Séminaire BOURBAKI
64ème année, 2011-2012, n$^{\text{o}}$ 1049

Janvier 2012 / revised June 13, 2015

AVERAGE RANK OF ELLIPTIC CURVES
[after Manjul Bhargava and Arul Shankar]

by **Bjorn POONEN**

1. INTRODUCTION

1.1. Elliptic curves

An **elliptic curve** E over $\mathbb{Q}$ is the projective closure of a curve $y^2 = x^3 + Ax + B$ for some fixed $A, B \in \mathbb{Q}$ satisfying $4A^3 + 27B^2 \neq 0$ (the inequality is the condition for the curve to be smooth). Such curves are interesting because

1. they are the simplest algebraic varieties whose rational points are not completely understood, and
2. they are the simplest examples of projective algebraic groups of positive dimension.

The abelian group $E(\mathbb{Q})$ of rational points on E is finitely generated [Mor22]. Hence $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ for some nonnegative integer r (the **rank**) and some finite abelian group T (the **torsion subgroup**). The torsion subgroup is well understood, thanks to B. Mazur [Maz77], but the rank remains a mystery. Already in 1901, H. Poincaré [Poi01, p. 173] asked what is the range of possibilities for the minimum number of generators of $E(\mathbb{Q})$, but it is not known even whether r is bounded. There are algorithms that compute r successfully in practice, given integers A and B of moderate size, but to know that the algorithms terminate in general, it seems that one needs a conjecture: either the finiteness of the Shafarevich–Tate group Ш (or of its p-primary part for some prime p), or the Birch and Swinnerton-Dyer conjecture that r equals the **analytic rank** $r_{\text{an}} := \operatorname{ord}_{s=1} L(E, s)$ [BSD65].

The main results of Bhargava and Shankar (Section 1.4) concern the average value of r as E ranges over all elliptic curves over $\mathbb{Q}$.

1.2. Selmer groups

There is essentially only one known proof that $E(\mathbb{Q})$ is finitely generated. The hardest step involves proving the finiteness of $E(\mathbb{Q})/nE(\mathbb{Q})$ for some $n \geq 2$. This is done by embedding $E(\mathbb{Q})/nE(\mathbb{Q})$ into the n-**Selmer group** $\operatorname{Sel}_n(E)$, which we now define.

For each prime p, let $\mathbb{Q}_p$ be the field of p-adic numbers; also define $\mathbb{Q}_\infty := \mathbb{R}$. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. We write $\mathrm{H}^1(\mathbb{Q}, E)$, for example, to denote the profinite group cohomology $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}}))$.

Fix $n \geq 2$. For any abelian group or group scheme G, let $G[n]$ be the kernel of multiplication-by-n on G. Taking cohomology of

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \to 0$$

over $\mathbb{Q}$ and $\mathbb{Q}_p$ leads to the exact rows in the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow & & \\ 0 & \longrightarrow & \displaystyle\prod_{p\leq\infty} \frac{E(\mathbb{Q}_p)}{nE(\mathbb{Q}_p)} & \xrightarrow{\alpha} & \displaystyle\prod_{p\leq\infty} \mathrm{H}^1(\mathbb{Q}_p, E[n]) & \longrightarrow & \displaystyle\prod_{p\leq\infty} \mathrm{H}^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0 \end{array} \tag{1}$$

The group $\mathrm{H}^1(\mathbb{Q}, E[n])$ turns out to be infinite, and it is difficult to determine which of its elements are in the image of $E(\mathbb{Q})/nE(\mathbb{Q})$. But because arithmetic over $\mathbb{Q}_p$ is easier than arithmetic over $\mathbb{Q}$, one can determine which elements are *locally* in the image. With this in mind, define

$$\mathrm{Sel}_n(E) := \{x \in \mathrm{H}^1(\mathbb{Q}, E[n]) : \beta(x) \in \mathrm{image}(\alpha)\}$$

Diagram (1) shows that the subgroup $\mathrm{Sel}_n(E) \subseteq \mathrm{H}^1(\mathbb{Q}, E[n])$ is an upper bound for the image of $E(\mathbb{Q})/nE(\mathbb{Q})$. In fact, if we define also the **Shafarevich–Tate group**

$$Ш = Ш(E) := \ker\left(\mathrm{H}^1(\mathbb{Q}, E) \to \prod_{p\leq\infty} \mathrm{H}^1(\mathbb{Q}_p, E)\right),$$

then diagram (1) yields an exact sequence

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \mathrm{Sel}_n(E) \longrightarrow Ш[n] \longrightarrow 0. \tag{2}$$

Moreover, it turns out that $\mathrm{Sel}_n(E)$ is finite and computable.

1.3. Averaging over all elliptic curves

The average of an infinite sequence of real numbers $a_1, a_2, \ldots$ is defined as $\lim_{n\to\infty}(a_1 + \cdots + a_n)/n$, if the limit exists. This may depend on the ordering of the terms. Hence, to define the average rank of elliptic curves, we should first decide how to order them.

Tables such as [BK75, Cre97, Cre, Ste] order elliptic curves by their conductor N. But it is not known even how many elliptic curves have conductor $< X$ asymptotically as $X \to \infty$, so we cannot hope to prove anything nontrivial about averages for this ordering. Ordering by minimal discriminant runs into the same difficulty.

Therefore we order by height, which we now define. Elliptic curves $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + A'x + B'$ over $\mathbb{Q}$ are isomorphic if and only if there exists $q \in \mathbb{Q}^\times$ such that $(A', B') = (q^4 A, q^6 B)$. Therefore each isomorphism class contains a unique representative E_{AB} with $(A, B) \in \mathbb{Z}^2$ **minimal** in the sense that there is no prime p with $p^4 | A$ and $p^6 | B$. Let $\mathscr{E}$ be the set of all such E_{AB}. Define the (naïve) **height** $H(E_{AB}) = H(A, B) := \max\{|4A^3|, 27B^2\}$. (Other authors replace 4 and 27 by other positive constants; it is only the *exponents* that matter in the proofs.) For $X \in \mathbb{R}$, define $\mathscr{E}_{<X} := \{E \in \mathscr{E} : H(E) < X\}$. For any $\phi\colon \mathscr{E} \to \mathbb{R}$, define its **average** by

$$\mathrm{Average}(\phi) := \lim_{X \to \infty} \frac{\sum_{E \in \mathscr{E}_{<X}} \phi(E)}{\sum_{E \in \mathscr{E}_{<X}} 1},$$

if the limit exists. Define $\overline{\mathrm{Average}}(\phi)$ and $\underline{\mathrm{Average}}(\phi)$ similarly, but using lim sup or lim inf, respectively.

We may speak also of the **probability** or **density** of the set of elliptic curves satisfying a given property. Namely, the property P can be identified with its characteristic function $\chi_P\colon \mathscr{E} \to \{0, 1\}$; then define $\mathrm{Prob}(P) = \mathrm{Average}(\chi_P)$. Similarly define $\overline{\mathrm{Prob}}(P)$ and $\underline{\mathrm{Prob}}(P)$.

