RANKS "CHEAT SHEET"

ALICE SILVERBERG

This is a "cheat sheet", which means that it consists of information packaged in a concise and efficient way so that it can easily be used as a quick reference. The topic is ranks of elliptic curves, mostly over $\mathbb{Q}$.

This is a slightly revised version of the handout I wrote as a supplement to my survey talk "Distributions of Ranks of Elliptic Curves" at MSRI's Connections for Women: Arithmetic Statistics workshop in January of 2011. Updates might continue on my website [36]. I thank the organizers and participants of the MSRI workshop, and I thank the WIN2 organizers for the opportunity to publish this in the WIN2 Proceedings volume.

1. Mordell-Weil group, rank, and Tate-Shafarevich group

An elliptic curve E over a field K is a smooth projective curve that has an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

Discriminant: If E is $y^2 = x^3 + Ax + B$ then

$$\Delta(E) := -16(4A^3 + 27B^2) \neq 0.$$

Mordell-Weil Theorem. *If K is finitely generated over the prime field, then the Mordell-Weil group $E(K)$ is a finitely generated abelian group:*

$$E(K) \cong \mathbb{Z}^{\mathrm{rank}(E(K))} \oplus E(K)_{\mathrm{tors}}$$

with $\mathrm{rank}(E(K)) \in \mathbb{Z}^{\geq 0}$ *and* $E(K)_{\mathrm{tors}}$ *a finite abelian group.*

Tate-Shafarevich group (for E over a number field K)**:**

$$Ш(E/K) := \ker \left[H^1(K, E) \to \prod_v H^1(K_v, E) \right]$$

where $H^1(F, E) := H^1(\mathrm{Gal}(\bar{F}/F), E(\bar{F}))$, and the map is induced from the inclusions $\mathrm{Gal}(\bar{K}_v/K_v) \hookrightarrow \mathrm{Gal}(\bar{K}/K)$.

Tate-Shafarevich Conjecture. $Ш(E/K)$ *is finite.*

This work was supported by the National Science Foundation under grant CNS-0831004. I thank Manjul Bhargava, Noam Elkies, Joseph Silverman, Mark Watkins, and Yuri Zarhin for helpful comments.

2. L-function, analytic rank, and BSD (Birch and Swinnerton-Dyer) Conjecture

Fix $E/\mathbb{Q}$. Below, p will denote primes. Replace E by an isomorphic curve with integer coefficients and $|\Delta(E)|$ minimal and let

$$a_p := p + 1 - \#E(\mathbb{F}_p).$$

Then

$$L(E,s) := \prod_{p \nmid \Delta(E)} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid \Delta(E)} (1 - a_p p^{-s})^{-1}.$$

The product converges for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$.

Theorem 2.1 (Wiles et al. [43, 40, 5])**.** *If $E/\mathbb{Q}$, then $L(E,s)$ has an analytic continuation to $\mathbb{C}$ and a functional equation relating $L(E,s)$ and $L(E,2-s)$. More precisely, let N_E denote the conductor of E and let $\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$. Then*

$$\Lambda(E,s) = w_E \Lambda(E, 2-s) \tag{1}$$

with root number $w_E \in \{\pm 1\}$.

Define

$$\mathrm{rank}_{\mathrm{an}}(E) := \mathrm{ord}_{s=1} L(E,s).$$

BSD I Conjecture. $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathrm{an}}(E)$.

Theorem 2.2 (Kolyvagin, Gross-Zagier, Wiles et al. [27, 28, 20, 43, 40, 5])**.** *If* $\mathrm{rank}_{\mathrm{an}}(E) \leq 1$, *then* $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathrm{an}}(E)$ *and* $Ш(E/\mathbb{Q})$ *is finite.*

Theorem 2.3 (Bhargava-Shankar [4])**.** *A positive proportion of elliptic curves E over $\mathbb{Q}$ satisfy* $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathrm{an}}(E) = 0$, *and thus satisfy BSD I.*

Define

$$\Omega := \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1 x + a_3|} \in \mathbb{R}.$$

For $P = (x,y) \in E(\mathbb{Q})$, write $x = \frac{u}{v}$ with $u, v \in \mathbb{Z}$ in lowest terms, and define:

Naive height:

$$h(P) := \log \max(|u|, |v|), \qquad \hat{h}(O) = 0.$$

Néron-Tate height:

$$\hat{h}(P) := \frac{1}{2} \lim_{n \to \infty} \frac{h(2^n P)}{4^n}, \qquad \hat{h}(O) = 0.$$

Define the **Néron-Tate pairing**, a bilinear form on $E(\mathbb{Q})$, by

$$\langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

With $\{P_1, \ldots, P_r\}$ a $\mathbb{Z}$-basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, define the **regulator**

$$R := \det(\langle P_i, P_j \rangle)_{1 \leq i \leq r, 1 \leq j \leq r}.$$

Since E is projective, $E(\mathbb{Q}_p) = E(\mathbb{Z}_p)$ and one can define:

$$E_0(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) : P \text{ reduces to a non-singular point in } E(\mathbb{F}_p)\}.$$

Tamagawa numbers: Define

$$c_p := \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)).$$

(If E has good reduction at p, then $c_p = 1$.)

BSD II Conjecture.

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{\mathrm{rank}_{\mathrm{an}}(E)}} = \frac{\Omega R \# Ш(E/\mathbb{Q}) \prod_{p|\Delta(E)} c_p}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}.$$

Verification of BSD II for all $E/\mathbb{Q}$ with $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$ and conductor < 5000 was recently completed in [19, 9].

3. (Un)boundedness

Folklore Question. *Are ranks of elliptic curves over $\mathbb{Q}$ unbounded?*

Examples 3.1.

(i) In 2006, Elkies [15] posted an elliptic curve E for which $E(\mathbb{Q}) \cong \mathbb{Z}^r$ with $r \geq 28$.

(ii) The highest rank over $\mathbb{Q}$ that is known exactly is 19, due to Elkies [14] in 2009 (and it has torsion $\mathbb{Z}/2\mathbb{Z}$).

(iii) The highest rank over $\mathbb{Q}$ known in the family $y^2 = x^3 + Dx$ is 14, due to Watkins in 2002 (see the Acknowledgments on p. 331 of [1]).

(iv) The highest rank over $\mathbb{Q}$ known in the family $y^2 = x^3 + k$ is ≥ 15, due to Elkies [16] in 2009.

(v) The highest rank over $\mathbb{Q}$ known in the family $x^3 + y^3 = k$ is 11, due to Elkies & Rogers [17] in 2004.

(vi) See the webpages maintained by Dujella [12, 13] for rank records of elliptic curves over $\mathbb{Q}$ with prescribed torsion.

Theorem 3.2 (Mazur et al. [30, 8, 2, 20])**.** *Given $E/\mathbb{Q}$, there is an infinite tower of number fields $K_1 \subsetneq K_2 \cdots$ such that $|\mathrm{rank}(E(K_i)) - \frac{1}{2}[K_i : \mathbb{Q}]| \leq C$ with C independent of i.*

Definition 3.3. An elliptic curve E over a function field $k(t)$ is *constant* if E is isomorphic over $k(t)$ to an elliptic curve over k, and is *isotrivial* if $j(E) \in k$.

Theorem 3.4 (Tate-Shafarevich [39], Ulmer [41])**.** *Ranks of non-constant elliptic curves over $\mathbb{F}_q(t)$ are unbounded (in both the isotrivial and non-isotrivial cases).*

(Special case of) Lang-Néron Theorem. *If k is a field and E is a non-constant elliptic curve over $k(t)$, then $E(k(t))$ is a finitely generated abelian group.*

Folklore Question. *Are ranks of non-constant elliptic curves over $\mathbb{C}(t)$ unbounded? (Both the isotrivial and non-isotrivial cases are open.)*

Example 3.5 (Shioda [35])**.** Over $\mathbb{C}(t)$, $y^2 = x^3 + t^{360} + 1$ has rank 68.

