Proc. Int. Cong. of Math. – 2018
Rio de Janeiro, Vol. 2 (417–432)

HEURISTICS FOR THE ARITHMETIC OF ELLIPTIC CURVES

Bjorn Poonen

Abstract

This is an introduction to a probabilistic model for the arithmetic of elliptic curves, a model developed in a series of articles of the author with Bhargava, Kane, Lenstra, Park, Rains, Voight, and Wood. We discuss the theoretical evidence for the model, and we make predictions about elliptic curves based on corresponding theorems proved about the model. In particular, the model suggests that all but finitely many elliptic curves over $\mathbb{Q}$ have rank ≤ 21, which would imply that the rank is uniformly bounded.

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ (see Silverman [2009] for basic definitions). Let $E(\mathbb{Q})$ be the set of rational points on E. The group law on E gives $E(\mathbb{Q})$ the structure of an abelian group, and Mordell [1922] proved that $E(\mathbb{Q})$ is finitely generated; let $\operatorname{rk} E(\mathbb{Q})$ denote its rank. The present survey article, based primarily on articles Poonen and Rains [2012], Bhargava, Kane, Lenstra, Poonen, and Rains [2015], and Park, Poonen, Voight, and Wood [2016], is concerned with the following question:

Question 1.1. Is $\operatorname{rk} E(\mathbb{Q})$ bounded as E varies over all elliptic curves over $\mathbb{Q}$?

Question 1.1 was implicitly asked by Poincaré [1901, p. 173] in 1901, even before $E(\mathbb{Q})$ was known to be finitely generated! Since then, many authors have put forth guesses, and the folklore expectation has flip-flopped at least once; see Poincaré [1950, p. 495, end of footnote (^{3})], Honda [1960, p. 98], Cassels [1966, p. 257], Tate [1974, p. 194], Mestre [1982], Mestre [1986, II.1.1 and II.1.2], Brumer [1992, Section 1], Ulmer [2002, Conjecture 10.5], and Farmer, Gonek, and Hughes [2007, (5.20)], or see Park, Poonen, Voight, and Wood [2016, Section 3.1] for a summary.

The writing of this article was supported in part by National Science Foundation grant DMS-1601946 and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033.
MSC2010: primary 11G05; secondary 11G40, 14G25, 14H52, 14K15.
Keywords: Elliptic curve, rank, Selmer group, Shafarevich–Tate group, abelian variety.

The present survey describes a probabilistic model for the arithmetic of elliptic curves, and presents theorems about the model that suggest that $\operatorname{rk} E(\mathbb{Q}) \le 21$ for all but finitely many elliptic curves E, and hence that $\operatorname{rk} E(\mathbb{Q})$ is bounded. Ours is not the first heuristic for boundedness: there is one by Rubin and Silverberg [2000, Remarks 5.1 and 5.2], for a family of quadratic twists and another by Granville, discussed in Watkins, Donnelly, Elkies, Fisher, Granville, and Rogers [2014, Section 11] and developed further in Watkins [2015]. Interestingly, the latter also suggests a bound of 21.

Modeling ranks directly is challenging because there are few theorems about the distribution of ranks. Also, although there exists extensive computational data that suggests answers to some questions (e.g., Balakrishnan, Ho, Kaplan, Spicer, Stein, and Weigandt [2016]), it seems that far more data would be needed to suggest answers to others. Therefore, instead of modeling ranks in isolation, we model ranks, Selmer groups, and Shafarevich–Tate groups simultaneously, so that we can calibrate and corroborate the model using a diverse collection of known results.

2 The arithmetic of elliptic curves

2.1 Counting elliptic curves by height. Every elliptic curve E over $\mathbb{Q}$ is isomorphic to the projective closure of a unique curve $y^2 = x^3 + Ax + B$ in which A and B are integers with $4A^3 + 27B^2 \ne 0$ (the smoothness condition) such that there is no prime p such that $p^4 | A$ and $p^6 | B$. Let $\mathscr{E}$ be the set of elliptic curves of this form, so $\mathscr{E}$ contains one curve in each isomorphism class. Define the height of $E \in \mathscr{E}$ by

$$\operatorname{ht} E := \max(|4A^3|, |27B^2|).$$

(This definition is specific to the ground field $\mathbb{Q}$, but it has analogues over other number fields.) Define

$$\mathscr{E}_{\le H} := \{E \in \mathscr{E} : \operatorname{ht} E \le H\}.$$

Ignoring constant factors, we have about $H^{1/3}$ integers A with $|4A^3| \le H$, and $H^{1/2}$ integers B with $|27B^2| \le H$. A positive fraction of such pairs (A, B) satisfy the smoothness condition and divisibility conditions, so one should expect $\#\mathscr{E}_{\le H}$ to be about $H^{1/3}H^{1/2} = H^{5/6}$. In fact, an elementary sieve argument [Brumer 1992, Lemma 4.3] proves the following:

Proposition 2.1. *We have*

$$\#\mathscr{E}_{\le H} = (2^{4/3}3^{-3/2}\zeta(10)^{-1} + o(1))\, H^{5/6}$$

as $H \to \infty$.

Define the density of a subset $S \subseteq \mathscr{E}$ as

$$\lim_{H\to\infty} \frac{\#(S \cap \mathscr{E}_{\le H})}{\#\mathscr{E}_{\le H}},$$

if the limit exists. For example, it is a theorem that 100% of elliptic curves E over $\mathbb{Q}$ have no nontrivial rational torsion points; this statement is to be interpreted as saying that the density of the set $S := \{E \in \mathscr{E} : E(\mathbb{Q})_{\text{tors}} = 0\}$ is 1 (even though there do exist E with $E(\mathbb{Q})_{\text{tors}} \neq 0$).

2.2 Elliptic curves over local fields. Our model will be inspired by theorems and conjectures about the arithmetic of elliptic curves over $\mathbb{Q}$. But before studying elliptic curves over $\mathbb{Q}$, we should thoroughly understand elliptic curves over local fields.

Let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ at a place v. There is a natural injective homomorphism $\text{inv}\colon \mathrm{H}^2(\mathbb{Q}_v, \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}$ that is an isomorphism if v is nonarchimedean.