Example 1.1. — B. Mazur's theorem [Maz77] bounds the possibilities for the torsion subgroup T. The Hilbert irreducibility theorem shows that each nonzero possibility for T occurs rarely. Together, they show that $\mathrm{Prob}(T \neq 0)$ is 0.

1.4. Main results of Bhargava and Shankar

THEOREM 1.2 ([BS15a, Theorem 1.1]). — $\mathrm{Average}(\#\,\mathrm{Sel}_2) = 3$.

If one averages not over all of $\mathscr{E}$, but over a subset defined by finitely many congruence conditions on A and B (e.g., $A \equiv 5 \pmod 7$ and $B \equiv 3 \pmod 4$), then the average is still 3 [BS15a, Theorem 1.3]. This is interesting, given that one of the successful techniques for constructing elliptic curves of moderately large rank has been to restrict attention to congruence classes so as to maximize $\#E(\mathbb{F}_p)$ for the first few primes p [Mes82].

A similar argument leads to

THEOREM 1.3 ([BS15b, Theorem 1]). — $\overline{\mathrm{Average}}(\#\,\mathrm{Sel}_3) \leq 4$.[(1)]

Again one can obtain the same bound for elliptic curves satisfying finitely many congruence conditions. One can even impose congruence conditions at *infinitely* many primes as long as one can show that the conditions at large primes together are sieving out a negligible subset.

It is still not known whether $\mathrm{Average}(r)$ exists, but Theorems 1.2 and 1.3 yield upper bounds on $\overline{\mathrm{Average}}(r)$:

(1) After the original version of this survey was written, Bhargava and Shankar proved the stronger statement $\mathrm{Average}(\#\,\mathrm{Sel}_3) = 4$.

COROLLARY 1.4 ([BS15b, Corollary 2]). — $\overline{\text{Average}}(r) \leq 7/6$.

Proof. — Let $s = \dim \mathrm{Sel}_3$. The injection $E(\mathbb{Q})/3E(\mathbb{Q}) \hookrightarrow \mathrm{Sel}_3(E)$ yields $r \leq s$. Combining this with $6s - 3 \leq 3^s$ bounds r in terms of $\#\,\mathrm{Sel}_3$; then apply $\overline{\text{Average}}$ and use Theorem 1.3. (Why $6s-3$? Since 3^s is a convex function, it suffices to connect the points $(s, 3^s)$ for $s = 0, 1, \ldots$ in order by line segments, and to take the equation of the line segment that crosses the horizontal line $y = 4$.) □

Further consequences of Theorem 1.3 make use of results of Dokchitser–Dokchitser and Skinner–Urban, whose context can be best understood if we introduce a few more quantities. Taking the direct limit of (2) as n ranges through powers of a prime p yields the p^∞-**Selmer group** $\mathrm{Sel}_{p^\infty}(E)$ fitting in an exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty}(E) \longrightarrow Ш[p^\infty] \longrightarrow 0. \tag{3}$$

Each term in (3) has the form $(\mathbb{Q}_p/\mathbb{Z}_p)^c \oplus (\text{finite})$ for some nonnegative integer c called the **corank**. Let $r_{p^\infty} := \operatorname{corank} \mathrm{Sel}_{p^\infty}(E)$. Let $s'_p := \dim \mathrm{Sel}_p(E) - \dim E[p](\mathbb{Q})$. If $Ш'$ is the quotient of $Ш$ by its maximal divisible subgroup, then $s'_p - r_{p^\infty} = \dim Ш'[p]$, which is even since $Ш'[p^\infty]$ is a finite group with a nondegenerate alternating pairing [Cas62]. By (3), $r_{p^\infty} - r = \operatorname{corank} Ш[p^\infty]$, which is 0 if and only if $Ш[p^\infty]$ is finite. To summarize,

$$s'_p \;\equiv\; r_{p^\infty} \overset{\text{ST}}{=} r \overset{\text{BSD}}{=} r_{\text{an}}, \tag{4}$$

where the congruence is modulo 2, and the equalities labeled with the initials of Shafarevich–Tate and Birch–Swinnerton-Dyer are conjectural. Also,

$$\dim \mathrm{Sel}_p \;\geq\; s'_p \;\geq\; r_{p^\infty} \;\geq\; r. \tag{5}$$

In the direction of the conjectural equality $r_{p^\infty} = r_{\text{an}}$, we have two recent theorems:

THEOREM 1.5 ([DD10, Theorem 1.4]). — *For every elliptic curve E over $\mathbb{Q}$, we have* $r_{p^\infty} \equiv r_{\text{an}} \pmod 2$.

The **root number** $w \in \{\pm 1\}$ of an elliptic curve E over $\mathbb{Q}$ may be defined as the sign of the functional equation for the L-function $L(E, s)$, so the conclusion of Theorem 1.5 may also be written $(-1)^{s'_p} = w$.

THEOREM 1.6 ([SU14, Theorem 2(b)]). — *For any odd prime p and elliptic curve E over $\mathbb{Q}$ satisfying mild technical hypotheses, if $r_{p^\infty} = 0$, then $r_{\text{an}} = 0$.*

Combining Theorems 1.3 (with congruence conditions), 1.5, and 1.6 leads to

THEOREM 1.7 ([BS15b, §4.1,4.2]). —

(a) $\underline{\text{Prob}}(\dim \mathrm{Sel}_3 = s'_3 = r_{3^\infty} = r = r_{\text{an}} = 0)$ *is positive.*
(b) $\underline{\text{Prob}}(\dim \mathrm{Sel}_3 = s'_3 = r_{3^\infty} = 1)$ *is positive.*

Sketch of proof. — S. Wong [Won01, §9] constructed a positive-density subset $\mathscr{F} \subset \mathscr{E}$ such that whenever $E \in \mathscr{F}$, its (-1)-twist is in $\mathscr{F}$ and has the opposite root number. By Example 1.1, one can assume that $E(\mathbb{Q})[3] = 0$ for every $E \in \mathscr{F}$. Then, by the sentence after Theorem 1.5, the parity of $\dim \mathrm{Sel}_3 = s_3'$ for $E \in \mathscr{F}$ is equidistributed. Moreover, $\mathscr{F}$ can be chosen so that Theorem 1.6 applies to every $E \in \mathscr{F}$, and so that the conclusion of Theorem 1.3 holds for $\mathscr{F}$. For large X, let p_0 be the proportion of curves in $\mathscr{F}$ with $\dim \mathrm{Sel}_3 = 0$; define p_1 similarly. Our bound on the average of $\#\mathrm{Sel}_3$ yields

$$p_0 \cdot 1 + p_1 \cdot 3 + \left(\frac{1}{2} - p_0\right) \cdot 9 + \left(\frac{1}{2} - p_1\right) \cdot 27 \;\leq\; 4 + o(1).$$

This, with $p_0, p_1 \leq 1/2 + o(1)$, implies $p_0 \geq 1/4 - o(1)$ and $p_1 \geq 5/12 - o(1)$. This proves the bounds for $\dim \mathrm{Sel}_3 = s_3'$. For $E \in \mathscr{F}$, if $s_3' = 0$, then $r_{3^\infty} = r = r_{\mathrm{an}} = 0$ too by (5) and Theorem 1.6. If $s_3' = 1$, then $r_{3^\infty} = 1$ too since $s_3' - r_{3^\infty} \in 2\mathbb{Z}_{\geq 0}$. □

Theorem 1.7(a) implies in particular that a positive proportion of elliptic curves over $\mathbb{Q}$ have both rank 0 and analytic rank 0 and hence satisfy the Birch and Swinnerton-Dyer conjecture that $r = r_{\mathrm{an}}$. Theorem 1.7(b) implies a conditional statement for rank 1:

Corollary 1.8 ([BS15b, §4.1]). — *If* Ш(E) *(or at least its* 3*-primary part) is finite for every elliptic curve* E *over* $\mathbb{Q}$*, then* $\underline{\mathrm{Prob}}(r = 1)$ *is positive.*

2. PREVIOUS WORK OF OTHER AUTHORS

This section exists only to put the theorems above in context. Readers impatient to understand the proof of Theorem 1.2 may jump to Section 3.

