank of $E(\mathbb{Q})$ in such families. We also deduce a lower bound on the density of curves E_k having rank 0 or (3-Selmer) rank 1, respectively.

7.1 An upper bound on the average rank of elliptic curves with vanishing j-invariant

For any elliptic curve $E/\mathbb{Q}$ with j-invariant 0, we write $r(E)$, $r_3(E)$, $r_\phi(E)$, and $r_{\hat\phi}(E)$ for the ranks of the groups $E(\mathbb{Q})$, $\mathrm{Sel}_3(E)$, $\mathrm{Sel}_\phi(E)$, and $\mathrm{Sel}_{\hat\phi}(E')$ respectively, where $E' = E/\ker\phi$.

Proposition 49. *For $\phi\colon E \to E'$ as above, we have*

(a) $r(E) \leq r_3(E) \leq r_\phi(E) + r_{\hat\phi}(E)$.

(b) *If $c(\phi) = 3^m$, then $m \equiv r_3(E) - \dim_{\mathbb{F}_3} E[3](\mathbb{Q}) \pmod 2$.*

Proof. Claim (a) follows from the exact sequence [34, Corollary 1],

$$0 \to \frac{E'(\mathbb{Q})[\hat\phi]}{\phi(E(\mathbb{Q})[3])} \to \mathrm{Sel}_\phi(E) \to \mathrm{Sel}_3(E) \to \mathrm{Sel}_{\hat\phi}(E') \to \frac{\text{Ш}(E')[\hat\phi]}{\phi(\text{Ш}(E)[3])} \to 0. \tag{22}$$

As ϕ is adjoint with respect to the Cassels–Tate pairing [18, Theorem 1.2], there is an induced non-degenerate alternating pairing on the $\mathbb{F}_3$-vector space $\frac{\text{Ш}(E')[\hat\phi]}{\phi(\text{Ш}(E)[3])}$. The latter therefore has even $\mathbb{F}_3$-dimension, and (b) now follows from (21) and (22). □

Theorem 50. *Let $m \in \mathbb{Z}$, and suppose $S \subset T_m$ is an acceptable set. Then the (limsup of the) average rank of E_k, for $k \in S$ ordered by absolute value, is at most $|m| + 3^{-|m|}$.*

Proof. First assume that $m \geq 0$. Then one has the general inequality

$$2r_\phi(E) + 1 - 2m \leq 3^{r_\phi(E) - m}, \tag{23}$$

so that

$$r_\phi(E) \leq m - \frac{1}{2} + \frac{|\mathrm{Sel}_\phi(E)|}{2 \cdot 3^m}.$$

By Theorem 4, the average size of $\mathrm{Sel}_\phi(E_k)$ for $k \in S \subset T_m$ is $1 + 3^m$, so we conclude that the limsup of the average of $r_\phi(E_k)$ is at most $m + \frac{1}{2}3^{-m}$. Similarly, the average size of $\mathrm{Sel}_{\hat{\phi}}(E_{-27k})$ is $1 + 3^{-m}$, so we conclude from the case $m = 0$ of inequality (23) that the limsup of the average of $r_{\hat{\phi}}(E_k)$ is at most $\frac{1}{2}3^{-m}$. Combining these bounds with Proposition 49(i), the limsup of the average rank of E_k for $k \in S$ is seen to be at most $m + 3^{-m}$. For $m < 0$, the roles of ϕ and $\hat{\phi}$ are reversed, so the average rank bounds that we obtain for m and $-m$ are the same. $\square$

Proof of Theorem 5. We observe that, by the explicit congruence description of T_m in §6.4, any $k \in T_m$ (for $|m| > 1$) must satisfy $p_j^2 \mid k$ for some $j \geq |m| - 1$, where we again use p_i to denote the i-th prime. Hence, by the uniformity estimate [11, Proposition 29], we have that

$$\sum_{|m| > M} \sum_{\substack{k \in T_m \\ k < X}} \mathrm{Sel}_\phi(E_k) = \sum_{j \geq M} O(X/p_j^2) = O(X/p_M),$$