Let E be an elliptic curve over $\mathbb{Q}_v$. Fix $n \ge 1$. Taking Galois cohomology in the exact sequence

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

yields a homomorphism $E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) \to \mathrm{H}^1(\mathbb{Q}_v, E[n])$. Let W_v be its image. If v is a nonarchimedean place not dividing n and E has good reduction, then W_v equals the subgroup of unramified classes in $\mathrm{H}^1(\mathbb{Q}_v, E[n])$ [Poonen and Rains 2012, Proposition 4.13].

The theory of the Heisenberg group [Mumford 1991, pp. 44–46] yields an exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{H} \longrightarrow E[n] \longrightarrow 1,$$

which induces a map of sets

$$q_v\colon \mathrm{H}^1(\mathbb{Q}_v, E[n]) \longrightarrow \mathrm{H}^2(\mathbb{Q}_v, \mathbb{G}_m) \xrightarrow{\text{inv}} \mathbb{Q}/\mathbb{Z}.$$

It turns out that q_v is a quadratic form in the sense that $q_v(x+y) - q_v(x) - q_v(y)$ is bi-additive [Zarhin 1974b, §2]. Moreover, $q_v|_{W_v} = 0$ [O'Neil 2002, Proposition 2.3]. In fact, using Tate local duality one can show that W_v is a maximal isotropic subgroup of $\mathrm{H}^1(\mathbb{Q}_v, E[n])$ with respect to q_v [Poonen and Rains 2012, Proposition 4.11].

2.3 Selmer groups and Shafarevich–Tate groups. Now let E be an elliptic curve over $\mathbb{Q}$. Let $\mathbf{A} = \prod_v'(\mathbb{Q}_v, \mathbb{Z}_v)$ be the adèle ring of $\mathbb{Q}$; here v ranges over nontrivial places of $\mathbb{Q}$, Write $E(\mathbf{A})$ for $\prod_v E(\mathbb{Q}_v)/nE(\mathbb{Q}_v)$, and write $\mathrm{H}^1(\mathbf{A}, E[n])$ for the restricted product

$\prod_v'(\mathrm{H}^1(\mathbb{Q}_v, E[n]), W_v)$. We have a commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E[n]) \\ \downarrow & & \downarrow \beta \\ E(\mathbf{A})/nE(\mathbf{A}) & \xrightarrow{\alpha} & \mathrm{H}^1(\mathbf{A}, E[n]). \end{array}$$

The n-Selmer group is defined by $\mathrm{Sel}_n E := \beta^{-1}(\operatorname{im}\alpha) \subseteq \mathrm{H}^1(\mathbb{Q}, E[n])$. (This is equivalent to the classical definition; we have only replaced $\prod_v \mathrm{H}^1(\mathbb{Q}_v, E[n])$ with a subgroup $\mathrm{H}^1(\mathbf{A}, E[n])$ into which α and β map.) The reason for defining $\mathrm{Sel}_n E$ is that it is a computable finite upper bound for (the image of) $E(\mathbb{Q})/nE(\mathbb{Q})$. On the other hand, the Shafarevich–Tate group is defined by

$$Ш = Ш(E) := \ker\left(\mathrm{H}^1(\mathbb{Q}, E) \to \prod_v \mathrm{H}^1(\mathbb{Q}_v, E)\right).$$

It is a torsion abelian group with an alternating pairing

$$[\ ,\ ]\colon Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$$

defined by Cassels. Conjecturally, Ш is finite; in this case, $[\ ,\ ]$ is nondegenerate and #Ш is a square [Cassels 1962]. The definitions easily yield an exact sequence

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \mathrm{Sel}_n E \longrightarrow Ш[n] \longrightarrow 0, \tag{1}$$

so $Ш[n]$ is measuring the difference between $\mathrm{Sel}_n E$ and the group $E(\mathbb{Q})/nE(\mathbb{Q})$ it is trying to approximate.

Each group in (1) decomposes according to the factorization of n into powers of distinct primes, so let us restrict to the case in which $n = p^e$ for some prime p and nonnegative integer e. Taking the direct limit over e yields an exact sequence

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

of $\mathbb{Z}_p$-modules in which $\mathrm{Sel}_{p^\infty} E := \varinjlim \mathrm{Sel}_{p^e} E$ and $Ш[p^\infty] := \bigcup_{e\geq 0} Ш[p^e]$. Moreover, one can show that if $E(\mathbb{Q})[p] = 0$ (as holds for 100% of curves), then $\mathrm{Sel}_{p^e} E \to (\mathrm{Sel}_{p^\infty} E)[p^e]$ is an isomorphism (cf. Bhargava, Kane, Lenstra, Poonen, and Rains [2015, Proposition 5.9(b)]), so no information about the individual p^e-Selmer groups has been lost in passing to the limit.

2.4 The Selmer group as an intersection of maximal isotropic direct summands. If $\xi = (\xi_v) \in \mathrm{H}^1(\mathbf{A}, E[n])$, then for all but finitely many v we have $\xi_v \in W_v$ and hence $q_v(\xi_v) = 0$, so we may define $Q(\xi) := \sum_v q_v(\xi_v)$. This defines a quadratic form $Q : \mathrm{H}^1(\mathbf{A}, E[n]) \to \mathbb{Q}/\mathbb{Z}$.

Theorem 2.2.

(a) *Each of* $\operatorname{im}\alpha$ *and* $\operatorname{im}\beta$ *is a maximal isotropic subgroup of* $\mathrm{H}^1(\mathbf{A}, E[n])$ *with respect to* Q *[Poonen and Rains 2012, Theorem 4.14(a)].*

(b) *If* n *is prime or* $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *is surjective, then* β *is injective. (See Poonen and Rains [ibid., Proposition 3.3(e)] and Bhargava, Kane, Lenstra, Poonen, and Rains [2015, Proposition 6.1].)*

By definition, $\beta(\mathrm{Sel}_n E) = (\operatorname{im}\alpha) \cap (\operatorname{im}\beta)$. Thus, under either hypothesis in (b), $\mathrm{Sel}_n E$ is isomorphic to an intersection of maximal isotropic subgroups of $\mathrm{H}^1(\mathbf{A}, E[n])$.

Moreover, $\operatorname{im}\alpha$ is a direct summand of $\mathrm{H}^1(\mathbf{A}, E[n])$ [ibid., Corollary 6.8]. It is conjectured that $\operatorname{im}\beta$ is a direct summand as well, at least for asymptotically 100% of elliptic curves over $\mathbb{Q}$ [ibid., Conjecture 6.9], and it could hold for all of them.