2.1. Average analytic rank

Using analogues of Weil's "explicit formula", many authors have given conditional bounds on the average *analytic* rank, both for the family of quadratic twists of a fixed elliptic curve over $\mathbb{Q}$, and for the family $\mathscr{E}$ of all elliptic curves over $\mathbb{Q}$. *All these analytic results over* $\mathbb{Q}$ *are conditional on the Riemann hypothesis for the* L*-functions of the elliptic curves involved.* At the time that some of these results were proved, the assertion that the L-function admits an analytic continuation to $\mathbb{C}$ was an assumption too, but today this is a consequence of the theorem that all elliptic curves over $\mathbb{Q}$ are modular [BCDT01].

D. Goldfeld [Gol79] proved the conditional bound $\overline{\mathrm{Average}}(r_{\mathrm{an}}) \leq 3.25$ for the family of quadratic twists of a fixed elliptic curve E over $\mathbb{Q}$, and conjectured that the correct constant was $1/2$. The constant 3.25 was later improved to 1.5 by D. R. Heath-Brown [HB04, Theorem 3].

For the family of all elliptic curves over $\mathbb{Q}$, A. Brumer proved the conditional bound $\overline{\mathrm{Average}}(r_{\mathrm{an}}) \leq 2.3$ [Bru92]. He also proved the same bound for elliptic curves over $\mathbb{F}_q(t)$

unconditionally. In the case of $\mathbb{F}_q(t)$, the inequality $r \le r_{\mathrm{an}}$ is known, so one deduces $\overline{\mathrm{Average}}(r) \le 2.3$ in this setting. Over $\mathbb{Q}$, the constant 2.3 was improved to 2 by Heath-Brown [HB04, Theorem 1] and to 25/14 by M. Young [You06]. The latter implied the (conditional) positivity of $\underline{\mathrm{Prob}}(r_{\mathrm{an}} \le 1)$, and then also of $\underline{\mathrm{Prob}}(r = r_{\mathrm{an}} \le 1)$, because $r_{\mathrm{an}} \le 1$ implies $r = r_{\mathrm{an}}$ ([Kol88, Kol90, GZ86] with [BFH90] or [MM91]).

Conditional bounds on $\overline{\mathrm{Average}}(r_{\mathrm{an}})$ for other algebraic families of elliptic curves and abelian varieties have been given by É. Fouvry and J. Pomykała [FP93], P. Michel [Mic95, Mic97], J. Silverman [Sil98], and R. Wazir [Waz04].

2.2. Distribution of Selmer groups

For the family of elliptic curves $y^2 = x^3 + k$ over $\mathbb{Q}$, É. Fouvry proved $\overline{\mathrm{Average}}(3^{r/2}) < \infty$, by bounding the average size of the Selmer group associated to a 3-isogeny (a slight generalization of the Selmer groups we have considered so far) [Fou93]. This implies that $\overline{\mathrm{Average}}(r) < \infty$ in this family.

Recall our notation $s_p' := \dim \mathrm{Sel}_p(E) - \dim E(\mathbb{Q})[p]$. For the family of quadratic twists of $y^2 = x^3 - x$ over $\mathbb{Q}$, Heath-Brown proved not only that $\mathrm{Average}(s_2') = 3$ but also that

$$\mathrm{Prob}\,(s_2' = d) = \left(\prod_{j \ge 0} (1 + 2^{-j})^{-1}\right)\left(\prod_{j=1}^{d} \frac{2}{2^j - 1}\right) \tag{6}$$

for each $d \in \mathbb{Z}_{\ge 0}$ [HB93, HB94]. P. Swinnerton-Dyer [SD08] and D. Kane [Kan13] generalized this by obtaining the same distribution for the family of quadratic twists of any E over $\mathbb{Q}$ with $E[2] \subset E(\mathbb{Q})$ but no rational cyclic 4-isogeny. Heath-Brown's approach was used also by G. Yu [Yu06] to prove finiteness of $\overline{\mathrm{Average}}(\#\,\mathrm{Sel}_2)$ for the family of all elliptic curves with $E[2] \subset E(\mathbb{Q})$. In certain subfamilies of this, surprises occur: see [Yu05].

A probabilistic model predicting the distribution of s_p' for any prime p was proposed in [PR12]; for $p = 2$ the prediction is consistent with (6).

Earlier, C. Delaunay [Del01] proposed a heuristic for the distribution of $\#Ш$, in analogy with the Cohen–Lenstra heuristics [CL84].

Finally, there is a conjecture that elliptic curves tend to have the smallest rank compatible with the root number, which is expected to be equidistributed. This was proposed in [Gol79] for the case of quadratic twists of a fixed curve, but it is probably true more generally. In other words, it is expected that $\mathrm{Prob}(r = 0)$ and $\mathrm{Prob}(r = 1)$ are both 1/2. See also [KS99b, §5] and [KS99a].

The three predictions above are compatible with the equation $s_p' = \dim Ш[p] + r$ arising from (2): see [PR12, §5].

2.3. Average size of Selmer groups over function fields

The closest parallel to the work of Bhargava and Shankar is a 2002 article by A. J. de Jong proving the analogue of Theorem 1.3 for function fields, with a slightly weaker bound [dJ02]. Namely, for any finite field $\mathbb{F}_q$ of characteristic not 3, de Jong proved

$\overline{\text{Average}}(\#\operatorname{Sel}_3) \le 4 + \epsilon(q)$ for the family of all elliptic curves over $\mathbb{F}_q(t)$, where $\epsilon(q)$ is an explicit rational function of q tending to 0 as $q \to \infty$. This implies a corresponding bound for $\overline{\text{Average}}(r)$ for such $\mathbb{F}_q(t)$. Moreover, de Jong gave heuristics that in hindsight hint that $\text{Average}(\#\operatorname{Sel}_3) = 4$ not only for $\mathbb{F}_q(t)$ but also for $\mathbb{Q}$.