where the implied constant is independent of M. Theorem 50 therefore gives the following bound on the (limsup of the) average rank of the elliptic curves E_k for nonzero $k \in \mathbb{Z}$:

$$\limsup \operatorname{avg}_{k \in \mathbb{Z}} r(E_k) \leq \lim_{M \to \infty} \sum_{m=-M}^{M} \mu(T_m)(|m| + 3^{-|m|}) + O(1/p_M) = \sum_{m=-\infty}^{\infty} \mu(T_m)(|m| + 3^{-|m|}),$$

where $\mu(T_m)$ denotes the density of integers in the set T_m. Using Proposition 34 and the explicit description given in §6.4 of T_m as the disjoint union

$$T_m = \bigcup_n \bigcup T_{\Pi_1, \Pi_2},$$

we can estimate the densities $\mu(T_m)$ to arbitrary precision. One may also prove, e.g., that

$$\sum_{|m| > 5} \mu(T_m)(|m| + 3^{-|m|}) < 0.001.$$

A computation in Mathematica produces the table of densities in the introduction, and it follows that the average rank of E_k is less than 1.29.

We obtain a better bound on the average rank if we combine with the recent work of Alpoge [1], who proves that the average size of the 2-Selmer group of E_k, $k \in S$, is 3. Since the 3-Selmer ranks—and therefore (due to the work of [21]) the 2-Selmer parity—is constant for 100% of E_k for $k \in T_m$ by Theorems 4(ii) and 49(ii), this implies that the average rank of E_k, $k \in S$, is less than 4/3 on any T_m, giving the bound:

$$\operatorname{avg}_{k \in \mathbb{Z}} r(E) \leq \sum_{m=-1}^{1} \mu(T_m)(|m| + 3^{-|m|}) + \frac{4}{3}(1 - \mu(S_1 \cup S_0 \cup S_1)) < 1.21.$$

$\square$

7.2 A lower bound on the proportion of elliptic curves with vanishing j-invariant having 3-Selmer rank 0 or 1

Proof of Theorem 6. Let s_0 denote the liminf of the natural density of $k \in T_0$ for which $r_\phi(E_k) = 0$. Then by Theorem 4(iii), s_0 is also the liminf of the natural density of $k \in T_0$ for which $r_{\hat{\phi}}(E_k) = 0$. Since the average size of $|\mathrm{Sel}_\phi(E_k)|$, $k \in \mathbb{Z}$, is 2, we must have

$$s_0 \cdot 1 + (1 - s_0) \cdot 3 \leq 2,$$

implying $s_0 \geq 1/2$. It follows that a lower density of at least $1/2$ of the curves E_k, $k \in T_0$, satisfy $r_\phi(E_k) = r_{\hat{\phi}}(E_k) = r_3(E_k) = 0$, and thus $r(E_k) = 0$. Theorem 6 follows, since the density of T_0 is at least .399, and $(1/2)(.399) > .199$. $\square$

Proof of Theorem 7. Let s_1 denote the liminf of the natural density of $k \in T_1$ for which $r_\phi(E_k) = 1$. Then by Theorem 4(iii), s_1 is also the liminf of the natural density of $k \in T_1$ for which $r_{\hat{\phi}}(E_k) = 0$. Since the average size of $|\mathrm{Sel}_\phi(E_k)|$, $k \in T_1$, is 4, we see that

$$s_1 \cdot 3 + (1 - s_1) \cdot 9 \leq 4,$$

implying $s_1 \geq 5/6$. In conjunction with the exact sequence (22), this implies that a lower density of at least $5/6$ of the curves E_k, $k \in T_1$, satisfy $r_{\hat{\phi}}(E_k) = 0$ and $r_\phi(E_k) = r_3(E_k) = 1$ (and under the assumption that $Ш(E_k)[3^\infty]$ is finite, that $r(E_k) = 1$ as well). The identical argument with T_{-1} in place of T_1 shows that a lower density of at least $5/6$ of the curves E_k, $k \in T_{-1}$, satisfy $r_\phi(E_k) = 0$ and $r_{\hat{\phi}}(E_k) = 1$. By (22) and the fact that $\frac{Ш(E')[\hat{\phi}]}{\phi(Ш(E)[3])}$ has even rank, these curves also satisfy $r_3(E_k) = 1$ (and again $r(E_k) = 1$ under the assumption that $Ш(E_{-27k})[3]$ is trivial). Theorem 7 now follows, because the density of $T_1 \cup T_{-1}$ is at least .494, and $(5/6)(.494) > .411$. $\square$

Since $.199 + .411 = .61$, we conclude that at least 61% of all E_k have rank 0 or 1, which is Corollary 8.