2.5 The Birch and Swinnerton-Dyer conjecture. See Wiles [2006] for an introduction to the Birch and Swinnerton-Dyer conjecture more detailed than what we present here, and see Stein and Wuthrich [2013, Section 8] for some more recent advances towards it.

Let $E \in \mathscr{E}$. To E one can associate its L-function $L(E, s)$, a holomorphic function initially defined when $\operatorname{Re} s$ is sufficiently large, but known to extend to a holomorphic function on $\mathbb{C}$ (this is proved using the modularity of E). Just as the Dirichlet analytic class number formula expresses the residue at $s = 1$ of the Dedekind zeta function of a number field k in terms of the arithmetic of k, the Birch and Swinnerton-Dyer conjecture expresses the leading term in the Taylor expansion of $L(E, s)$ around $s = 1$ in terms of the arithmetic of E. We will state it only in the case that $\mathrm{rk}\, E(\mathbb{Q}) = 0$ since that is all that we will need. In addition to the quantities previously associated to E, we need

- the real period Ω, defined as the integral over $E(\mathbb{R})$ of a certain 1-form; and
- the Tamagawa number c_p for each finite prime p, a p-adic volume analogous to the real period.

Also define

$$\text{Ш}_0(E) := \begin{cases} \#\text{Ш}(E), & \text{if } \mathrm{rk}\, E(\mathbb{Q}) = 0; \\ 0, & \text{if } \mathrm{rk}\, E(\mathbb{Q}) > 0. \end{cases}$$

Conjecture 2.3 (The rank 0 part of the Birch and Swinnerton-Dyer conjecture)**.** *If $E \in \mathscr{E}$, then*

$$L(E,1) = \frac{Ш_0\ \Omega\ \prod_p c_p}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}. \tag{2}$$

Remark 2.4. In the case where the rank $r := \mathrm{rk}\, E(\mathbb{Q})$ is greater than 0, Conjecture 2.3 states only that $L(E,1) = 0$, whereas the full Birch and Swinnerton-Dyer conjecture predicts that $\mathrm{ord}_{s=1} L(E,s) = r$ and predicts the leading coefficient in the Taylor expansion of $L(E,s)$ at $s = 1$.

Let $H = \mathrm{ht}\, E$. Following Lang [1983] (see also Goldfeld and Szpiro [1995], de Weger [1998], Hindry [2007], Watkins [2008], and Hindry and Pacheco [2016]), we estimate the typical size of $Ш_0$ by estimating all the other quantities in (2) as $H \to \infty$; see Park, Poonen, Voight, and Wood [2016, Section 6] for details. The upshot is that if we average over E and ignore factors that are $H^{o(1)}$, then (2) simplifies to $1 \sim Ш_0\,\Omega$ and we obtain $Ш_0 \sim \Omega^{-1} \sim H^{1/12}$. More precisely:

- $\prod_p c_p = H^{o(1)}$ [de Weger 1998, Theorem 3], [Hindry 2007, Lemma 3.5], [Watkins 2008, pp. 114–115], [Park, Poonen, Voight, and Wood 2016, Lemma 6.2.1];
- $\#E(\mathbb{Q})_{\mathrm{tors}} \le 16$ [Mazur 1977];
- $\Omega = H^{-1/12+o(1)}$ [Hindry 2007, Lemma 3.7], [Park, Poonen, Voight, and Wood 2016, Corollary 6.1.3]; and
- the Riemann hypothesis for $L(E,s)$ implies that $L(E,1) \le H^{o(1)}$ [Iwaniec and Sarnak 2000, p. 713]. In fact, it is reasonable to expect $\operatorname{Average}_{E \in \mathscr{E}_{\le H}} L(E,1) \asymp 1$. (The symbol $\asymp$ means that the left side is bounded above and below by positive constants times the right side.)

Thus we expect

$$\operatorname*{Average}_{E \in \mathscr{E}_{\le H}} Ш_0(E) = H^{1/12+o(1)} \tag{3}$$

as $H \to \infty$.

3 Modeling elliptic curves over $\mathbb{Q}$

3.1 Modeling the p-Selmer group. According to Theorem 2.2, $\mathrm{Sel}_p E$ is isomorphic to an intersection of maximal isotropic subspaces in an infinite-dimensional quadratic

space over $\mathbb{F}_p$. So one might ask whether one could make sense of choosing maximal isotropic subspaces in an infinite-dimensional quadratic space at random, so that one could intersect two of them to obtain a space whose distribution is conjectured to be that of $\mathrm{Sel}_p E$. This can be done by equipping an infinite-dimensional quadratic space with a locally compact topology [Poonen and Rains 2012, Section 2], but the resulting distribution can be obtained more simply by working within a $2n$-dimensional quadratic space and taking the limit as $n \to \infty$. Now every nondegenerate $2n$-dimensional quadratic space with a maximal isotropic subspace is isomorphic to the quadratic space $V_n = (\mathbb{F}_p^{2n}, Q)$, where Q is the quadratic form

$$Q(x_1, \dots, x_n, y_1, \dots, y_n) := x_1 y_1 + \cdots + x_n y_n.$$

Therefore we conjecture that the distribution of $\dim_{\mathbb{F}_p} \mathrm{Sel}_p E$ as E varies over $\mathscr{E}$ equals the limit as $n \to \infty$ of the distribution of the dimension of the intersection of two maximal isotropic subspaces in V_n chosen uniformly at random from the finitely many possibilities. The limit exists and can be computed explicitly; this yields the formula on the right in the following:

Conjecture 3.1 (Poonen and Rains [ibid., Conjecture 1.1]). *For each $s \geq 0$, the density of $\{E \in \mathscr{E} : \dim_{\mathbb{F}_p} \mathrm{Sel}_p E = s\}$ equals*

$$\prod_{j \geq 0} (1 + p^{-j})^{-1} \prod_{j=1}^{s} \frac{p}{p^j - 1}. \tag{4}$$

Remark 3.2. Let E_d be the elliptic curve $dy^2 = x^3 - x$ over $\mathbb{Q}$. Heath-Brown [1993, 1994] proved that the density of integers d such that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2 E_d - 2 = s$ equals

$$\prod_{j \geq 0} (1 + 2^{-j})^{-1} \prod_{j=1}^{s} \frac{2}{2^j - 1},$$

matching (4) for $p = 2$. (The -2 is there to remove the "causal" contribution to $\dim \mathrm{Sel}_2 E_d$ coming from $E_d(\mathbb{Q})[2]$.) As we have explained, this result is a natural consequence of the theory of Section 2.4, but in fact Heath-Brown's result came first and the theory was reverse engineered from it [Poonen and Rains 2012]! Heath-Brown's result was extended by Swinnerton-Dyer [2008] and Kane [2013] to the family of quadratic twists of any $E \in \mathscr{E}$ with $E[2] \subseteq E(\mathbb{Q})$ and no cyclic 4-isogeny.