The approaches of de Jong and Bhargava–Shankar are similar. Namely, both count integral models of geometric objects representing elements of $\operatorname{Sel}_n(E)$. (For $n = 3$, these objects are plane cubic curves.) But the more delicate estimates, essential for obtaining an asymptotically *sharp* upper bound on $\sum_{E \in \mathscr{E}_{<X}} \#\operatorname{Sel}_{2 \text{ or } 3}(E)$ and a matching lower bound (for Sel_2), are unique to Bhargava–Shankar.

3. BACKGROUND: n-DIAGRAMS AND BINARY QUARTIC FORMS

Each element of $\mathrm{H}^1(\mathbb{Q}, E[n])$ has a geometric avatar, called an n-diagram. To count Selmer group elements, we will count the possibilities for the coefficients of the polynomial equations defining their avatars. We follow [CFO+08, §1.3] in Sections 3.1–3.3, and [BSD63] in Section 3.5. The goal of this section is (10).

3.1. Diagrams

Fix a field k, a separable closure $\overline{k}$, and an elliptic curve E over k. A **diagram** for E is a morphism of varieties from an E-torsor C to a variety S. An **isomorphism of diagrams** is given by an isomorphism of E-torsors $C \to C'$ and an isomorphism of varieties $S \to S'$ making the obvious square commute.

3.2. n-diagrams

Let $O \in E(k)$ be the identity. Fix an integer $n \ge 2$ with $\operatorname{char} k \nmid n$. The **trivial n-diagram** is the diagram $E \to \mathbb{P}^{n-1}$ determined by the linear system $|nO|$, where E is viewed as trivial E-torsor. More generally, an **n-diagram** is a twist $C \to S$ of the trivial n-diagram, i.e., a diagram that becomes isomorphic to the trivial n-diagram after base extension of both to $\overline{k}$. In particular, S must be a **Brauer-Severi variety**, a twist of projective space. (For this reason, n-diagrams are called Brauer-Severi diagrams in [CFO+08, §1.3].)

The automorphism group of the trivial n-diagram over $\overline{k}$ is given by $E[n]$ acting as translations on E and acting compatibly on $\mathbb{P}^{n-1}$. Galois descent theory then yields a bijection

$$\frac{\{n\text{-diagrams for } E\}}{\text{isomorphism}} \longleftrightarrow \mathrm{H}^1(k, E[n]). \tag{7}$$

Remark 3.1. — Elements of $\mathrm{H}^1(k, E[n])$ are in bijection also with geometric objects called n-coverings [CFO+08, §1.2]. But it is the n-diagrams that are easiest to count.

Remark 3.2. — The action of $E[n]$ on $\mathbb{P}^{n-1}$ is given by an injective homomorphism $E[n] \to \mathrm{PGL}_n$.

3.3. Solvable and locally solvable n-diagrams

The homomorphism $\mathrm{H}^1(k, E[n]) \to \mathrm{H}^1(k, E)$ corresponds to sending an n-diagram $C \to S$ to the torsor C. Its kernel, which is isomorphic to $E(k)/nE(k)$ (cf. (1)), corresponds to the set of n-diagrams $C \to S$ for which C has a k-point; such n-diagrams are called **solvable**:

$$\frac{\{\text{solvable } n\text{-diagrams for } E\}}{\text{isomorphism}} \longleftrightarrow \frac{E(k)}{nE(k)}. \tag{8}$$

An n-diagram $C \to S$ over $\mathbb{Q}$ is **locally solvable** if C has a $\mathbb{Q}_p$-point for all $p \leq \infty$. In this case, S too has a $\mathbb{Q}_p$-point for all $p \leq \infty$, and hence $S \simeq \mathbb{P}^{n-1}$, by the local-global principle for the Brauer group. (Not every n-diagram with $S \simeq \mathbb{P}^{n-1}$ is locally solvable, however.) By (1), we have a bijection

$$\frac{\{\text{locally solvable } n\text{-diagrams for } E\}}{\text{isomorphism}} \longleftrightarrow \mathrm{Sel}_n(E). \tag{9}$$

3.4. Binary quartic forms

With an eye towards Section 3.5, we consider the space $\mathbb{Q}[x, y]_4$ of binary quartic forms. There is a left action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{Q}[x, y]_4$ given by $(\gamma \cdot f)(x, y) := f((x, y)\gamma)$ (we view (x, y) as a row vector). This induces an action of $\mathrm{GL}_2(\mathbb{Q})$ on the algebra $\mathbb{Q}[a, b, c, d, e]$ of polynomial functions in the coefficients of $f := ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$. The subalgebra of SL_2-invariants is $\mathbb{Q}[a, b, c, d, e]^{\mathrm{SL}_2} = \mathbb{Q}[I, J] = \mathbb{Q}[A, B]$, where

$$\begin{aligned} I &:= 12ae - 3bd + c^2 & A &:= -I/3 \\ J &:= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 & B &:= -J/27. \end{aligned}$$

(Why $-1/3$ and $-1/27$? To make the Jacobian statement in Section 3.5 true.) A quartic form is separable if and only if its discriminant $\Delta := -(4A^3+27B^2)$ is nonzero. If $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ and $f \in \mathbb{Q}[x, y]_4$, then $A(\gamma \cdot f) = (\det \gamma)^4 A(f)$ and $B(\gamma \cdot f) = (\det \gamma)^6 B(f)$. Thus the twisted GL_2-action $\gamma * f := (\det \gamma)^{-2}(\gamma \cdot f)$ induces a PGL_2-action preserving A and B.

3.5. Locally solvable 2-diagrams and binary quartic forms

Let $f \in \mathbb{Q}[x, y]_4$ be such that $\Delta(f) \neq 0$. Let C be the curve $z^2 = f(x, y)$ in the weighted projective plane $\mathbb{P}(1, 1, 2)$. Let $\operatorname{Jac} C$ be its Jacobian. Then there is an isomorphism between $\operatorname{Jac} C$ and the elliptic curve $y^2 = x^3 + A(f)x + B(f)$, and the isomorphism depends algebraically on the coefficients of f. In fact, this makes $C \xrightarrow{(x:y)} \mathbb{P}^1$ a 2-diagram. There is an approximate converse: any locally solvable 2-diagram for E is a degree 2 morphism $C \to \mathbb{P}^1$ equipped with an isomorphism $\operatorname{Jac} C \to E$ such that C has a $\mathbb{Q}_p$-point for all $p \leq \infty$; such a curve C is given by $z^2 = f(x, y)$ in $\mathbb{P}(1, 1, 2)$, for some $f(x, y) \in \mathbb{Q}[x, y]_4$ such that $\Delta(f) \neq 0$.

Two locally solvable 2-diagrams are isomorphic if and only if the associated morphisms $C \to \mathbb{P}^1$ and $C' \to \mathbb{P}^1$ are isomorphic *forgetting the torsor structures* (if there

exists an isomorphism of such morphisms, there is also an isomorphism respecting the torsor structures, because the automorphism group of E over $\mathbb{Q}$ is never larger than $\{\pm 1\}$). And two such morphisms are isomorphic if and only if corresponding quartic forms are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent after multiplying one by an element of $\mathbb{Q}^{\times 2}$. If the quartic forms already have the same invariants, then the element of $\mathbb{Q}^{\times 2}$ is unnecessary.