8 The average size of the ϕ-Selmer group over a number field

In this section, we generalize Theorem 2 to the case where the ground field is an arbitrary number field F, and from this generalization we deduce Theorems 11–14. The main tool is [13, Thm. 13], which gives a general framework for geometry-of-numbers methods over arbitrary global fields. We recall the setup and the notation.

First, recall that the elliptic curves E_k of j-invariant 0 over F (and the associated isogenies $\phi_k : E_k \to E_{-27k}$) are classified up to isomorphism by the value of k, where we view k as an element of F^*/F^{*6}. To order the elliptic curves E_k over F up to isomorphism, we use a natural height function on F^*/F^{*6}, defined as follows: if $\tilde{k} \in F^*$ is a representative for $k \in F^*/F^{*6}$, and $I(\tilde{k})$ is the ideal

$$I(\tilde{k}) := \{a \in F\colon a^6\tilde{k} \in \mathcal{O}_F\},$$

then

$$H(k) := N(I(\tilde{k}))^6 \prod_{\mathfrak{p} \in M_\infty} |\tilde{k}|_p,$$

where M_∞ denotes the set of infinite places of F. There is also a natural height function on the set $F_\infty := \prod_{\mathfrak{p}\in M_\infty} F_\mathfrak{p}$, defined by

$$H((k_\mathfrak{p})_{\mathfrak{p}\in M_\infty}) = \prod_{\mathfrak{p}\in M_\infty} |k_\mathfrak{p}|_\mathfrak{p}.$$

In order to take averages over subsets of E_k defined by local (congruence) conditions on k, we require a notion of functions on F that are defined by local conditions. We say a function $\psi\colon F \to [0,1]$ is *defined by local congruence conditions* if there exist local functions $\psi_\mathfrak{p}\colon F_\mathfrak{p} \to [0,1]$ for every finite place $\mathfrak{p}$ of F, and a function $\psi_\infty\colon F_\infty \to [0,1]$, such that the following two conditions hold:

(1) For all $w \in F$, the product $\psi_\infty(w)\prod_{\mathfrak{p}\notin M_\infty}\psi_\mathfrak{p}(w)$ converges to $\psi(w)$.

(2) For each finite place $\mathfrak{p}$, and for $\mathfrak{p}=\infty$, the function $\psi_\mathfrak{p}$ is nonzero on some open set and locally constant outside some closed subset of $F_\mathfrak{p}$ of measure 0.

A subset of F is said to be *defined by local congruence conditions* if its characteristic function is defined by local congruence conditions.

Let Σ_0 be the fundamental domain for the action of F^* on F as constructed in [13, §3.4], where $\alpha \in F^*$ acts on $\beta \in F$ by $\alpha.\beta = \alpha^6\beta$. Then it is shown in [13, §3.4] that Σ_0 is defined by local congruence conditions. For any $X > 0$, let F_X denote the set of $k \in F^*$ such that $H(k) < X$. Then $\Sigma_0 \cap F_X$ is finite [13, §3.4]. We will think of the elliptic curves E_k as elements of Σ_0, so that the set of all E_k, with $k \in F^*/F^{*6}$ and $H(k) < X$, is naturally in bijection with the finite set $\Sigma_0 \cap F_X$.