3.2 Modeling the p^e-Selmer group. If p is replaced by p^e, then we should replace $\mathbb{F}_p^{2n}$ by $V_n := ((\mathbb{Z}/p^e\mathbb{Z})^{2n}, Q)$. But now there are different types of maximal isotropic subgroups up to isomorphism. For example, if $e = 2$, then $(\mathbb{Z}/p^2\mathbb{Z})^n \times \{0\}^n$ and $(p\mathbb{Z}/p^2\mathbb{Z})^{2n}$

are both maximal isotropic subgroups; of these, only the first is a direct summand of V_n. In what follows, we will use only direct summands, for reasons to be explained at the end of this section.

Conjecture 3.3. *If we intersect two random maximal isotropic direct summands of* $V_n := ((\mathbb{Z}/p^e\mathbb{Z})^{2n}, Q)$ *and take the limit as* $n \to \infty$ *of the resulting distribution, we obtain the distribution of* $\mathrm{Sel}_{p^e} E$ *as* E *varies over* $\mathscr{E}$.

For $m \geq 1$, let $\sigma(m)$ denote the sum of the positive divisors of m. One can prove that the limit as $n \to \infty$ of the average size of the random intersection equals $\sigma(p^e)$, and there is an analogous result for positive integers m not of the form p^e [Bhargava, Kane, Lenstra, Poonen, and Rains 2015, Proposition 5.20]. This suggests the following:

Conjecture 3.4 (Poonen and Rains [2012, Conjecture 1(b)], Bhargava, Kane, Lenstra, Poonen, and Rains [2015, Section 5.7], Bhargava and Shankar [2013a, Conjecture 4])**.** *For each positive integer* m,

$$\operatorname*{Average}_{E \in \mathscr{E}} \#\mathrm{Sel}_m E = \sigma(m).$$

(The average is interpreted as the limit as $H \to \infty$ *of the average over* $\mathscr{E}_{\leq H}$.*)*

One could similarly compute the higher moments of the conjectural distribution; see Poonen and Rains [2012, Proposition 2.22(a)] and Bhargava, Kane, Lenstra, Poonen, and Rains [2015, Section 5.5].

There are several reasons why insisting upon direct summands in Conjecture 3.3 seems right:

- Conjecturally, both of the maximal isotropic subgroups arising in the arithmetic of the elliptic curve *are* direct summands: see the last paragraph of Section 2.4.
- Requiring direct summands is essentially the only way to make the model for $\mathrm{Sel}_{p^e} E$ consistent with the model for $\mathrm{Sel}_p E$, given that $\mathrm{Sel}_p E \simeq (\mathrm{Sel}_{p^e} E)[p]$ for 100% of curves [ibid., Remark 6.12].
- It leads to Conjecture 3.4, which has been proved for $m \leq 5$ [Bhargava and Shankar 2015a,b, 2013a,b].

3.3 Modeling the p^∞-Selmer group and the Shafarevich–Tate group. Choosing a maximal isotropic direct summand of $((\mathbb{Z}/p^e\mathbb{Z})^{2n}, Q)$ compatibly for all e is equivalent to choosing a maximal isotropic direct summand of the quadratic $\mathbb{Z}_p$-module $V_n := (\mathbb{Z}_p^{2n}, Q)$. This observation will lead us to a process that models $\mathrm{Sel}_{p^e} E$ for all e simultaneously, or equivalently, that models $\mathrm{Sel}_{p^\infty} E$ directly. To simplify notation, for any

$\mathbb{Z}_p$-module X, let X' denote $X \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$; if X is a $\mathbb{Z}_p$-submodule of V_n, then X' is a $\mathbb{Z}_p$-submodule of V_n'.

Now choose maximal isotropic direct summands Z and W of V_n with respect to the measure arising from taking the inverse limit over e of the uniform measure on the set of maximal isotropic direct summands of $(\mathbb{Z}/p^e\mathbb{Z})^{2n}$ [Bhargava, Kane, Lenstra, Poonen, and Rains 2015, Sections 2 and 4]; then we conjecture that the limiting distribution of $Z' \cap W'$ as $n \to \infty$ equals the distribution of $\mathrm{Sel}_{p^\infty} E$ as E varies over $\mathscr{E}$. Again, the point is that this limiting distribution is compatible with the previously conjectured distribution for $\mathrm{Sel}_{p^e} E$ for each nonnegative integer e, and the conjecture for $\mathrm{Sel}_{p^e} E$ was based on *theorems* about Selmer groups of elliptic curves (see Section 2.4).

Even better, using the same ingredients, we can model $\mathrm{rk}\, E(\mathbb{Q})$ and $Ш[p^\infty]$ at the same time:

Conjecture 3.5 (Bhargava, Kane, Lenstra, Poonen, and Rains [ibid., Conjecture 1.3])**.** *If we choose maximal isotropic direct summands Z and W of $(\mathbb{Z}_p^{2n}, Q)$ at random as above, and we define*

$$R := (Z \cap W)', \qquad S := Z' \cap W', \qquad T := S/R,$$

then the limit as $n \to \infty$ of the distribution of the exact sequence

$$0 \longrightarrow R \longrightarrow S \longrightarrow T \longrightarrow 0$$

equals the distribution of the sequence

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

as E varies over $\mathscr{E}$.