Let $V = \operatorname{Spec} \mathbb{Q}[a,b,c,d,e]$ be the moduli space of quartic forms, and let $\mathcal{S} = \operatorname{Spec} \mathbb{Q}[A,B]$. Let $V' \subset V$ and $\mathcal{S}' \subset \mathcal{S}$ be the open subvarieties defined by $\Delta \neq 0$. There is a morphism $V \to \mathcal{S}$ taking a quartic form to its pair of invariants. Let V_{AB} be the fiber above $(A,B) \in \mathcal{S}'(\mathbb{Q})$. Define the locally solvable subset $V(\mathbb{Q})^{\mathrm{ls}} \subset V'(\mathbb{Q})$ as the set of $f \in \mathbb{Q}[x,y]_4$ with $\Delta \neq 0$ such that $z^2 = f(x,y)$ has a $\mathbb{Q}_p$-point for all $p \leq \infty$. Define $V_{AB}(\mathbb{Q})^{\mathrm{ls}}$ similarly. For each $(A,B) \in \mathcal{S}'(\mathbb{Q})$, combining the previous paragraph with (9) for $n = 2$ and $E = E_{AB}$ yields a bijection

$$\mathrm{PGL}_2(\mathbb{Q}) \Big\backslash V_{AB}(\mathbb{Q})^{\mathrm{ls}} \longleftrightarrow \mathrm{Sel}_2(E_{AB}). \tag{10}$$

Which quartic forms on the left side correspond to the identity in $\mathrm{Sel}_2(E_{AB})$? Those with a linear factor over $\mathbb{Q}$.

Remark 3.3. — Similarly, $\mathrm{Sel}_3(E_{AB})$ can be related to $\mathrm{PGL}_3(\mathbb{Q})$-orbits of ternary cubic forms; this is what is used to prove Theorem 1.3.

4. PROOF OF THE THEOREM ON 2-SELMER GROUPS

Our goal is to sketch the proof of Theorem 1.2. For lack of space, our presentation will necessarily omit many details, so the actual proof is more difficult than we might make it seem. Also, in contrast to [BS15a], we will phrase the proof in adelic terms. This has advantages and disadvantages as far as exposition is concerned, but does not really change any of the key arguments.

4.1. Strategy of the proof

For $X \in \mathbb{R}$, define

$$\begin{aligned} \mathcal{S}(\mathbb{Z})_{<X} &:= \left\{ (A,B) \in \mathbb{Z}^2 : \Delta \neq 0,\ (A,B) \text{ is minimal and } H(A,B) < X \right\} \\ V(\mathbb{Q})^{\mathrm{ls}}_{<X} &:= \text{the subset of } V(\mathbb{Q})^{\mathrm{ls}} \text{ mapping into } \mathcal{S}(\mathbb{Z})_{<X}. \end{aligned} \tag{11}$$

Summing the sizes of the sets in (10) over $(A,B) \in \mathcal{S}(\mathbb{Z})_{<X}$ yields

$$\# \left(\mathrm{PGL}_2(\mathbb{Q}) \Big\backslash V(\mathbb{Q})^{\mathrm{ls}}_{<X} \right) = \sum_{E \in \mathscr{E}_{<X}} \# \mathrm{Sel}_2(E). \tag{12}$$

From now on, we forget about Selmer groups and estimate the left side of (12).

If our job were to estimate the number of integral points in a region $\Omega \subset \mathbb{R}^n$, we would compute the volume of Ω and argue that it is a good estimate provided that the shape of Ω is reasonable. But according to (12), we need to count (orbits of) *rational*

points. So instead of viewing $\mathbb{Z}$ as a lattice in $\mathbb{R}$, we view $\mathbb{Q}$ as a lattice in the ring of adeles

$$\mathbf{A} := \left\{ (x_p) \in \prod_{p \le \infty} \mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for all but finitely many } p \right\}.$$

How do we define an adelic region $V(\mathbf{A})^{\mathrm{ls}}_{<X}$ whose set of rational points is $V(\mathbb{Q})^{\mathrm{ls}}_{<X}$? Inspired by (11), we define

$$\begin{aligned}
\mathcal{S}(\mathbb{R})_{<X} &:= \{ (A,B) \in \mathcal{S}'(\mathbb{R}) : H(A,B) < X \} \\
\mathcal{S}(\mathbb{Z}_p)^{\min} &:= \big((\mathbb{Z}_p \times \mathbb{Z}_p) - (p^4\mathbb{Z}_p \times p^6\mathbb{Z}_p) \big) - (\text{zeros of } \Delta) \\
\mathcal{S}(\mathbf{A})_{<X} &:= \mathcal{S}(\mathbb{R})_{<X} \times \prod_{\text{finite } p} \mathcal{S}(\mathbb{Z}_p)^{\min} \\
V(\mathbb{Q}_p)^{\mathrm{ls}} &:= \{ f \in V(\mathbb{Q}_p) : \Delta \neq 0 \text{ and } z^2 = f(x,y) \text{ has a } \mathbb{Q}_p\text{-point} \} \\
V(\mathbf{A})^{\mathrm{ls}} &:= V(\mathbf{A}) \cap \prod_{p \le \infty} V(\mathbb{Q}_p)^{\mathrm{ls}} \\
V(\mathbf{A})^{\mathrm{ls}}_{<X} &:= \text{the subset of } V(\mathbf{A})^{\mathrm{ls}} \text{ mapping into } \mathcal{S}(\mathbf{A})_{<X}.
\end{aligned}$$

One might expect the rest of the proof to proceed as follows:

1. Define an adelic measure on $\mathrm{PGL}_2(\mathbb{Q}) \backslash V(\mathbf{A})^{\mathrm{ls}}_{<X}$ and compute its volume.
2. Show that $\#\left(\mathrm{PGL}_2(\mathbb{Q}) \backslash V(\mathbb{Q})^{\mathrm{ls}}_{<X} \right)$ is well approximated by that adelic volume.

But statement 2 turns out to be false! It will be salvaged by excluding the quartic forms with a linear factor, i.e., those corresponding to the identity in a Selmer group. In other words, it is $\sum_{E \in \mathscr{E}_{<X}} (\#\,\mathrm{Sel}_2(E) - 1)$ that is approximated by the adelic volume.

4.2. Computing the adelic volume

The space $\mathbb{Q}_p$ has the usual Haar measure μ_p (Lebesgue measure if $p = \infty$). The adelic measure on $\mathbf{A}$ is the product of these. The product $\prod_{\text{finite } p} \mu_p(\mathcal{S}(\mathbb{Z}_p)^{\min})$ converges, so $\mathcal{S}(\mathbf{A})_{<X}$ inherits an adelic measure from $\mathbf{A}^2$. In fact, $\mu_\infty(\mathcal{S}(\mathbb{R})_{<X}) = 4 \cdot 4^{-1/3} 27^{-1/2} X^{5/6}$ (area of a rectangle) and $\mu_p(\mathcal{S}(\mathbb{Z}_p)^{\min}) = 1 - p^{-4}p^{-6}$, and the product is $\mu(\mathcal{S}(\mathbf{A})_{<X}) = cX^{5/6}$, where $c := 2^{4/3}3^{-3/2}\zeta(10)^{-1}$.