A family $\{E_k\}$ of sextic twists defined by local congruence conditions is then a subset $\Sigma_1 \subset \Sigma_0$ defined by local congruence conditions. In that case, the characteristic function χ_{Σ_1} of Σ_1 factors as

$$\chi_{\Sigma_1} = \chi_{\Sigma_{1,\infty}} \prod_{\mathfrak{p}\notin M_\infty} \chi_{\Sigma_{1,\mathfrak{p}}}.$$

For each finite place $\mathfrak{p}$ of F, let $\Sigma_{1,\mathfrak{p}}$ be the subset of $F_\mathfrak{p}$ whose characteristic function is $\chi_{\Sigma_{1,\mathfrak{p}}}$, and let $\Sigma_{1,\infty}$ be the subset of F_∞ whose characteristic function is $\chi_{\Sigma_{1,\infty}}$. Let $\mathcal{O}_\mathfrak{p}$ denote the completion of the ring of integers $\mathcal{O}_F$ at $\mathfrak{p}$, and $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation normalized so that the valuation of a uniformizer is 1. We say that the family of elliptic curves E_k defined by Σ_1 is *large* if $\Sigma_{1,\mathfrak{p}}$ contains the set $\mathcal{O}_\mathfrak{p}(2) = \{k \in \mathcal{O}_\mathfrak{p}\colon v_\mathfrak{p}(k) < 2\}$ for all but finitely many finite places $\mathfrak{p}$, and if $\Sigma_{1,\infty}$ is a non-empty union of cosets in F_∞^*/F_∞^{*6}. Recall that $\Sigma_{0,\mathfrak{p}} = \mathcal{O}_\mathfrak{p}(6) \supset \mathcal{O}_\mathfrak{p}(2)$ for all finite $\mathfrak{p}$, so Σ_0 is itself large.

To state the analogue of Theorem 2 over F, we define

$$c_\infty(\phi_k) := \prod_{\mathfrak{p}\in M_\infty} c_\mathfrak{p}(\phi_{k_\mathfrak{p}})$$

for any $k = (k_\mathfrak{p}) \in F_\infty^*$, and also let $F_{\infty,X}$ be the set of $k \in F_\infty$ with height less than X.

Theorem 51. *Let Σ_1 be a large family of elliptic curves E_k. When the elliptic curves E_k, $k \in \Sigma_1$, are ordered by the height $H(k)$ of k, the average size of $\mathrm{Sel}_{\phi_k}(E_k)$ is*

$$1 + \frac{\displaystyle\int_{k\in\Sigma_{1,\infty}\cap F_{\infty,1}} c_\infty(\phi_k)\, d\mu_\infty^*(k)}{\displaystyle\int_{k\in\Sigma_{1,\infty}\cap F_{\infty,1}} d\mu_\infty^*(k)} \prod_{\mathfrak{p}\notin M_\infty} \frac{\displaystyle\int_{k\in\Sigma_{1,\mathfrak{p}}} c_\mathfrak{p}(\phi_k)dk}{\displaystyle\int_{k\in\Sigma_{1,\mathfrak{p}}} dk}.$$

Here, dk denotes the Haar measure on $\mathcal{O}_\mathfrak{p}$, normalized so that $\mathcal{O}_\mathfrak{p}$ has volume 1, and $d\mu_\infty^*(k)$ is the Haar measure on F_∞ normalized so that the covolume of $\mathcal{O}_F$ in F_∞ is 1.

Proof. By duality, we may replace ϕ by $\hat{\phi}$ and E_k by E'_k. Then by Corollary 40, it suffices to count the number of irreducible locally soluble $\mathrm{SL}_2(F)$-orbits on $V(F)$ with discriminant in Σ_1 and with height less than X. Theorem 51 then follows from the very general counting result [13, Thm. 13]. To apply that result to our situation, we take $G = \mathrm{SL}_2$ and $V = \mathrm{Sym}^3 2$, the space of binary cubic forms. The GIT quotient S is the affine line $\mathbb{A}^1$ and the map $\mathrm{inv} : V \to S$ is the discriminant $f \mapsto \mathrm{disc}(f)$. We take $V(F)^{\mathrm{irr}}$ to be the subset of irreducible cubic forms, and the weight function m_0 is the characteristic function of $V(F)^{\mathrm{loc.\,sol.}} \cap \mathrm{inv}^{-1}(\kappa.\Sigma_1) \subset V(F)$, for some nonzero $\kappa \in \mathcal{O}_F$, which we will choose momentarily. The $\mathfrak{p}$-adic integrals in Theorem 51 coincide with those in [13, Thm. 13] by Theorems 27 and 28. Finally, we note that the Tamagawa number $\tau_{\mathrm{SL}_2,F}$ equals 1. Thus, it remains to verify the six axioms in [13, Thm. 13].