There are several pieces of indirect evidence for the rank and Ш predictions of Conjecture 3.5:

- Each of R and $E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some nonnegative integer r, called the $\mathbb{Z}_p$-corank of the module.
- The $\mathbb{Z}_p$-corank of R is 0 or 1, with probability $1/2$ each [ibid., Proposition 5.6]. Likewise, a variant of a conjecture of Goldfeld (see Goldfeld [1979, Conjecture B] and Katz and Sarnak [1999a,b]) predicts that $\mathrm{rk}\, E(\mathbb{Q})$ (which equals the $\mathbb{Z}_p$-corank of $E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$) is $0, 1, \geq 2$ with densities $1/2, 1/2, 0$, respectively.
- The group T is finite and carries a nondegenerate alternating pairing with values in $\mathbb{Q}_p/\mathbb{Z}_p$, just as $Ш[p^\infty]$ conjecturally does (the p-part of the Cassels pairing). In particular, $\#T$ is a square.

- [Smith 2017] has proved a result analogous to Conjecture 3.5 for the family of quadratic twists of any $E \in \mathscr{E}$ with $E[2] \subseteq E(\mathbb{Q})$ and no cyclic 4-isogeny.

Further evidence is that there are in fact *three* distributions that have been conjectured to be the distribution of $Ш[p^\infty]$ as E varies over rank r elliptic curves, and these three distributions coincide [Bhargava, Kane, Lenstra, Poonen, and Rains 2015, Theorems 1.6(c) and 1.10(b)]. This is so even in the cases with $r \geq 2$, which conjecturally occur with density 0. For a fixed nonnegative integer r, the three distributions are as follows:

1. A distribution defined by Delaunay [2001, 2007] and Delaunay and Jouhet [2014], who adapted the Cohen–Lenstra heuristics for class groups [Cohen and Lenstra 1984].

2. The limit as $n \to \infty$ of the distribution of $T := (Z' \cap W')/(Z \cap W)'$ when (Z, W) is sampled from the set of pairs of maximal isotropic direct summands of $(\mathbb{Z}_p^{2n}, Q)$ satisfying $\mathrm{rk}_{\mathbb{Z}_p}(Z \cap W) = r$. (This set of pairs is the set of $\mathbb{Z}_p$-points of a scheme of finite type, so it carries a natural measure [Bhargava, Kane, Lenstra, Poonen, and Rains 2015, Sections 2 and 4].)

3. The limit as $n \to \infty$ through integers of the same parity as r of the distribution of $(\mathrm{coker}\, A)_{\mathrm{tors}}$ when A is sampled from the space of matrices in $\mathrm{M}_n(\mathbb{Z}_p)$ satisfying $A^T = -A$ and $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r$; here $\ker A$ and $\mathrm{coker}\, A$ are defined by viewing A as a $\mathbb{Z}_p$-linear homomorphism $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$.

The last of these is inspired by the theorem of Friedman and Washington [1989] that for each odd prime p, the limit as $n \to \infty$ of the distribution $\mathrm{coker}\, A$ for $A \in \mathrm{M}_n(\mathbb{Z}_p)$ chosen at random with respect to Haar measure equals the distribution conjectured by Cohen and Lenstra to be the distribution of the p-primary part of the class group of a varying imaginary quadratic field.

3.4 Modeling the rank of an elliptic curve. In the previous section, we saw in the third construction that conditioning on $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r$ yields the conjectural distribution of $Ш[p^\infty]$ for rank r curves. The simplest possible explanation for this would be that sampling A at random from $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}} := \{A \in \mathrm{M}_n(\mathbb{Z}_p) : A^T = -A\}$ *without* conditioning on $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ caused $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ to be distributed like the rank of an elliptic curve.

What is the distribution of $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$? If n is even, then the locus in $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ defined by $\det A = 0$ is the set of $\mathbb{Z}_p$-points of a hypersurface, which has Haar measure 0, so $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = 0$ with probability 1. If n is odd, however, then $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ cannot be 0, because $n - \mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ is the rank of A, which is even for an alternating matrix. For n odd, it turns out that $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = 1$ with probability 1. If we imagine that n was chosen large and with random parity, then the result is that $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ is 0 or 1, with probability $1/2$ each. This result agrees with the variant of Goldfeld's conjecture mentioned above.

This model cannot, however, distinguish the relative frequencies of curves of various ranks ≥ 2, because in the model the event $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) \geq 2$ occurs with probability 0.

Therefore we propose a refined model in which instead of sampling A from $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$, we sample A from the set $\mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\leq X}$ of matrices in $\mathrm{M}_n(\mathbb{Z})_{\mathrm{alt}}$ with entries bounded by a number X *depending on the height H of the elliptic curve being modeled*, tending to ∞ as $H \to \infty$. This way, for elliptic curves of a given height H, the model predicts a potentially positive but diminishing probability of each rank ≥ 2 (the probability that an integer point in a box lies on a certain subvariety), and we can quantify the rate at which this probability tends to 0 as $H \to \infty$ in order to count curves of height up to H having each given rank. In fact, we let n grow with H as well.

Here, more precisely, is the refined model. To model an elliptic curve E of height H, using functions $\eta(H)$ and $X(H)$ to be specified later, we do the following:

1. Choose n to be an integer of size about $\eta(H)$ of random parity (e.g., we could choose n uniformly at random from $\{\lceil \eta(H) \rceil, \lceil \eta(H) \rceil + 1\}$).

2. Choose $A_E \in \mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\leq X(H)}$ uniformly at random, independently for each E.

3. Define random variables $Ш'_E := (\mathrm{coker}\, A)_{\mathrm{tors}}$ and $\mathrm{rk}'_E := \mathrm{rk}_{\mathbb{Z}}(\ker A)$.

Think of $Ш'_E$ as the "pseudo-Shafarevich–Tate group" of E and rk'_E as the "pseudo-rank" of E; their behavior is intended to model the actual Ш and rank.

To complete the description of the model, we must specify the functions $\eta(H)$ and $X(H)$. We do this by asking "How large is $Ш_0$ on average?", both in the model and in reality. Recall from (3) that we expect

$$\operatorname*{Average}_{E \in \mathscr{E}_{\leq H}} Ш_0(E) = H^{1/12+o(1)}. \tag{5}$$

Define

$$Ш'_{E,0} := \begin{cases} \#Ш'_E, & \text{if } \mathrm{rk}'_E = 0; \\ 0, & \text{if } \mathrm{rk}'_E > 0. \end{cases}$$

Using that the determinant of an $n \times n$ matrix is given by a polynomial of degree n in the entries, we can prove that

$$\operatorname*{Average}_{E \in \mathscr{E}_{\leq H}} Ш'_{E,0} = X(H)^{\eta(H)(1+o(1))}, \tag{6}$$

assuming that $\eta(H)$ does not grow too quickly with H. Comparing (5) and (6) suggests choosing $\eta(H)$ and $X(H)$ so that $X(H)^{\eta(H)} = H^{1/12+o(1)}$. We assume this from now on. It turns out that we will not need to know any more about $\eta(H)$ and $X(H)$ than this.