Although $V(\mathbf{A})^{\mathrm{ls}} \subset \mathbf{A}^5$ is a restricted direct product and not a direct product, it is a union of direct products that can be given an adelic measure as above. The action of $\mathrm{PGL}_2(\mathbb{Q})$ is measure-preserving, so the quotient $\mathrm{PGL}_2(\mathbb{Q}) \backslash V(\mathbf{A})^{\mathrm{ls}}_{<X}$ inherits the measure.

Let $\mathcal{E} \to \mathcal{S}'$ be the universal elliptic curve in short Weierstrass form. Let W be the moduli space of pairs (f, P) where f is a quartic form of nonzero discriminant and P is a point on $z^2 = f(x,y)$. The group scheme $\mathrm{PGL}_{2,\mathcal{S}'}$ acts on W (transforming both f and P). The forgetful $\mathcal{S}'$-morphism $F\colon W \to V'$ is an $\mathcal{E}$-torsor, and is $\mathrm{PGL}_{2,\mathcal{S}'}$-equivariant. In fact, $W \to \mathcal{S}'$ is a homogeneous space under $\mathcal{E} \underset{\mathcal{S}'}{\times} \mathrm{PGL}_{2,\mathcal{S}'}$. The stabilizer of $(x^3y + Axy^3 + By^4, (1:0:0))$ is $\mathcal{E}[2]$ embedded diagonally (see Remark 3.2), so $W \simeq$

$\left(\mathcal{E} \underset{\mathcal{S}'}{\times} \mathrm{PGL}_{2,\mathcal{S}'}\right) \Big/ \mathcal{E}[2]$. The quotient $\mathcal{S}'$-morphism $q\colon W \to \mathrm{PGL}_{2,\mathcal{S}'}\backslash W \simeq \mathcal{E}/\mathcal{E}[2] \simeq \mathcal{E}$ is a PGL_2-torsor, and it turns out to admit a rational section.

We obtain a commutative (but not cartesian) diagram

$$\begin{array}{ccc} W & \xrightarrow{q} & \mathcal{E} \\ {\scriptstyle F}\downarrow & & \downarrow \\ V' & \longrightarrow & \mathcal{S}'. \end{array}$$

Let $W(\mathbf{A})_{<X}$ be the subset of $W\left(\prod_{p\le\infty}\mathbb{Q}_p\right)$ (not of $W(\mathbf{A})$!) mapping into $V(\mathbf{A})^{\mathrm{ls}}_{<X}$. Let $\mathcal{E}(\mathbf{A})_{<X}$ be the subset of $\mathcal{E}\left(\prod_{p\le\infty}\mathbb{Q}_p\right)$ mapping into $\mathcal{S}(\mathbf{A})_{<X}$.

We define the measure of a subset of $W(\mathbf{A})_{<X}$ by integrating over $V(\mathbf{A})^{\mathrm{ls}}_{<X}$ the measure of the fibers of F, where each full fiber, an $E_{AB}(\mathbf{A})$-torsor, is assigned the mass 1 Haar measure. Define a measure on $\mathcal{E}(\mathbf{A})_{<X}$ in the same way by integrating over $\mathcal{S}(\mathbf{A})_{<X}$. It turns out that the fibers of $W(\mathbf{A})_{<X} \xrightarrow{q} \mathcal{E}(\mathbf{A})_{<X}$ outside a measure-zero subset are $\mathrm{PGL}_2(\mathbf{A})$-torsors, and that the Tamagawa measure μ_{Tam} on these torsors is compatible with the measures on $W(\mathbf{A})_{<X}$ and $\mathcal{E}(\mathbf{A})_{<X}$.

Now consider

$$\begin{array}{ccc} \mathrm{PGL}_2(\mathbb{Q})\backslash W(\mathbf{A})_{<X} & \xrightarrow{q} & \mathcal{E}(\mathbf{A})_{<X} \\ {\scriptstyle F}\downarrow & & \downarrow \\ \mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbf{A})^{\mathrm{ls}}_{<X} & \longrightarrow & \mathcal{S}(\mathbf{A})_{<X}. \end{array}$$

Working counterclockwise from $\mathcal{S}(\mathbf{A})_{<X}$, we have

$$\begin{aligned} \mu(\mathcal{E}(\mathbf{A})_{<X}) &= \mu(\mathcal{S}(\mathbf{A})_{<X}) \\ \mu\left(\mathrm{PGL}_2(\mathbb{Q})\backslash W(\mathbf{A})_{<X}\right) &= \mu_{\mathrm{Tam}}\left(\mathrm{PGL}_2(\mathbf{A})\Big/\mathrm{PGL}_2(\mathbb{Q})\right)\ \ \mu(\mathcal{E}(\mathbf{A})_{<X}) \\ \mu\left(\mathrm{PGL}_2(\mathbb{Q})\backslash W(\mathbf{A})_{<X}\right) &= \mu\left(\mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbf{A})^{\mathrm{ls}}_{<X}\right), \end{aligned}$$

and the **Tamagawa number**

$$\tau(\mathrm{PGL}_2) := \mu_{\mathrm{Tam}}\left(\mathrm{PGL}_2(\mathbf{A})\Big/\mathrm{PGL}_2(\mathbb{Q})\right)$$

is known to be 2, so

$$\mu\left(\mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbf{A})^{\mathrm{ls}}_{<X}\right) = 2\,\mu(\mathcal{S}(\mathbf{A})_{<X}) = 2cX^{5/6}. \tag{13}$$

4.3. Counting rational points in adelic regions

Proposition 4.1 (Denominator for Average($\#\,\mathrm{Sel}_2 - 1$)). — *As* $X \to \infty$,

$$\sum_{E\in\mathscr{E}_{<X}} 1 = \#\mathcal{S}(\mathbb{Z})_{<X} = (1+o(1))\,\mu\left(\mathcal{S}(\mathbf{A})_{<X}\right).$$

Proof. — The first equality is trivial. Now, $\#\mathcal{S}(\mathbb{Z})_{<X}$ is the number of integral points (A, B) in a large rectangle that remain after sieving out those satisfying $p^4|A$ and $p^6|B$ for some prime p and discarding those with $4A^3+27B^2=0$. The sieving is elementary, and can be handled either by a Möbius inversion argument [Bru92, Lemma 4.3], or by sieving at the first few primes with the Chinese remainder theorem and then arguing that the number of points removed by sieving at all the remaining large primes is negligible. This leaves $(1+o(1))cX^{5/6}$ points. The (A, B) with $4A^3+27B^2=0$ have the form $(-3n^2, 2n^3)$; there are only $O(X^{1/6})$ such points of height up to X, so discarding them does not affect the asymptotics. (For related calculations over number fields, see [Bek04].) □

Let $V(\mathbb{Q})^{\mathrm{ls},\,\cancel{\text{linear}}}_{<X}$ be the set of $f \in V(\mathbb{Q})^{\mathrm{ls}}_{<X}$ that have no rational linear factor. Most of the rest of the section will be devoted to the proof of the following:

Proposition 4.2 (Numerator for Average($\#\operatorname{Sel}_2 -1$)). — *As* $X \to \infty$,

$$\sum_{E\in\mathscr{E}_{<X}} (\#\operatorname{Sel}_2(E)-1) = \#\left(\mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbb{Q})^{\mathrm{ls},\,\cancel{\text{linear}}}_{<X}\right)$$
$$= (1+o(1))\,\mu\left(\mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbf{A})^{\mathrm{ls}}_{<X}\right).$$

Ideally, we could choose a fundamental domain $\mathcal{F}$ for the action of $\mathrm{PGL}_2(\mathbb{Q})$ on $V(\mathbf{A})^{\mathrm{ls}}_{<X}$ and simply count the rational points of $V(\mathbb{Q})^{\mathrm{ls},\,\cancel{\text{linear}}}_{<X}$ in it. In an attempt to construct such an $\mathcal{F}$ we use the theory of integral models of binary quartic forms.