Axiom - (G,V) is satisfied since the unique invariant disc is a degree four polynomial and SL_2 is semisimple. To guarantee that Axiom - Local Condition is satisfied, it is enough to let $\kappa = 3$. Indeed, this follows from the proof of Theorem 41, which works over any finite extension of $\mathbb{Q}_p$. Axiom - Local Spreading is satisfied since there is a section of $\mathrm{inv}\colon V \to S$ defined over $\mathcal{O}_F[1/2]$ given by $k \mapsto 3x^2y + (k/4)y^3$. Axiom - Counting at Infinity I and II is verified exactly as in the case of PGL_2 acting on binary quartic forms [13, §4.1]. Finally, to verify Axiom - Uniformity Estimate in our situation, note that by Propositions 22 and 35, the set $\mathrm{inv}^{-1}(\Sigma_{1,\mathfrak{p}}) \subset V(\mathcal{O}_\mathfrak{p})$ contains all cubic forms with discriminant not divisible by $\mathfrak{p}^2$, for all but finitely many primes $\mathfrak{p}$ of F. The uniformity estimate therefore follows from [12, Thm. 17]. □

Proof of Theorem 11. We take $\Sigma_1 = \Sigma_0$ in Theorem 51 and use Proposition 39 to compute the archimedean factor. □

Proof of Theorem 12. The proofs of parts (i) and (ii) are identical to the case $F = \mathbb{Q}$, where for part (ii) we use Theorem 51 in place of Theorem 2.

To prove the final statements of the theorem, we need to compute $c_\mathfrak{p}(\phi_k)$ for $k \in \mathcal{O}_F$ and for sufficiently many primes $\mathfrak{p}$ of F. If $\mathfrak{p}$ is any finite prime of F above $p \notin \{2, 3, \infty\}$, then we have the following generalization of Proposition 34: if $k \in \mathcal{O}_\mathfrak{p}$ is sixth-power-free, and χ_K denotes the quadratic character attached to $K = F_\mathfrak{p}(\sqrt{k})$, then

$$c_\mathfrak{p}(\phi_k) = \begin{cases} 3^{-\chi_K(\mathfrak{p})} & \text{if } \sqrt{-3} \notin F_\mathfrak{p} \text{ and } v_\mathfrak{p}(k) \in \{2,4\}; \\ 1 & \text{otherwise.} \end{cases} \tag{24}$$

This follows from Table 1 in [22] and Tate's algorithm, which shows that the condition $v_\mathfrak{p}(k) \in \{2, 4\}$ is equivalent to E_k having reduction type IV or IV*.

As F does not contain $\sqrt{-3}$, there are infinitely many places $\mathfrak{p}$ of F for which $F_\mathfrak{p}$ does not contain $\sqrt{-3}$. It then follows from (24) that for any $m \in \mathbb{Z}$, the set of $k \in F^*/F^{*6}$ for which $c(\phi_k) = 3^m$ has positive density.

On the other hand, if F contains $\sqrt{-3}$, then $c(\phi_k) = 1$ for all $k \in F^*/F^{*6}$, by Proposition 52 below. In other words, $F^*/F^{*6} = T_0(F)$. □

Proposition 52. *Let F be a number field containing $\sqrt{-3}$. Then $c(\phi_k) = 1$ for any $k \in F^*$.*

