BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 39, Number 4, Pages 455–474
S 0273-0979(02)00952-7
Article electronically published on July 8, 2002

# RANKS OF ELLIPTIC CURVES

KARL RUBIN AND ALICE SILVERBERG

Abstract. This paper gives a general survey of ranks of elliptic curves over the field of rational numbers. The rank is a measure of the size of the set of rational points. The paper includes discussions of the Birch and Swinnerton-Dyer Conjecture, the Parity Conjecture, ranks in families of quadratic twists, and ways to search for elliptic curves of large rank.

## Introduction

L. J. Mordell began his famous paper [49] with the words "Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."

The history of elliptic curves is a long one, and exciting applications for elliptic curves continue to be discovered. Recently, important and useful applications of elliptic curves have been found to cryptography [29], [48], for factoring large integers [35], and for primality proving [17], [1], [18]. The mathematical theory of elliptic curves was crucial in the proof of Fermat's Last Theorem [76].

It is easy to find the rational points on a line. There is a well-known method for parametrizing the rational points on a conic $C$ in the plane: namely, if $P$ is a rational point on $C$, then every line through $P$ intersects $C$ in $P$ and one other point, and this gives a bijection between the rational points on $C$ and the slopes of the rational lines through $P$, which can be identified with the rational points on the projective line. Thus, it is easy to find the rational points on a plane curve defined by a linear or quadratic equation. Increasing the degree of the polynomial, the next case to consider is that of cubics. This brings us to the case of elliptic curves.

In this paper we give a survey of ranks of elliptic curves over the field of rational numbers. The rank of an elliptic curve is a measure of the size of the set of rational points. In 1901 Henri Poincaré [60] stated that the rank is obviously very important in the classification of rational cubics. The major open questions about elliptic curves today, including the Birch and Swinnerton-Dyer Conjecture, have to do with the rank (see [66]).

Received by the editors January 5, 2002, and, in revised form, February 1, 2002.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11-02, 14G05, 11G40, 14H52.

The authors thank the NSF (grants DMS-9800881 and DMS-9988869), the Alexander von Humboldt Foundation, and the Universität Erlangen-Nürnberg. Silverberg also thanks the NSA (grant MDA904-99-1-0007), MSRI, and AIM.

We begin by giving the basic definitions about elliptic curves over the field of rational numbers, including the definition of the rank. We discuss the Birch and Swinnerton-Dyer Conjecture and the Parity Conjecture, and consider ranks in families of quadratic twists. We give lower bounds for densities of quadratic twists with a given rank, and in the process consider ranks of elliptic curves over the function field $\mathbf{Q}(t)$. We also discuss some ways to search for elliptic curves of large rank.

The authors thank B. Mazur and J.-P. Serre for helpful comments on an earlier version of the paper.

## 1. Elliptic curves over $\mathbf{Q}$

An elliptic curve over the field $\mathbf{Q}$ of rational numbers is a curve $E$ defined by a Weierstraß equation

$$y^2 \;=\; x^3 + ax + b \tag{1}$$

where $a, b \in \mathbf{Z}$ and

$$\Delta \;:=\; -16(4a^3 + 27b^2) \;\neq\; 0.$$

The condition that the discriminant $\Delta$ be nonzero is equivalent to the curve being smooth. It is also equivalent to the cubic $x^3 + ax + b$ having 3 different complex roots.

We can view an elliptic curve $E$ as a curve in projective space $\mathbf{P}^2$, with homogeneous equation $y^2z = x^3 + axz^2 + bz^3$, and one point at "infinity", namely $(0, 1, 0)$. This point $\infty$ is the point where all vertical lines meet. Write

$$E(\mathbf{Q}) \;=\; \{\text{rational solutions } (x, y) \text{ of } y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

**Basic Problem.** Given an elliptic curve $E$, find all of its rational points $E(\mathbf{Q})$.

**Example 1.1.** Let $E$ be the elliptic curve $y^2 = x^3 - x$. We obtain three points on the curve by setting $y = 0$. It is easy to show that these are the only integer-valued points on $E$. It is true, but much more difficult to show, that these are the only rational points on $E$, i.e.,

$$E(\mathbf{Q}) \;=\; \{(0, 0), (1, 0), (-1, 0), \infty\}.$$

This was proved by Fermat using his method of infinite descent (see §§X, XV, XVI in Chapter II of [75]).