Silverman Specialization Theorem ([37])**.** *If E_t is a non-constant elliptic curve over $\mathbb{Q}(t)$, then for all but finitely many $s \in \mathbb{Q}$ the specialization map $E_t(\mathbb{Q}(t)) \to E_s(\mathbb{Q})$ is injective, so*

$$\operatorname{rank}(E_s(\mathbb{Q})) \geq \operatorname{rank}(E_t(\mathbb{Q}(t))).$$

Folklore Question. *Are ranks of non-constant elliptic curves over $\mathbb{Q}(t)$ unbounded? (Both the isotrivial and non-isotrivial cases are open.)*

Example 3.6. Elkies [15] constructed a non-isotrivial elliptic curve of rank ≥ 18 over $\mathbb{Q}(t)$.

4. Distribution

Rank Distribution Conjecture. *The elliptic curves over $\mathbb{Q}$ with rank ≥ 2 have density zero (in some appropriate sense), and the rest are evenly split between ranks 0 and 1.*

In all the Bhargava-Shankar results below, the elliptic curves are ordered by height.

Theorem 4.1 (Bhargava-Shankar [4])**.** *At least $\frac{5}{8}$ of elliptic curves over $\mathbb{Q}$ have rank 0 or 1.*

Theorem 4.2 (Bhargava-Shankar [4])**.** *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank 0, and if $Ш(E/\mathbb{Q})$ is finite for all elliptic curves E over $\mathbb{Q}$ then a positive proportion have rank 1.*

Conjecture 4.3 (Watkins [42])**.**

$$\#\{E/\mathbb{Q} \text{ with positive even rank and } |\Delta_{\min}(E)| \leq X\} \sim cX^{19/24}(\log X)^{3/8}.$$

Theorem 4.4 (Mazur-Rubin [31])**.** *For each number field K,*

(i) *there are infinitely many E/K with $E(K) = 0$, and*
(ii) *if $Ш(E/K)$ is finite for all E/K, then there are infinitely many E/K with $E(K) \cong \mathbb{Z}$.*

5. Averages

Folklore Conjecture. *The average rank of elliptic curves over $\mathbb{Q}$ is $\frac{1}{2}$.*

Rank Distribution Conjecture $\implies$ Folklore Conjecture.
In what follows, the upper bounds for averages are upper bounds for the lim sup.

Theorem 5.1 (Bhargava-Shankar, in preparation)**.** *The average rank of elliptic curves over $\mathbb{Q}$ is ≤ 0.99 ([4] gives $\leq 1\frac{1}{6} = 1.1666\ldots$).*

Theorem 5.2 (de Jong [23])**.** *The average rank of elliptic curves over $\mathbb{F}_q(t)$ (ordered by height) is $\leq 1.5 + O(\frac{1}{q})$ (e.g., < 2 if $q \geq 7$). In fact (as pointed out by Poonen), $\leq 1\frac{1}{6} + O(\frac{1}{q})$, and < 1.44 if $q \geq 4$, and < 1.28 if $q \geq 7$.*

6. Parity

Parity Conjecture. $\operatorname{rank}(E) \equiv \operatorname{rank}_{\mathrm{an}}(E) \pmod 2$.

BSD I $\implies$ Parity Conjecture.

Theorem 6.1 (Monsky [32]). *If E is an elliptic curve over $\mathbb{Q}$ and $Ш(E/\mathbb{Q})$ is finite, then the Parity Conjecture holds for E.*

See [11] for results over other number fields.

Equidistribution of Root Numbers Conjecture. *The root numbers w_E from (1) are 1 half the time and -1 half the time.*

Equidistribution of Root Numbers Conjecture + Parity Conjecture $\implies$
the rank is even half the time and odd half the time.

7. Quadratic Twists

Fix $E/\mathbb{Q}$. If $E : y^2 = x^3 + Ax + B$ and $d \in \mathbb{Z}^{\neq 0}$, then the quadratic twist of E by d is

$$E_d : y^2 = x^3 + Ad^2x + Bd^3.$$

Let

$$N_*(X) := \#\{\text{squarefree } d \in \mathbb{Z} : |d| \leq X, \operatorname{rank}(E_d(\mathbb{Q})) \text{ is } *\}.$$

Then

$$N_{\geq 0}(X) \sim \frac{12}{\pi^2} X.$$

Trivial Bound. *For each $E/\mathbb{Q}$ with all its 2-torsion defined over $\mathbb{Q}$, there exists $C_E > 0$ such that for all squarefree $d \in \mathbb{Z}$ with $|d| > 2$,*

$$\operatorname{rank}(E_d(\mathbb{Q})) \leq C_E \frac{\log|d|}{\operatorname{loglog}|d|}.$$