Lemma 4.3 (Existence of integral models [BSD63, Lemmas 3, 4, and 5])
Any locally solvable quartic form $f \in \mathbb{Q}[x, y]$ *with* $A \in 2^4\mathbb{Z}$ *and* $B \in 2^6\mathbb{Z}$ *is* $\mathrm{PGL}_2(\mathbb{Q})$*-equivalent to a quartic form in* $\mathbb{Z}[x, y]$.

To avoid some inconsequential technicalities, we ignore the 2^4 and 2^6 in the rest of our exposition. We also ignore the points in $V(\mathbb{Q})^{\mathrm{ls},\,\cancel{\text{linear}}}_{<X}$ with a nontrivial stabilizer in $\mathrm{PGL}_2(\mathbb{Q})$: one can show that the contribution from these is negligible.

Define $\widehat{\mathbb{Z}} := \prod_{\text{finite } p}\mathbb{Z}_p$, and define $V(\widehat{\mathbb{Z}})^{\mathrm{ls}}$ in the obvious way. The proof of Lemma 4.3 shows also that every quartic form in $V(\mathbf{A})^{\mathrm{ls}}_{<X}$ is $\mathrm{PGL}_2(\mathbb{Q})$-equivalent to one in $V(\mathbb{R})^{\mathrm{ls}}_{<X} \times V(\widehat{\mathbb{Z}})^{\mathrm{ls}}$ (if we ignore 2^4 and 2^6).

An explicit fundamental domain $\mathcal{F}^{\mathbb{R}}$ for $\mathrm{PGL}_2(\mathbb{Z})\backslash V(\mathbb{R})^{\mathrm{ls}}$ can be obtained by combining Gauss's fundamental domain for $\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})$ with an easily described fundamental domain for $\mathrm{PGL}_2(\mathbb{R})\backslash V(\mathbb{R})^{\mathrm{ls}}$. By the previous paragraph, if $\mathcal{F}^{\mathbb{R}}_{<X} := \{f \in \mathcal{F}^{\mathbb{R}} : H(f) < X\}$, then every quartic form in $V(\mathbf{A})^{\mathrm{ls}}_{<X}$ is $\mathrm{PGL}_2(\mathbb{Q})$-equivalent to one in the subset $\mathcal{F} := \mathcal{F}^{\mathbb{R}}_{<X} \times V(\widehat{\mathbb{Z}})^{\mathrm{ls}}$ (if we ignore 2^4 and 2^6). Rational points in $\mathcal{F}$ now are integral points in $\mathcal{F}^{\mathbb{R}}_{<X}$ satisfying local solvability.

There are two problems with $\mathcal{F}$:

1. The region $\mathcal{F}^{\mathbb{R}}_{<X}$ has a narrow cusp stretching to infinity, which makes it hard to approximate its number of integral points by its volume.

2. The set $\mathcal{F}$ is not a fundamental domain! (Although integral points in $\mathcal{F}^{\mathbb{R}}_{<X}$ cannot be $\mathrm{PGL}_2(\mathbb{Z})$-equivalent, they can still be $\mathrm{PGL}_2(\mathbb{Q})$-equivalent. This phenomenon can happen only for quartic forms whose discriminant is divisible by p^2 for some prime p. For instance,

$$p^2x^4 + px^3y + x^2y^2 + xy^3 + y^4 \quad \text{and} \quad x^4 + x^3y + x^2y^2 + pxy^3 + p^2y^4$$

are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent.)

Problem 1 is solved by an idea from [Bha05, §2.2], namely to average over a "compact continuum" of $\mathrm{PGL}_2(\mathbb{R})$-translates of $\mathcal{F}^{\mathbb{R}}_{<X}$. This fattens the cusp enough that the volume estimate applies to the "main body" obtained by cutting off most of the cusp. It turns out that the severed part contains a disproportionately large number of integral points, but they are all from the quartic forms with a rational linear factor; on the other hand, the main body contains few quartic forms with a rational linear factor; this explains why we exclude them to obtain a count approximated by a volume.

Problem 2 is more serious. One solution might be to find some way to select one $\mathrm{PGL}_2(\mathbb{Z})$-orbit of integral quartic forms within each $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class. A more elegant solution is to select them all, but to weight each one by $1/n$ where n is the number of possibilities. By an argument involving the class number of PGL_2 being 1, this weight turns out to be expressible as a product over all primes p of local weights defined analogously in terms of the number of $\mathrm{PGL}_2(\mathbb{Z}_p)$-orbits of quartic form over $\mathbb{Z}_p$ within a $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence class. (Strictly speaking, one also needs to take into account the orders of stabilizers in defining these weights.) The situation is now similar to that in the proof of Proposition 4.1, in which we counted integral points with a weight that was 1 or 0 according to whether it was minimal (at every prime p) or not. If we approximate the actual weights by the product of the local weights at the first few primes, then the weighted count of integral points can be approximated by a weighted volume. It remains to show that the number of points at which the actual weight differs from the approximate weight is negligible. The local weight turns out to be 1 whenever $p^2 \nmid \Delta$, so it suffices to sum the following bound over all primes p beyond a large number:

Lemma 4.4 ([BS15a, Proposition 3.16]). — *The number of* $\mathrm{PGL}_2(\mathbb{Z})$*-orbits of integral quartic forms of height less than* X *such that* $\Delta \neq 0$ *and* $p^2|\Delta$ *is* $O(p^{-3/2}X^{5/6})$.

The proof of Lemma 4.4 is the trickiest part of the whole argument. The observation that Δ is a polynomial in a, b, c, d, e is enough to prove Lemma 4.4 for primes p up to a small fractional power of X, but it is not known for an arbitrary polynomial how to obtain suitable bounds on the number of values divisible by the square of a *larger* prime [Gra98, Poo03]. Bhargava and Shankar resolve the difficulty in a surprising way: using [Woo09, Theorem 4.1.1], they identify the set of quartic forms with the set of quartic rings with monogenized cubic resolvent, which admits an (at most 12)-to-1 map to the much larger set of quartic rings with cubic resolvent, which is in bijection with

$(\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}))$-orbits of pairs of ternary quadratic forms [Bha04, Theorem 1]. Then they do the counting in this larger set, whose size was calculated in [Bha05, Theorem 7].