Over the complex numbers, a line intersects an elliptic curve in three points (counting multiplicity), and if two of these points are rational then so is the third. One can use this fact to define an addition law on $E(\mathbf{Q})$. Namely, given $P, Q \in E(\mathbf{Q})$, draw the line through $P$ and $Q$. Let $R$ be the third point of intersection of that line with $E$, and define $P + Q$ to be the third point of intersection of $E$ with the (vertical) line through $R$ and $\infty$.

Figure 1 shows (among other things) the graph of the real-valued points on the elliptic curve $y^2 = x^3 - x + 1$, and an example of its addition law.

Concretely, if $E$ is the elliptic curve $y^2 = x^3 + ax + b$, and $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbf{Q})$ with $x_1 \neq x_2$, then

$$P + Q = \left( \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_3 - \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \right).$$

**Theorem 1.2.** *With the above addition law, $E(\mathbf{Q})$ is a commutative group with $\infty$ as the identity element.*

Under this operation, three collinear points on the curve sum to the identity

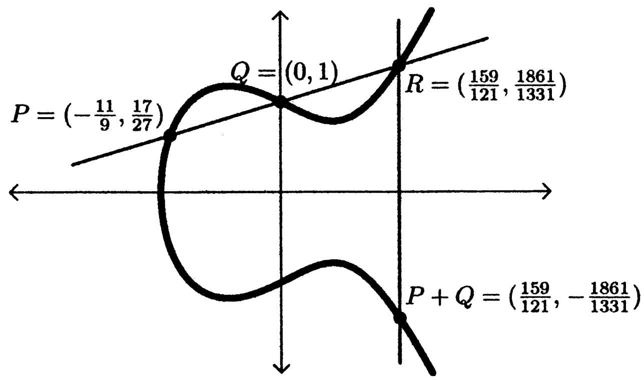


FIGURE 1. $y^2 = x^3 - x + 1$ and its addition law

element. We note that proving associativity is nontrivial.

The following important result was proved by Mordell using Fermat's method of descent.

**Theorem 1.3** (Mordell [49]). *If $E$ is an elliptic curve over $\mathbf{Q}$, then the commutative group $E(\mathbf{Q})$ is finitely generated.*

**Definition 1.4.** By Mordell's theorem we can write

$$E(\mathbf{Q}) \;\cong\; \mathbf{Z}^r \;\oplus\; E(\mathbf{Q})_{\mathrm{tors}}$$

where $r$ is a nonnegative integer and $E(\mathbf{Q})_{\mathrm{tors}}$ is the subgroup of elements of finite order in $E(\mathbf{Q})$. This subgroup is called the *torsion subgroup* of $E(\mathbf{Q})$. The integer $r$ is called the *rank* of $E$ and is written $\mathrm{rank}(E)$.

**Example 1.5.** For the curve $y^2 = x^3 - x$ of Example 1.1,

$$E(\mathbf{Q}) = E(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad \mathrm{rank}(E) = 0.$$

In other words, each of the points $(0,0)$, $(1,0)$, and $(-1,0)$ has order 2 in $E(\mathbf{Q})$.

## 2. Torsion subgroups

The torsion subgroup is "well-understood". First, there is an effective algorithm to determine $E(\mathbf{Q})_{\mathrm{tors}}$ given $E$.

**Theorem 2.1** (Nagell [54], Lutz [36]). *Let $E$ be the elliptic curve $y^2 = x^3 + ax + b$. If $(x, y) \in E(\mathbf{Q})_{\mathrm{tors}}$ and $(x, y) \neq \infty$, then*
(i) *$x, y \in \mathbf{Z}$,*
(ii) *either $y = 0$, or $y^2$ divides $4a^3 + 27b^2$.*

Second, a deep theorem of Mazur states which finite groups can occur as torsion subgroups of elliptic curves.

**Theorem 2.2** (Mazur [39]). *If $E$ is an elliptic curve, then $E(\mathbf{Q})_{\mathrm{tors}}$ is one of the following 15 groups:*
(i) *$\mathbf{Z}/n\mathbf{Z}$, with $1 \le n \le 10$ or $n = 12$,*
(ii) *$\mathbf{Z}/2m\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, with $1 \le m \le 4$.*

Each of the groups in Theorem 2.2 occurs infinitely often as the torsion subgroup of an elliptic curve over $\mathbf{Q}$.

**Example 2.3.** Let $E$ be the curve $y^2 = x^3 - x$ of Example 1.1. By the Nagell-Lutz theorem, the nontrivial rational torsion points $(x, y)$ have $y \in \{0, \pm 1, \pm 2\}$. The only such points are $(-1, 0), (0, 0), (1, 0)$.