Goldfeld Conjecture ([18]). *The average rank of elliptic curves over $\mathbb{Q}$ in families of quadratic twists is $\frac{1}{2}$.*

Assuming the Parity and Goldfeld Conjectures, then:

$$N_0(X) \sim N_1(X) \sim \frac{6}{\pi^2} X, \qquad N_{\geq 2}(X) = o(X).$$

Theorem 7.1 (Heath-Brown [22]). *Assuming BSD I and the Riemann Hypothesis for L-functions of elliptic curves, then the average rank of elliptic curves over $\mathbb{Q}$ in families of quadratic twists is ≤ 1.5.*

Theorem 7.2 (Heath-Brown [21]). *The average rank of the quadratic twists E_d of $E : y^2 = x^3 - x$ with d odd is $\leq 1.2645\ldots$.*

See [44, 45, 46, 6] for related results.

Conjecture 7.3 (Conrey et al. [7]). *$N_{\geq 2,even}(X) \sim c_E X^{3/4}(\log X)^{b_E}$ with 4 possibilities for b_E, depending on $[\mathbb{Q}(E[2]):\mathbb{Q}]$, and with $0.5 \leq b_E < 1.4$.*

Theorem 7.4 (see [S5] for attributions). *For **some** $E/\mathbb{Q}$:*

$$N_0(X) \gg X,\ N_1(X) \gg X,\ N_{\geq 2}(X) \gg X^{\frac{1}{3}},\ N_{\geq 3}(X) \gg X^{\frac{1}{6}},\ N_{\geq 4}(X) \to \infty.$$

*Assuming the Parity Conjecture: $N_{\geq 1}(X) \geq \frac{6}{\pi^2}X$ for all sufficiently large X and $N_{\geq 2}(X) \gg X^{\frac{1}{2}}$ for **all** $E/\mathbb{Q}$, while for **some** $E/\mathbb{Q}$: $N_{\geq 3}(X) \gg X^{\frac{1}{3}}$, $N_{\geq 4}(X) \gg X^{\frac{1}{6}}$, and $N_{\geq 5}(X) \to \infty$.*

8. Selmer Groups and Selmer Ranks

For E over a number field K, define the **m-Selmer group**:

$$S_m(E/K) := \bigcap_v \mathrm{res}_v^{-1}\left(\kappa_v(E(K_v)/mE(K_v))\right) \subseteq H^1(K, E[m])$$

where the short exact sequence

$$0 \to E[m] \to E(\bar{K}) \xrightarrow{m} E(\bar{K}) \to 0$$

induces

$$\begin{array}{ccccccc}
0 \to & E(K)/mE(K) & \xrightarrow{\kappa} & H^1(K,E[m]) & \xrightarrow{\lambda} & H^1(K,E(\bar{K}))[m] & \to 0 \\
& \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow & \\
0 \to & E(K_v)/mE(K_v) & \xrightarrow{\kappa_v} & H^1(K_v,E[m]) & \xrightarrow{\lambda_v} & H^1(K_v,E(\bar{K}_v))[m] & \to 0
\end{array}$$

with $\kappa(P) := [\sigma \mapsto \sigma(Q) - Q]$ where $2Q = P$.

This induces a short exact sequence of finite abelian groups killed by m:

$$0 \to E(K)/mE(K) \xrightarrow{\kappa} S_m(E/K) \xrightarrow{\lambda} Ш(E/K)[m] \to 0.$$

Define a **"modified" p-Selmer rank**:

$$s_p(E/K) := \dim_{\mathbb{F}_p} S_p(E/K) - \dim_{\mathbb{F}_p} E(K)[p] \in \mathbb{Z}^{\geq 0}.$$

Then

$$s_p(E/K) = \mathrm{rank}(E(K)) + \dim_{\mathbb{F}_p} Ш(E/K)[p] \geq \mathrm{rank}(E(K)).$$

