352

ASTÉRISQUE

2013

SÉMINAIRE BOURBAKI
VOLUME 2011/2012
EXPOSÉS 1043-1058

(1049) *Average rank of elliptic curves*

Bjorn POONEN

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Janvier 2012
64e année, 2011-2012, no 1049, p. 187 à 204

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 [**37**]. 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 [**33**], but the rank remains a mystery. Already in 1901, H. Poincaré [**39**, 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* $r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(E, s)$ [**8**].

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* $\mathrm{Sel}_n(E)$, 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

(1)

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

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 $a_1, a_2, \dots$ 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 **[6, 14, 15, 44]** 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 $(A', B') = (q^4A, q^6B)$. 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 **[33]** 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 ([**4**, 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 [**4**, 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 **[34]**.

A similar argument leads to

THEOREM 1.3 ([**5**, Theorem 1]). — $\overline{\text{Average}}(\#\,\text{Sel}_3) \leq 4$.

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 Average(r) exists, but Theorems 1.2 and 1.3 yield upper bounds on $\overline{\text{Average}}(r)$:

COROLLARY 1.4 ([**5**, Corollary 2]). — $\overline{\text{Average}}(r) \leq 7/6$.

Proof. — Let $s = \dim \text{Sel}_3$. The injection $E(\mathbb{Q})/3E(\mathbb{Q}) \hookrightarrow \text{Sel}_3(E)$ yields $r \leq s$. Combining this with $6s - 3 \leq 3^s$ bounds r in terms of $\#\,\text{Sel}_3$; 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* $\text{Sel}_{p^\infty}(E)$ fitting in an exact sequence

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

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 $r_{p^\infty} := \text{corank}\,\text{Sel}_{p^\infty}(E)$. Let $s'_p := \dim \text{Sel}_p(E) - \dim E[p](\mathbb{Q})$. 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 [**12**]. By (3), $r_{p^\infty} - r = \text{corank}\,Ш[p^\infty]$, 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,

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

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

THEOREM 1.5 ([**18**, Theorem 1.4]). — *For every elliptic curve E over $\mathbb{Q}$, we have* $r_{p^\infty} \equiv r_{\text{an}} \pmod 2$.