**Example 2.4** (See Table 3 of [34])**.** Suppose $t \in \mathbf{Q}$ and $t \neq 0, -1$. Let $E$ be

$$y^2 + (1 - t - t^2)xy + (t^2 + t^3)y = x^3 + (t^2 + t^3)x^2. \tag{2}$$

Then $E$ is an elliptic curve, $(0, 0) \in E(\mathbf{Q})$, and one can check that

$$7 \cdot (0, 0) = \infty.$$

By Mazur's theorem, the subgroup generated by $(0, 0)$ must be all of $E(\mathbf{Q})_{\text{tors}}$, so

$$E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/7\mathbf{Z}.$$

Conversely, one can show that every elliptic curve over $\mathbf{Q}$ with torsion subgroup of order 7 is isomorphic to a curve of the form (2) for some $t \in \mathbf{Q}$.

## 3. Ranks

There are no analogues of Theorems 2.1 or 2.2 for ranks:

- there is no known algorithm guaranteed to determine $\operatorname{rank}(E)$;
- it is not known exactly which integers can occur as the rank of an elliptic curve.

For the first question, there are algorithms for computing both upper bounds and lower bounds for $\operatorname{rank}(E)$; with luck and enough work, they might be equal.[1] For the second, it is not even known if the set of ranks of elliptic curves over $\mathbf{Q}$ is bounded.

Table 1 shows, for certain $r$ between 4 and 24, the date of publication (in print or electronically) of an elliptic curve known to have rank at least $r$.

Table 1. Rank records

| **Rank $\geq$** | **Year** | **Discoverers** |
|---|---|---|
| 3 | 1945 | Billing [2] |
| 4 | 1945 | Wiman [77] |
| 6 | 1974 | Penney & Pomerance [58] |
| 7 | 1975 | Penney & Pomerance [59] |
| 8 | 1977 | Grunewald & Zimmert [21] |
| 9 | 1977 | Brumer & Kramer [6] |
| 12 | 1982 | Mestre [40] |
| 14 | 1986 | Mestre [41] |
| 15 | 1992 | Mestre [44] |
| 17 | 1992 | Nagao [50] |
| 19 | 1992 | Fermigier [13] |
| 20 | 1993 | Nagao [51] |
| 21 | 1994 | Nagao & Kouya [53] |
| 22 | 1997 | Fermigier [14] |
| 23 | 1998 | Martin & McMillen [37] |
| 24 | 2000 | Martin & McMillen [38] |

*Note:* In the early 1950's, Néron [56], [57] showed that there exist elliptic curves with rank $\geq 11$, but his proof did not yield examples.

[1] See p. 193 of [70].

The curve in Table 1 with rank at least 24 is

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x + \\ &504224992484910670010801799168082726759443756222911415116. \end{aligned}$$

(Note that this is not exactly in the form (1), but it can be put in that form by a simple change of variables, at the expense of increasing the size of the coefficients. See (3) below.) The rank is "at least" 24 because Martin and McMillen exhibited 24 independent points in $E(\mathbf{Q})$, but it has not been proved that the rank is exactly 24.

Many of the ideas for finding elliptic curves of high rank are due to Mestre. See §9 below.

## 4. Elliptic curves over arbitrary fields

To fully understand elliptic curves over $\mathbf{Q}$ it is helpful to study elliptic curves over finite fields (see §5) and over function fields (see §8 and §9).

If $F$ is a field, an elliptic curve over $F$ is a nonsingular curve defined by a generalized Weierstraß equation

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

with $a_i \in F$. (Compare with (1). If the characteristic of $F$ is not 2, then we can complete the square in $y$ and change variables to make $a_1 = a_3 = 0$; similarly if the characteristic is not 3, we can suppose that $a_2 = 0$.) Such a curve always has a single point at infinity in projective space $\mathbf{P}^2(F)$.

Conversely, one can show that every nonsingular plane cubic with coefficients in $F$ that has a point in $\mathbf{P}^2(F)$ has an equation of the form (3).