If $Ш(E/K)[p^\infty]$ is finite, then $\dim_{\mathbb{F}_p} Ш(E/K)[p]$ is even, so

$$s_p(E/K) \equiv \mathrm{rank}(E(K)) \pmod 2.$$

Define the **p^∞-Selmer group** $S_{p^\infty}(E/K)$ and **p^∞-Selmer rank** $s_{p^\infty}(E/K)$:

$$S_{p^\infty}(E/K) := \varinjlim S_{p^n}(E/K) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{s_{p^\infty}(E/K)} \oplus (\text{finite abelian } p\text{-group}).$$

There is a short exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to S_{p^\infty}(E/K) \to Ш(E/K)[p^\infty] \to 0.$$

Since $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}(E(K))}$, if $Ш(E/K)[p^\infty]$ is finite then $s_{p^\infty}(E/K) = \mathrm{rank}(E(K))$.

p-Selmer Parity Theorem (Monsky [32], Nekovář [33], Kim [25], Dokchitser-Dokchitser [10]). *For $E/\mathbb{Q}$, $s_{p^\infty}(E/\mathbb{Q}) \equiv \mathrm{rank}_{\mathrm{an}}(E) \pmod 2$.*

Bhargava Conjecture. *For each $n > 1$, and varying $E/\mathbb{Q}$ ordered by height, the average size of $S_n(E/\mathbb{Q})$ is $\sum_{d|n} d$.*

For a proof when $n = 2$ see [3], for $n = 3$ see [4]; $n = 4$ and 5 are work in preparation by Bhargava & Shankar.

Bhargava Conjecture for an infinite sequence of n + Parity Conjecture + Equidistribution of root numbers $\implies$ Rank Distribution Conjecture.

Theorem 8.1 (Mazur-Rubin [31] & Klagsbrun [26]). *For E over a number field K with a real embedding, if $E[2](K) = 0$ and $s \in \mathbb{Z}^{\geq 0}$ then there are infinitely many quadratic twists E_d of E with $s_2(E_d/K) = s$.*

For each prime p, let

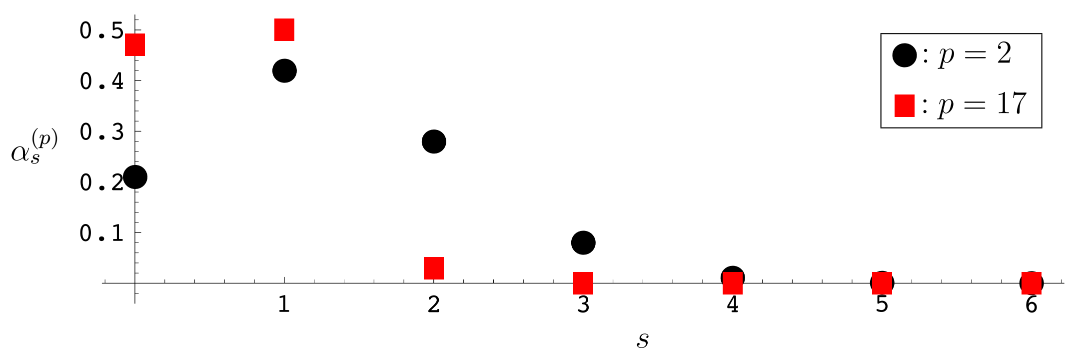
$$\alpha_s^{(p)} := \eta_p \prod_{j=1}^{s} \frac{p}{p^j - 1} \quad \text{where} \quad \eta_p := \prod_{j=0}^{\infty} \frac{1}{1 + \frac{1}{p^j}} = \frac{1}{2} \prod_{j=0}^{\infty} \left(1 - \frac{1}{p^{2j+1}}\right).$$

Then

$$\sum_{s=0}^{\infty} \alpha_s^{(p)} = 1.$$

As $p \to \infty$,

$$\alpha_0^{(p)} \to \frac{1}{2}, \quad \alpha_1^{(p)} \to \frac{1}{2}, \quad \text{and} \quad \alpha_s^{(p)} \to 0 \text{ for all } s \geq 2.$$



For example, when $p = 2$:

$$\alpha_0^{(2)} = \eta_2 \approx 0.21, \qquad \alpha_1^{(2)} = 2\eta_2 \approx 0.42, \qquad \alpha_2^{(2)} = \frac{2\eta_2}{3} \approx 0.28,$$

$$\alpha_3^{(2)} = \frac{4\eta_2}{21} \approx .08, \qquad \alpha_4^{(2)} = \frac{8\eta_2}{315} \approx .01.$$