Proof. For any finite place $\mathfrak{p}$ of F, we have $c_{\mathfrak{p}}(\phi_k) = \alpha \cdot c_p(E_{-27k})/c_p(E_k)$, where $\alpha = \left|\frac{\phi_k^* \omega'}{\omega}\right|_{\mathfrak{p}}^{-1}$; this result is due to Schaefer [39, Lem. 3.8] (see also [22, Lem. 4.2]). Here, ω' and ω denote Néron differentials for E_{-27k} and E_k, and $|\cdot|_{\mathfrak{p}}$ is the normalized $\mathfrak{p}$-adic absolute value. Since F contains $\sqrt{-3}$, we have $E_{-27k} \simeq E_k$. Thus, ϕ is an endomorphism of degree 3, and hence must be $\sqrt{-3}$, up to a unit. It follows that $c_{\mathfrak{p}}(\phi_k) = 1$ if $\mathfrak{p}$ is not above 3 or ∞. If $\mathfrak{p}$ is above 3, then $c_{\mathfrak{p}}(\phi_k) = \alpha = |\sqrt{-3}|_{\mathfrak{p}}^{-1}$. If $\mathfrak{p}$ is an infinite place, then $\mathfrak{p}$ is complex and $c_{\mathfrak{p}}(\phi_k) = 1/3 = |\sqrt{-3}|_{\mathfrak{p}}^{-1}$, by Proposition 39. By the product formula, we conclude

$$c(\phi_k) = \prod_{\mathfrak{p}|\infty} |\sqrt{-3}|_{\mathfrak{p}}^{-1} \prod_{\mathfrak{p}|3} |\sqrt{-3}|_{\mathfrak{p}}^{-1} = 1,$$

as desired. □

It now follows from Theorem 51 and Proposition 52 that when F contains $\sqrt{-3}$, the average size of both the ϕ- and $\hat{\phi}$-Selmer groups is 2. By the arguments in Section 7, we conclude that the average rank of E_k, for $k \in F^*/F^{*6}$ ordered by height, is at most 1, and that 50% of the E_k have rank 0. This proves Theorem 14.

On the other hand, if F does not contain $\sqrt{-3}$, then we proceed as in the proof of Theorem 5, to show that the average rank of E_k, for $k \in F^*/F^{*6}$, is bounded. Since $T_0(F)$ and $T_1(F)$ each have positive density, the same arguments as in Section 7 then show that a positive proportion of E_k have 3-Selmer rank 0 and thus also Mordell-Weil rank 0, and a positive proportion of E_k have 3-Selmer rank 1. This proves Theorem 13.

Acknowledgments

We are grateful to Benedict Gross and Ila Varma for helpful conversations, and to the referee for helpful comments. The first author was supported by a Simons Investigator Grant and NSF grant DMS-1001828. The second author was supported by NSF grants DMS-1100511 and DMS-1502161. The third author was partially supported by NSF grant DMS-0943832.

References

[1] L. Alpoge, Ph.D. thesis, Princeton University, in preparation.

[2] L. Alpoge, The average number of integral points on elliptic curves is bounded, preprint (`arXiv:1412.1047`).

[3] M. Bhargava, Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* **159** (2004), no. 1, 217–250.

[4] M. Bhargava, Mass formulae for local fields, and conjectures on the density of number fields discriminants, *Internat. Math. Research Notices* (2007), Article ID rnm052, 20 pages.

[5] M. Bhargava and B. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. *Automorphic representations and L-functions,* 23–91*, Tata Inst. Fundam. Res. Stud. Math.* **22**, Tata Inst. Fund. Res., Mumbai, 2013.

[6] M. Bhargava, Z. Klagsbrun, R. Lemke Oliver, and A. Shnidman, Three-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field, preprint (`arXiv:1709.09790`).

[7] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, *Ann. of Math.* (2) **181** (2015), no. 1, 191–242.

[8] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, *Ann. of Math.* (2) **181** (2015), no. 2, 587–621.

[9] M. Bhargava and A. Shankar, The average number of elements in the 4-Selmer groups of elliptic curves is 7, preprint (`arXiv:1312.7333v1`).

[10] M. Bhargava and A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, preprint (`arXiv:1312.7859`).

[11] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.* **193** (2013), no. 2, 439–499.

[12] M. Bhargava, A. Shankar, and X. Wang. Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces, preprint (`arXiv:1512.03035`).

[13] M. Bhargava, A. Shankar, and X. Wang. Geometry-of-numbers methods over global fields II: Coregular representations, preprint.

[14] T. Browning, Many cubic surfaces contain rational points, preprint (`arXiv:1701.00525`).