3.5 Consequences of the model. To see what distribution of ranks is predicted by the refined model, we must calculate the distribution of ranks of alternating matrices whose entries are integers with bounded absolute value; the relevant result, whose proof is adapted from Eskin and Katznelson [1995], is the following:

Theorem 3.6 (cf. Park, Poonen, Voight, and Wood [2016, Theorem 9.1.1])**.** *If $1 \le r \le n$ and $n - r$ is even, and $A \in \mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\le X}$ is chosen uniformly at random, then*

$$\mathrm{Prob}(\mathrm{rk}(\ker A) \ge r) \asymp_n (X^n)^{-(r-1)/2}.$$

(The subscript n on the symbol $\asymp$ means that the implied constants depend on n.)

Theorem 3.6 implies that for fixed $r \ge 1$ and $E \in \mathscr{E}$ of height H,

$$\mathrm{Prob}(\mathrm{rk}'_E \ge r) = (X(H)^{\eta(H)})^{-(r-1)/2+o(1)} = H^{-(r-1)/24+o(1)}. \tag{7}$$

Using this, and the fact $\#\mathscr{E}_{\le H} \asymp H^{5/6} = H^{20/24}$ (Proposition 2.1), we can now sum (7) over $E \in \mathscr{E}_{\le H}$ to prove the following theorem about our model:

Theorem 3.7 (Park, Poonen, Voight, and Wood [ibid., Theorem 7.3.3])**.** *The following hold with probability* 1*:*

$$\begin{aligned}
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E = 0\} &= H^{20/24+o(1)}\\
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E = 1\} &= H^{20/24+o(1)}\\
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E \ge 2\} &= H^{19/24+o(1)}\\
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E \ge 3\} &= H^{18/24+o(1)}\\
&\vdots\\
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E \ge 20\} &= H^{1/24+o(1)}\\
\#\{E \in \mathscr{E}_{\le H} : \mathrm{rk}'_E \ge 21\} &\le H^{o(1)},\\
\#\{E \in \mathscr{E} : \mathrm{rk}'_E > 21\} &\text{ is finite.}
\end{aligned}$$

This suggests the conjecture that the same statements hold for the *actual* ranks of elliptic curves over $\mathbb{Q}$. In particular, we conjecture that $\mathrm{rk}\, E(\mathbb{Q})$ is uniformly bounded, bounded by the maximum of the ranks of the conjecturally finitely many elliptic curves of rank > 21.

Remark 3.8. Elkies [2006] has found infinitely many elliptic curves over $\mathbb{Q}$ of rank ≥ 19, and one of rank ≥ 28; these have remained the records since 2006.

4 Generalizations

4.1 Elliptic curves over global fields. What about elliptic curves over other global fields K? Let $\mathscr{E}_K$ be a set of representatives for the isomorphism classes of elliptic curves over K. Let $B_K := \limsup_{E \in \mathscr{E}_K} \operatorname{rk} E(K)$. For example, the conjecture suggested by Theorem 3.7 predicts that $20 \le B_{\mathbb{Q}} \le 21$.

Theorem 4.1 (Těit and Šafarevič [1967], Ulmer [2002])**.** *If K is a global function field, then $B_K = \infty$.*

Even for number fields, B_K can be arbitrarily large (but maybe still always finite):

Theorem 4.2 (Park, Poonen, Voight, and Wood [2016, Theorem 12.4.2])**.** *There exist number fields K of arbitrarily high degree such that $B_K \ge [K : \mathbb{Q}]$.*

Examples of number fields K for which B_K is large include fields in anticyclotomic towers and certain multiquadratic fields; see Park, Poonen, Voight, and Wood [ibid., Section 12.4].

A naive adaptation of our heuristic (see Park, Poonen, Voight, and Wood [ibid., Sections 12.2 and 12.3]) would suggest $20 \le B_K \le 21$ for every global field K, but Theorems 4.1 and 4.2 contradict this conclusion. Our rationalization of this is that the elliptic curves of high rank in Theorems 4.1 and 4.2 are special in that they are definable over a proper subfield of K, and these special curves exhibit arithmetic phenomena that our model does not take into account. To exclude these curves, let $\mathscr{E}_K^\circ$ be the set of $E \in \mathscr{E}_K$ such that E is not a base change of a curve from a proper subfield, and let $B_K^\circ := \limsup_{E \in \mathscr{E}_K^\circ} \operatorname{rk} E(K)$. It is possible that $B_K^\circ < \infty$ for every global field K.

Remark 4.3. On the other hand, it is not true that $B_K^\circ \le 21$ for all number fields, as we now explain. Shioda [1992] proved that $y^2 = x^3 + t^{360} + 1$ has rank 68 over $\mathbb{C}(t)$. In fact, it has rank 68 also over $K(t)$ for a suitable number field K. For this K, specialization yields infinitely many elliptic curves in $\mathscr{E}_K^\circ$ of rank ≥ 68. Thus $B_K^\circ \ge 68$. See Park, Poonen, Voight, and Wood [2016, Remark 12.3.1] for details.

4.2 Abelian varieties.

Question 4.4. For abelian varieties A over number fields K, is there a bound on $\operatorname{rk} A(K)$ depending only on $\dim A$ and $[K : \mathbb{Q}]$?