As when $F = \mathbf{Q}$, the set $E(F)$ of $F$-points (including the point at infinity) is an abelian group under the geometric composition law described in §1. For example, the theory of elliptic functions shows that if $E$ is an elliptic curve defined over the complex numbers $\mathbf{C}$, then there are a lattice $L \subset \mathbf{C}$ and an analytic group isomorphism $E(\mathbf{C}) \cong \mathbf{C}/L$. Thus the group $E(\mathbf{C})$ is not finitely generated. However, for certain fields one does have an analogue of Mordell's Theorem (Theorem 1.3):

**Theorem 4.1** (Néron [56])**.** *If $K$ is either $\mathbf{Q}$ or a finite field, $F$ is a finitely generated extension of $K$, and $E$ is an elliptic curve defined over $F$, then the group $E(F)$ is finitely generated.*

## 5. The Birch and Swinnerton-Dyer Conjecture

Fix an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbf{Q}$. For every prime number $p$ not dividing the discriminant $\Delta = 16(4a^3 + 27b^2)$ of $E$, we can reduce $a$ and $b$ modulo $p$ and view $E$ as an elliptic curve over the finite field $\mathbf{F}_p$. Reduction modulo $p$ induces a group homomorphism

$$E(\mathbf{Q}) \longrightarrow E(\mathbf{F}_p).$$

The idea of Birch and Swinnerton-Dyer was that the larger $E(\mathbf{Q})$ is, the larger the $E(\mathbf{F}_p)$'s should be "on average" as $p$ varies. The size of $E(\mathbf{Q})$ can be measured by $\operatorname{rank}(E)$, but how can one measure the average size of the $E(\mathbf{F}_p)$'s?

**Definition 5.1.** For every prime number $p$ not dividing $\Delta$ let

$$\begin{aligned} N_p &= \#E(\mathbf{F}_p) \\ &= 1 + \#\big\{0 \le x, y \le p-1 : y^2 \equiv x^3 + ax + b \pmod{p}\big\}. \end{aligned}$$

**Theorem 5.2** (Hasse [22], [23])**.** *For every prime $p$ not dividing $\Delta$,*

$$p + 1 - 2\sqrt{p} < N_p < p + 1 + 2\sqrt{p}.$$

To test their idea, in the 1950's Birch and Swinnerton-Dyer computed

$$\pi_E(X) := \prod_{p \le X, p \nmid \Delta} \frac{N_p}{p} \tag{4}$$

as $X$ grows, for certain elliptic curves $E$.

Figure 2 shows the behavior of $\pi_{E_d}(X)$ for $X$ up to about $1.5 \times 10^7$ for five different curves $E_d : y^2 = x^3 - d^2x$ (using the first five values of $d$ in Table 2 of §6, so these curves have ranks 0, 1, 2, 3, and 4). The horizontal axis is $\log\log(X)$ and the vertical axis is $\log(\pi_{E_d}(X))$.

From their data Birch and Swinnerton-Dyer [3] were led to conjecture that

$$\pi_E(X) \sim C(\log(X))^{\mathrm{rank}(E)} \tag{5}$$

as $X \to \infty$ for some constant $C$ depending only on $E$. (Note that this relation is consistent with the data in Figure 2 — if the axes were to scale, then the slopes of the lines would be the ranks of the curves.) The function $\pi_E$ does not behave very nicely and therefore is difficult to work with. Birch and Swinnerton-Dyer stated a related conjecture, using the $L$-function of $E$ in place of $\pi_E$.

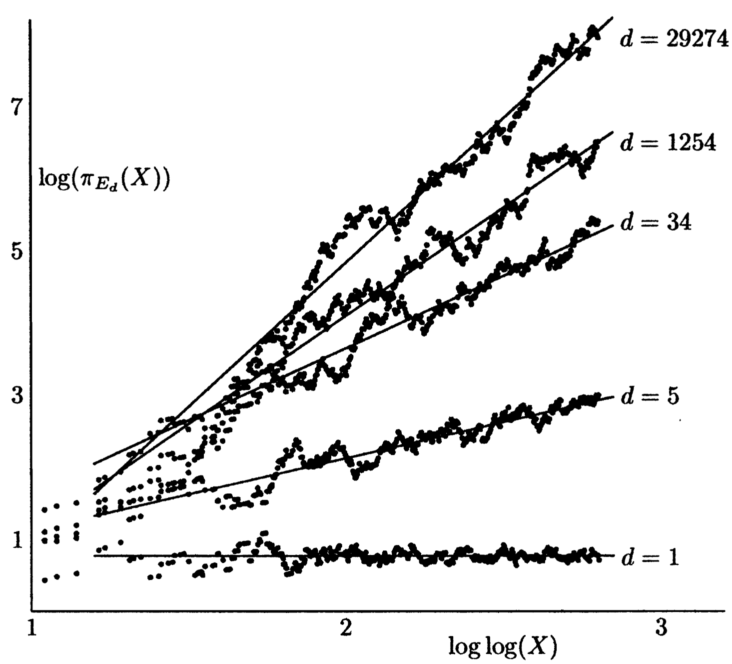


FIGURE 2. Birch and Swinnerton-Dyer data for $y^2 = x^3 - d^2x$

**Definition 5.3.** Define the Hasse-Weil $L$-function of $E$, a function of a complex variable $s$, by

$$L(E,s) \;=\; \prod_{p\nmid\Delta}\Big(1-\frac{1+p-N_p}{p^s}+\frac{p}{p^{2s}}\Big)^{-1}\times\prod_{p\mid\Delta}\ell_p(E,s)^{-1} \tag{6}$$

where $\ell_p(E,s)$ is a certain polynomial in $p^{-s}$ with the property that $\ell_p(E,1)\neq 0$ (see for example p. 196 of [70]).