[15] M. Bhargava and I. Varma, The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders, *Proc. Lond. Math. Soc.* (3) **112** (2016), no. 2, 235–266.

[16] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, Cambridge, 1991.

[17] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** 1966, 193–291.

[18] J. W. S. Cassels, Arithmetic on curves of genus 1, VIII: On conjectures of Birch and Swinnerton-Dyer, *J. reine angew. Math.* **217** (1965), 180–199.

[19] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[20] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[21] T. Dokchitser and V. Dokchitser, On the Birch–Swinnerton-Dyer quotient modulo squares, *Ann. of Math.* **172** (2010), no.1, 567–596.

[22] T. Dokchitser and V. Dokchitser, Local invariants of isogenous elliptic curves, *Trans. Amer. Math. Soc.* **367** (2015), no. 6, 4339–4358.

[23] V. Dokchitser, Root numbers of non-abelian twists of elliptic curves (with an appendix by Tom Fisher), *Proc. London Math. Soc.* (3) **91** (2005), no. 2, 300–324.

[24] G. Eisenstein, Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré à quatre indéterminées, *J. reine angew. Math.* **27** (1844), 75–79.

[25] É. Fouvry, Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$, *Séminaire de Théorie des Nombres, Paris, 1990-91, Progr. Math.* **108**, Birkhäuser Boston, MA, 1993.

[26] B. Gross and J. Parson, On the local divisibility of Heegner points, *Number theory, analysis and geometry*, 215–241, Springer, New York, 2012.

[27] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, *Invent. Math.* **111** (1993), no. 1, 171–195.

[28] D. Hilbert, *Theory of Algebraic Invariants* (1897; trans. R. C. Laubenbacher, ed. B. Sturmfels), Cambridge University Press 1993.

[29] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York 1969.

[30] E. Liverance, Binary cubic forms with many integral points, `http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/0998-8.pdf`

[31] D. Kane, On the Ranks of the 2-Selmer Groups of Twists of a Given Elliptic Curve, *Algebra & Number Theory* **7** (2013), 1253–1279.

[32] D. Kane and J. Thorne, On the ϕ-Selmer groups of the elliptic curves $y^2 = x^3 - Dx$, *Mathematical Proceedings of the Cambridge Philosophical Society* (2016), `http://dx.doi.org/10.17863/CAM.1298`.

[33] Z. Klagsbrun, B. Mazur, and K. Rubin, Disparity in Selmer ranks of quadratic twists of elliptic curves, *Ann. of Math.* (2) 178 (2013), no. 1, 287–320.

[34] R. Kloosterman and E. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, *J. Number Theory* **99** (2003), no. 1, 148–163.

[35] D. Kriz and C. Li, Goldfeld's conjecture and congruences between Heegner points, *Forum Math. Sigma* **7** (2019), e15, 80pp.

[36] B. Poonen and E. Rains, Random maximal isotropic subspaces and Selmer groups, *J. Amer. Math. Soc.*, **25** (2012), no. 1, 245–269. arXiv: 1009.0287

[37] S. Ruth, A bound on the average rank of j-invariant zero elliptic curves, Ph.D. thesis, Princeton University (2014).

[38] P. Satgé, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986), no. 3, 294–317.

[39] E. Schaefer, Class groups and Selmer groups, *J. Number Theory* **56** (1996), no. 1, 79–114.

[40] I. Schur, *Vorlesungen über Invariantentheorie*, Grundlehren der mathematischen Wissenschaften **143**, Springer: Berlin 1968.

[41] E. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951), 203–362.

[42] H. P. F. Swinnerton-Dyer, The effect of twisting on the 2-Selmer group, *Math. Proc. Cambridge Philos. Soc.* **145** (2008), no. 3, 513–526.

[43] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, *Lecture Notes in Mathematics* **476** (Modular Forms in One Variable IV, Antwerp 1972; B. J. Birch and W. Kuyk, eds.), 33–52.

[44] J. Thorne, Vinberg's representations and arithmetic invariant theory, *Algebra Number Theory* **7** (2013), no. 9, 2331–2368.

[45] J. Thorne, E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3, *Forum Math. Pi* **3** (2015), e1, 41 pp.