This concludes the sketch of the proof of Proposition 4.2.

Remark 4.5. — The role of Lemma 4.4 is to ensure that we are not *overcounting* orbits. Without Lemma 4.4, we could still deduce $\overline{\text{Average}}(\#\,\mathrm{Sel}_2) \leq 3$.

Remark 4.6. — Calculations related to Lemma 4.4 are used in [BS15a] to compute not only $\text{Average}(\#\,\mathrm{Sel}_2)$, but also other averages, such as the average size of the 2-torsion subgroup of the class group of a maximal cubic order equipped with an element generating it as a ring.

4.4. End of proof

Dividing Proposition 4.2 by Proposition 4.1 and using the volume relation (13) yields

$$\text{Average}(\#\,\mathrm{Sel}_2 - 1) = \tau(\mathrm{PGL}_2) = 2.$$

Add 1.

ACKNOWLEDGEMENTS

I thank Manjul Bhargava for explaining to me many details of his work with Arul Shankar. I thank also Kęstutis Česnavičius, Jean-Louis Colliot-Thélène, John Cremona, Étienne Fouvry, Benedict Gross, Ruthi Hortsch, Jennifer Park, Joseph H. Silverman, Jack Thorne, and Jeanine Van Order for comments. The writing of this article was supported in part by National Science Foundation grant DMS-1069236. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[Bek04] Ebru Bekyel, *The density of elliptic curves having a global minimal Weierstrass equation*, J. Number Theory **109** (2004), no. 1, 41–58, DOI 10.1016/j.jnt.2004.06.003. MR2098475 (2005f:11109)

[Bha04] Manjul Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360. MR2113024 (2005k:11214)

[Bha05] ———, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR2183288

[BS15a] Manjul Bhargava and Arul 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, DOI 10.4007/annals.2015.181.1.3. MR3272925

[BS15b] ———, *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, DOI 10.4007/annals.2015.181.2.4. MR3275847

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin, 1975. MR0376533 (51 #12708)

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25. MR0146143 (26 #3669)

[BSD65] ———, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. MR0179168 (31 #3419)

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR1839918 (2002d:11058)

[Bru92] Armand Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472, DOI 10.1007/BF01232033. MR1176198 (93g:11057)

[BFH90] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, DOI 10.1007/BF01233440. MR1074487 (92a:11058)

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. MR0163915 (29 #1214)

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082 (85j:11144)

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068)

[Cre] ———, *Elliptic curve data*. Available at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html` .

[CFO+08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155, DOI 10.1515/CRELLE.2008.012. MR2384334 (2009g:11067)

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Mosc. Math. J. **2** (2002), no. 2, 281–311. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR1944508 (2003m:11080)

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065)

[DD10] Tim Dokchitser and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426 (2011h:11069)

[Fou93] 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., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 61–84 (French). MR1263524 (95b:11057)

[FP93] Étienne Fouvry and Jacek Pomykała, *Rang des courbes elliptiques et sommes d'exponentielles*, Monatsh. Math. **116** (1993), no. 2, 111–125, DOI 10.1007/BF01404006 (French, with English summary). MR1245858 (94g:11037)

[Gol79] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR564926 (81i:12014)

[Gra98] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009. MR1654759 (99j:11104)

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR833192 (87j:11057)

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195, DOI 10.1007/BF01231285. MR1193603 (93j:11038)

[HB94] ———, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR1292115 (95h:11064)

[HB04] ———, *The average analytic rank of elliptic curves*, Duke Math. J. **122** (2004), no. 3, 591–623, DOI 10.1215/S0012-7094-04-12235-3. MR2057019 (2004m:11084)

[Kan13] Daniel Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory **7** (2013), no. 5, 1253–1279, DOI 10.2140/ant.2013.7.1253. MR3101079

[KS99a] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR2000b:11070

[KS99b] ———, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), no. 1, 1–26, DOI 10.1090/S0273-0979-99-00766-1. MR1640151 (2000f:11114)

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $SH(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671 (Russian); English transl., Math. USSR-Izv. **32** (1989), no. 3, 523–541. MR954295 (89m:11056)

[Kol90] ———, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR1106906 (92g:11109)

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287 (80c:14015)

[Mes82] Jean-François Mestre, *Construction d'une courbe elliptique de rang ≥ 12*, C. R. Acad. Sci. Paris Sér. I Math. **295** (1982), no. 12, 643–644 (French, with English summary). MR688896 (84b:14019)

[Mic95] Philippe Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monatsh. Math. **120** (1995), no. 2, 127–136, DOI 10.1007/BF01585913 (French, with English summary). MR1348365 (96j:11077)

[Mic97] ———, *Le rang de familles de variétés abéliennes*, J. Algebraic Geom. **6** (1997), no. 2, 201–234 (French). MR1489113 (99e:14053)

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192.

[MM91] M. Ram Murty and V. Kumar Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475, DOI 10.2307/2944316. MR1109350 (92e:11050)

[Poi01] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Pures Appl. Math. (5) **7** (1901), 161–234.

[Poo03] Bjorn Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), no. 2, 353–373. MR1980998 (2004d:11094)

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483

[Sil98] Joseph H. Silverman, *The average rank of an algebraic family of elliptic curves*, J. Reine Angew. Math. **504** (1998), 227–236, DOI 10.1515/crll.1998.109. MR1656771 (99m:11066)

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277, DOI 10.1007/s00222-013-0448-1. MR3148103

[Ste] William A. Stein, *Modular forms database*. Available at `http://modular.math.washington.edu/Tables/index.html` .

[SD08] Peter Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526, DOI 10.1017/S0305004108001588. MR2464773 (2010d:11059)

[Waz04] Rania Wazir, *A bound for the average rank of a family of abelian varieties*, Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat. (8) **7** (2004), no. 1, 241–252 (English, with English and Italian summaries). MR2044269 (2004m:11087)

[Won01] Siman Wong, *On the density of elliptic curves*, Compositio Math. **127** (2001), no. 1, 23–54, DOI 10.1023/A:1017514507447. MR1832985 (2002d:11066)

[Woo09] Melanie Eggers Matchett Wood, *Moduli spaces for rings and ideals*, June 2009. Ph.D. thesis, Princeton University.

[You06] Matthew P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. **19** (2006), no. 1, 205–250, DOI 10.1090/S0894-0347-05-00503-5. MR2169047 (2006d:11072)

[Yu05] Gang Yu, *Average size of 2-Selmer groups of elliptic curves. II*, Acta Arith. **117** (2005), no. 1, 1–33, DOI 10.4064/aa117-1-1. MR2110501 (2006b:11054)

[Yu06] ———, *Average size of 2-Selmer groups of elliptic curves. I*, Trans. Amer. Math. Soc. **358** (2006), no. 4, 1563–1584 (electronic), DOI 10.1090/S0002-9947-05-03806-7. MR2186986 (2006j:11080)

Bjorn POONEN

Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307, U.S.A.
E-mail : poonen@math.mit.edu
Web : http://math.mit.edu/~poonen/