Poonen-Rains Conjecture ([34]). *Suppose $s \in \mathbb{Z}^{\geq 0}$, p is a prime, and K is a number field. Then the probability that an elliptic curve E over K has $s_p(E/K) = s$ is $\alpha_s^{(p)}$.*

It follows from the p-Selmer Parity Theorem that:
Poonen-Rains Conjecture + Parity Conjecture $\implies$ Rank Distribution Conjecture.

Theorem 8.2 (Kane [24], Swinnerton-Dyer [38]; see also Heath-Brown [21])**.** *Suppose $E/\mathbb{Q}$, $E[2] \subseteq E(\mathbb{Q})$, and E has no cyclic subgroup of order 4 defined over $\mathbb{Q}$. Then:*

(i) *the quadratic twists E_d of E have $s_2(E_d/\mathbb{Q}) = s$ with probability $\alpha_s^{(2)}$, and*
(ii) *the quadratic twists E_d of E have rank 0 with probability $\geq \alpha_0^{(2)} \approx .21$, rank ≤ 1 with probability $\geq \alpha_0^{(2)} + \alpha_1^{(2)} \approx .63$, and, if $Ш(E_d/\mathbb{Q})[2^\infty]$ is finite for all d, rank 1 with probability $\geq \alpha_1^{(2)} \approx 0.42$.*

9. Open Questions

Unless otherwise stated, the following questions are for elliptic curves over $\mathbb{Q}$.

Question 9.1. Determine whether ranks of elliptic curves are bounded or unbounded (in general, and in families) over $\mathbb{Q}$ (or over $\mathbb{C}(t)$, or over $\mathbb{Q}(t)$).

Question 9.2. Determine which non-negative integers can occur as ranks (in general, and in families).

Question 9.3. Find an algorithm guaranteed to determine the rank. (See [29] for an algorithm that depends on conjectures.)

Question 9.4. If r is a non-negative integer, how "often" does r occur as the rank?

Question 9.5. Determine the average rank (suitably defined).

Question 9.6. Answer such questions for elliptic curves over fields other than $\mathbb{Q}$ (e.g., other number fields, $\mathbb{Q}(t)$, etc.).

Question 9.7. Answer such questions for abelian varieties of dimension > 1.

Question 9.8. Find an elliptic curve over $\mathbb{Q}$ that you can prove has analytic rank ≥ 4.

Question 9.9. Find an elliptic curve over $\mathbb{Q}$ of analytic rank > 1 for which you can prove $Ш(E/\mathbb{Q})$ is finite.

Question 9.10. Find a good conjecture for the asymptotic value of $N_3(X)$.

Background Material

[B1] J. H. Silverman, The arithmetic of elliptic curves, Second edition, *Grad. Texts in Math.* **106**, Springer-Verlag, New York, 2009.
[B2] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, *Grad. Texts in Math.* **151**, Springer, New York, 1994.

Surveys

[S1] B. Bektemirov, B. Mazur, W. Stein, M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. **44** (2007), 233-254.

[S2] B. Poonen, *Average ranks of elliptic curves [after Manjul Bhargava and Arul Shankar]*, Séminaire Bourbaki, Janvier 2012, 64ème année, 2011–2012, no. 1049, 17 pp.

[S3] K. Rubin, A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. **39** (2002), 455–474.

[S4] A. Silverberg, *Open questions in arithmetic algebraic geometry*, in Arithmetic algebraic geometry (Park City, UT, 1999), 83–142, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.

[S5] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*, in Ranks of Elliptic Curves and Random Matrix Theory, eds. J. B. Conrey et al., London Math. Soc. Lect. Note Series **341**, Cambridge Univ. Press, 2007, 171–176.

[S6] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

References

[1] J. Aguirre, F. Castaeda, J. C. Peral, *High rank elliptic curves with torsion group* $\mathbb{Z}/(2\mathbb{Z})$, Math. Comp. **73** (2004), 323–331.

[2] M. Bertolini, H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63-74.