By restriction of scalars, we can reduce to the case $K = \mathbb{Q}$ at the expense of increasing the dimension. By "Zarhin's trick" that $A^4 \times (A^\vee)^4$ is principally polarized [Zarhin 1974a], we can reduce to the case that A is principally polarized, again at the expense of

increasing the dimension. For fixed $g \geq 0$, one can write down a family of projective varieties including all g-dimensional principally polarized abelian varieties over $\mathbb{Q}$, probably with each isomorphism class represented infinitely many times. We can assume that each abelian variety A is defined by a system of homogeneous polynomials with integer coefficients, in which the number of variables, the number of polynomials, and their degrees are bounded in terms of g. Define the height of A to be the maximum of the absolute values of the coefficients. Then the number of g-dimensional principally polarized abelian varieties over $\mathbb{Q}$ of height $\leq H$ is bounded by a polynomial in H. If there is a model involving a pseudo-rank rk'_A whose probability of exceeding r gets divided by at least a fixed fractional power of H each time r is incremented by 1, as we had for elliptic curves, then the pseudo-ranks are bounded with probability 1. This might suggest a positive answer to Question 4.4, though the evidence is much flimsier than in the case of elliptic curves.

Acknowledgments. I thank Nicolas Billerey, Serge Cantat, Andrew Granville, Eric Rains, Michael Stoll, and John Voight for comments.

References

Jennifer S. Balakrishnan, Wei Ho, Nathan Kaplan, Simon Spicer, William Stein, and James Weigandt (2016). "Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks". *LMS J. Comput. Math.* 19.suppl. A, pp. 351–370. MR: 3540965 (cit. on p. 418).

Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra Jr., Bjorn Poonen, and Eric Rains (2015). "Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves". *Camb. J. Math.* 3.3, pp. 275–321. MR: 3393023 (cit. on pp. 417, 420, 421, 424–426).

Manjul Bhargava and Arul Shankar (Dec. 27, 2013a). *The average number of elements in the 4-Selmer groups of elliptic curves is 7*. Preprint. arXiv: 1312.7333 (cit. on p. 424).

– (Dec. 30, 2013b). *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 (cit. on p. 424).

– (2015a). "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves". *Ann. of Math. (2)* 181.1, pp. 191–242. MR: 3272925 (cit. on p. 424).

– (2015b). "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". *Ann. of Math. (2)* 181.2, pp. 587–621. MR: 3275847 (cit. on p. 424).

Armand Brumer (1992). "The average rank of elliptic curves. I". *Invent. Math.* 109.3, pp. 445–472. MR: 1176198 (cit. on pp. 417, 418).

J. W. S. Cassels (1962). "Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung". *J. Reine Angew. Math.* 211, pp. 95–112. MR: 0163915 (cit. on p. 420).
– (1966). "Diophantine equations with special reference to elliptic curves". *J. London Math. Soc.* 41, pp. 193–291. MR: 0199150 (cit. on p. 417).
H. Cohen and Hendrik W. Lenstra Jr. (1984). "Heuristics on class groups of number fields". In: *Number theory, Noordwijkerhout 1983*. Vol. 1068. Lecture Notes in Math. Berlin: Springer, pp. 33–62. MR: 0756082 (cit. on p. 426).
Christophe Delaunay (2001). "Heuristics on Tate–Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$". *Experiment. Math.* 10.2, pp. 191–196. MR: 1837670 (cit. on p. 426).
– (2007). "Heuristics on class groups and on Tate–Shafarevich groups: the magic of the Cohen–Lenstra heuristics". In: *Ranks of elliptic curves and random matrix theory*. Vol. 341. London Math. Soc. Lecture Note Ser. Cambridge: Cambridge Univ. Press, pp. 323–340. MR: 2322355 (cit. on p. 426).
Christophe Delaunay and Frédéric Jouhet (2014). "p^ℓ-torsion points in finite abelian groups and combinatorial identities". *Adv. Math.* 258, pp. 13–45. MR: 3190422 (cit. on p. 426).
Noam D. Elkies (May 3, 2006). *$\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc.* Email to the number theory mailing list at NMBRTHRY@LISTSERV.NODAK.EDU (cit. on p. 428).
Alex Eskin and Yonatan R. Katznelson (1995). "Singular symmetric matrices". *Duke Math. J.* 79.2, pp. 515–547. MR: 1344769 (cit. on p. 428).
David W. Farmer, S. M. Gonek, and C. P. Hughes (2007). "The maximum size of L-functions". *J. Reine Angew. Math.* 609, pp. 215–236. MR: 2350784 (cit. on p. 417).
Eduardo Friedman and Lawrence C. Washington (1989). "On the distribution of divisor class groups of curves over a finite field". In: *Théorie des nombres, Quebec 1987*. Berlin: de Gruyter, pp. 227–239. MR: 1024565 (cit. on p. 426).
Dorian Goldfeld (1979). "Conjectures on elliptic curves over quadratic fields". In: *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*. Vol. 751. Lecture Notes in Math. Berlin: Springer, pp. 108–118. MR: 0564926 (cit. on p. 425).
Dorian Goldfeld and Lucien Szpiro (1995). "Bounds for the order of the Tate-Shafarevich group". *Compositio Math.* 97.1-2. Special issue in honour of Frans Oort, pp. 71–87. MR: 1355118 (cit. on p. 422).
D. R. Heath-Brown (1993). "The size of Selmer groups for the congruent number problem". *Invent. Math.* 111.1, pp. 171–195. MR: 1193603 (cit. on p. 423).
– (1994). "The size of Selmer groups for the congruent number problem. II". *Invent. Math.* 118.2. With an appendix by P. Monsky, pp. 331–370. MR: 1292115 (cit. on p. 423).
Marc Hindry (2007). "Why is it difficult to compute the Mordell–Weil group?" In: *Diophantine geometry*. Vol. 4. CRM Series. Ed. Norm., Pisa, pp. 197–219. MR: 2349656 (cit. on p. 422).

Marc Hindry and Amílcar Pacheco (2016). "An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic". *Mosc. Math. J.* 16.1, pp. 45–93. MR: 3470576 (cit. on p. 422).

Taira Honda (1960). "Isogenies, rational points and section points of group varieties". *Japan. J. Math.* 30, pp. 84–101. MR: 0155828 (cit. on p. 417).

H. Iwaniec and P. Sarnak (2000). "Perspectives on the analytic theory of L-functions". *Geom. Funct. Anal.* Special Volume. GAFA 2000 (Tel Aviv, 1999), pp. 705–741. MR: 1826269 (cit. on p. 422).

Daniel M. Kane (2013). "On the ranks of the 2-Selmer groups of twists of a given elliptic curve". *Algebra Number Theory* 7.5, pp. 1253–1279. MR: 3101079 (cit. on p. 423).