[3] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, to appear in Annals of Math., `http://arxiv.org/abs/1006.1002`.

[4] M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, to appear in Annals of Math., `http://arxiv.org/abs/1007.0052`.

[5] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843-939.

[6] S. Chang, *Note on the rank of quadratic twists of Mordell equations*, J. Number Theory **118** (2006), 53-61.

[7] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, in Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, 301–315.

[8] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495-523.

[9] B. Creutz, R. L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, J. Algebra **372** (2012), 673–701.

[10] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Math. **172** (2010), 567-596.

[11] T. Dokchitser, V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39-64.

[12] A. Dujella, *High rank elliptic curves with prescribed torsion*, `http://web.math.pmf.unizg.hr/~duje/tors/tors.html`

[13] A. Dujella, *Infinite families of elliptic curves with high rank and prescribed torsion*, `http://web.math.pmf.unizg.hr/~duje/tors/generic.html`

[14] A. Dujella, *Rank records history, Rank* = 19, `http://web.math.pmf.unizg.hr/~duje/tors/rkeq19.html`

[15] N. Elkies, *Z^28 in E(Q), etc.*, Number Theory Listserv posting, May 3, 2006, `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0605&L=nmbrthry&T=0&F=&S=&P=50`

[16] N. Elkies, *$j = 0$, rank 15; also 3-rank 6 and 7 in real and imaginary quadratic fields*, Number Theory Listserv posting, December 30, 2009, `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0912&L=NMBRTHRY&F=&S=&P=14012`

[17] N. D. Elkies, N. F. Rogers, *Elliptic curves $x^3 + y^3 = k$ of high rank*, in Algorithmic number theory (ANTS-VI), ed. D. Buell, Lecture Notes in Comput. Sci. **3076**, Springer, Berlin, 2004, 184–193.

[18] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), ed. M. B. Nathanson, Lect. Notes in Math. **751**, Springer, Berlin, 1979, 108–118.

[19] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein, C. Tarnită, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. Comp. **78** (2009), 2397-2425.

[20] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[21] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370.

[22] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math. J. **122** (2004), 591-623.

[23] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Mosc. Math. J. **2** (2002), 281-311.

[24] D. Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, to appear in Algebra & Number Theory.

[25] B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. **143** (2007), 47-72.

[26] Z. Klagsbrun, *Selmer ranks of quadratic twists of elliptic curves*, PhD thesis, University of California, Irvine, 2011.

[27] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{Ш}(E, \mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671 (= Math. USSR – Izvestija **32** (1989), no. 3, 523–541).

[28] V. A. Kolyvagin, *Euler systems*, in The Grothendieck Festschrift (Vol. II), eds. P. Cartier et al., Prog. in Math. **87**, Birkhäuser, Boston (1990), 435–483.

[29] Y. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk **26** (1971), no. 6 (162), 7–71.

[30] B. Mazur, *Modular curves and arithmetic*, in Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 185-211, PWN, Warsaw, 1984.

[31] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541-575.

[32] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), 415-420.

[33] J. Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), 99-104.

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

[35] T. Shioda, *Some remarks on elliptic curves over function fields*, Journées Arithmétiques, 1991 (Geneva), Astérisque **209** (1992), 99–114.

[36] A. Silverberg, updatable website for this cheat sheet, `http://math.uci.edu/~asilverb/connectionstalk.pdf`

[37] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

[38] P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), 513-526.
[39] J. T. Tate, I. R. Šafarevič, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), no. 4, 770–773 (= Soviet Math. Dokl. **8** (1967), no. 4, 917–920).
[40] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[41] D. Ulmer, *Elliptic curves with large rank over function fields*, Annals of Math. **155** (2002), 295-315.
[42] M. Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), 105-125.
[43] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141** (1995), 443–551.
[44] G. Yu, *Average size of 2-Selmer groups of elliptic curves. I*, Trans. Amer. Math. Soc. **358** (2006), 1563-1584.
[45] G. Yu, *Average size of 2-Selmer groups of elliptic curves. II*, Acta Arith. **117** (2005), 1-33.
[46] G. Yu, *On the quadratic twists of a family of elliptic curves*, Mathematika **52** (2005), 139-154.

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: asilverb@math.uci.edu