Nicholas M. Katz and Peter Sarnak (1999a). *Random matrices, Frobenius eigenvalues, and monodromy*. Vol. 45. American Mathematical Society Colloquium Publications. Amer. Math. Soc., pp. xii+419. MR: 1659828 (cit. on p. 425).

– (1999b). "Zeroes of zeta functions and symmetry". *Bull. Amer. Math. Soc. (N.S.)* 36.1, pp. 1–26. MR: 1640151 (cit. on p. 425).

William E. Lang (1983). "On Enriques surfaces in characteristic p. I". *Math. Ann.* 265.1, pp. 45–65. MR: 0719350 (cit. on p. 422).

B. Mazur (1977). "Modular curves and the Eisenstein ideal". *Inst. Hautes Études Sci. Publ. Math.* 47, 33–186 (1978). MR: 0488287 (cit. on p. 422).

Jean-François Mestre (1982). "Construction d'une courbe elliptique de rang ≥ 12". French, with English summary. *C. R. Acad. Sci. Paris Sér. I Math.* 295.12, pp. 643–644. MR: 0688896 (cit. on p. 417).

– (1986). "Formules explicites et minorations de conducteurs de variétés algébriques". French. *Compositio Math.* 58.2, pp. 209–232. MR: 0844410 (cit. on p. 417).

L. J. Mordell (1922). "On the rational solutions of the indeterminate equations of the third and fourth degrees". *Proc. Cambridge Phil. Soc.* 21, pp. 179–192 (cit. on p. 417).

David Mumford (1991). *Tata lectures on theta. III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Birkhäuser Boston Inc., pp. viii+202. MR: 1116553 (cit. on p. 419).

Catherine O'Neil (2002). "The period-index obstruction for elliptic curves". *J. Number Theory* 95.2. Erratum in *J. Number Theory* 109 (2004), no. 2, 390, pp. 329–339. MR: 1924106 (cit. on p. 419).

Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood (Feb. 3, 2016). *A heuristic for boundedness of ranks of elliptic curves*. Preprint, to appear in *J. Europ. Math. Soc.* arXiv: 1602.01431 (cit. on pp. 417, 422, 428, 429).

H. Poincaré (1901). "Sur les propriétés arithmétiques des courbes algébriques". *J. Pures Appl. Math. (5)* 7, pp. 161–234 (cit. on p. 417).

Henri Poincaré (1950). *Œuvres d'Henri Poincaré*. Vol. 5. Edited by Albert Châtelet. Paris: Gauthier-Villars. MR: 0044457 (cit. on p. 417).

Bjorn Poonen and Eric Rains (2012). "Random maximal isotropic subspaces and Selmer groups". *J. Amer. Math. Soc.* 25.1, pp. 245–269. MR: 2833483 (cit. on pp. 417, 419, 421, 423, 424).

Karl Rubin and Alice Silverberg (2000). "Ranks of elliptic curves in families of quadratic twists". *Experiment. Math.* 9.4, pp. 583–590. MR: 1806293 (cit. on p. 418).

Tetsuji Shioda (1992). "Some remarks on elliptic curves over function fields". *Astérisque* 209. Journées Arithmétiques, 1991 (Geneva), pp. 12, 99–114. MR: 1211006 (cit. on p. 429).

Joseph H. Silverman (2009). *The arithmetic of elliptic curves*. 2nd ed. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, pp. xx+513. MR: 2514094 (cit. on p. 417).

Alexander Smith (June 7, 2017). *2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture*. Preprint. arXiv: 1702.02325 (cit. on p. 426).

William Stein and Christian Wuthrich (2013). "Algorithms for the arithmetic of elliptic curves using Iwasawa theory". *Math. Comp.* 82.283, pp. 1757–1792. MR: 3042584 (cit. on p. 421).

Peter Swinnerton-Dyer (2008). "The effect of twisting on the 2-Selmer group". *Math. Proc. Cambridge Philos. Soc.* 145.3, pp. 513–526. MR: 2464773 (cit. on p. 423).

John T. Tate (1974). "The arithmetic of elliptic curves". *Invent. Math.* 23, pp. 179–206. MR: 0419359 (cit. on p. 417).

D. T. Tĕĭt and I. R. Šafarevič (1967). "The rank of elliptic curves". Russian. *Dokl. Akad. Nauk SSSR* 175, pp. 770–773. MR: 0237508 (cit. on p. 429).

Douglas Ulmer (2002). "Elliptic curves with large rank over function fields". *Ann. of Math. (2)* 155.1, pp. 295–315. MR: 1888802 (cit. on pp. 417, 429).

Mark Watkins (2008). "Some heuristics about elliptic curves". *Experiment. Math.* 17.1, pp. 105–125. arXiv: math/0608766. MR: 2410120 (cit. on p. 422).

– (Aug. 20, 2015). *A discursus on 21 as a bound for ranks of elliptic curves over $\mathbf{Q}$, and sundry related topics*. http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf (cit. on p. 418).

Mark Watkins, Stephen Donnelly, Noam D. Elkies, Tom Fisher, Andrew Granville, and Nicholas F. Rogers (2014). "Ranks of quadratic twists of elliptic curves". English, with English and French summaries. *Publ. math. de Besançon* 2014/2, pp. 63–98. MR: 3381037 (cit. on p. 418).

Benjamin M. M. de Weger (1998). "$A + B = C$ and big Ш's". English. *Quart. J. Math. Oxford Ser. (2)* 49.193, pp. 105–128. MR: 1617347 (cit. on p. 422).

Andrew Wiles (2006). "The Birch and Swinnerton-Dyer conjecture". In: *The millennium prize problems*. Clay Math. Inst., pp. 31–41. MR: 2238272 (cit. on p. 421).

Ju. G. Zarhin (1974a). "A remark on endomorphisms of abelian varieties over function fields of finite characteristic". Russian. *Izv. Akad. Nauk SSSR Ser. Mat.* 38, pp. 471–474. MR: 0354689 (cit. on p. 429).

Ju. G. Zarhin (1974b). “Noncommutative cohomology and Mumford groups”. Russian. *Mat. Zametki* 15, pp. 415–419. MR: 0354612 (cit. on p. 419).

Received 2017-11-30.

Bjorn Poonen
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139-4307
USA
poonen@math.mit.edu