It follows from Theorem 5.2 that $L(E,s)$ converges absolutely and uniformly on compact subsets of the complex half-plane $\{s\in\mathbf{C} : \mathrm{Re}(s)>3/2\}$. The Shimura-Taniyama Conjecture, recently proved by Breuil, Conrad, Diamond, and Taylor [5] by extending work of Wiles [76], implies the following long-standing conjecture of Hasse and Weil.

**Theorem 5.4** ([76], [72], [5])**.** *$L(E,s)$ has an analytic continuation to all of $\mathbf{C}$ and satisfies a functional equation*

$$\Lambda(s) \;=\; w_E\Lambda(2-s)$$

*where $w_E=\pm1$ and $\Lambda(s) \;=\; N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$ for some positive integer $N$ (depending on $E$).*

See for example p. 196 of [70] for a definition of the conductor $N$ of $E$.

While the Euler product (6) for $L(E,s)$ may not in general converge at $s=1$, *purely formally* evaluating (6) at $s=1$ gives

$$L(E,1) \;\text{“}{=}\text{”}\; \Big(\prod_{p\nmid\Delta}\frac{N_p}{p}\times\prod_{p\mid\Delta}\ell_p(E,1)\Big)^{-1}. \tag{7}$$

Thus, since there are only a finite number of terms in the second product, we can hope that the behavior of $L(E,s)$ near $s=1$ will reflect the average size of the $N_p$: the larger the $N_p$ are, the faster $L(E,s)$ will tend to 0 as $s$ tends to 1. The following quantitative version of this statement is part of the conjecture of Birch and Swinnerton-Dyer.

**Conjecture 5.5** (Birch and Swinnerton-Dyer [4])**.** *For every elliptic curve $E$,*

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

Goldfeld proved the following surprising result, which says in particular that the “purely formal” connection between $\pi_E(X)$ and $L(E,s)$ in (7) is off by a factor of $\sqrt{2}$.

**Theorem 5.6** (Goldfeld [16])**.** *Suppose that $\pi_E(X)\sim C(\log(X))^r$ with constants $C\in\mathbf{R}^+$ and $r\in\mathbf{R}$. Then $r=\mathrm{ord}_{s=1}L(E,s)$ and*

$$\lim_{s\to1}\frac{L(E,s)}{(s-1)^r}=\sqrt{2}e^{r\gamma}C^{-1}\prod_{p\mid\Delta}\ell_p(E,1)^{-1}$$

*where $\gamma$ is Euler's constant. In particular, if $r=0$ then*

$$L(E,1)=\sqrt{2}\Big(\prod_{p\nmid\Delta}\frac{N_p}{p}\times\prod_{p\mid\Delta}\ell_p(E,1)\Big)^{-1}.$$

The lines $\log(C)+r\log\log(X)$ in Figure 2 were calculated using (5), Theorem 5.6, and the full Birch and Swinnerton-Dyer Conjecture to determine $C$ and $r$. (Birch and Swinnerton-Dyer predicted not only the order of vanishing of $L(E,s)$ at $s=1$, but also the first nonvanishing coefficient of its Taylor expansion about $s=1$.)

**Definition 5.7.** With the Birch and Swinnerton-Dyer Conjecture in mind, call the order of vanishing of $L(E,s)$ at $s=1$ the *analytic rank* of $E$ and write

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

The following theorem, a combination of work of Kolyvagin [31], [32], Gross and Zagier [20], and others, is the best result to date in the direction of the Birch and Swinnerton-Dyer Conjecture.

**Theorem 5.8** ([31], [32], [20]). (i) $\mathrm{rank}_{\mathrm{an}}(E)=0 \Rightarrow \mathrm{rank}(E)=0$,
(ii) $\mathrm{rank}_{\mathrm{an}}(E)=1 \Rightarrow \mathrm{rank}(E)=1$.

Assertion (i) can be rephrased as "$L(E,1)\neq 0 \Rightarrow E(\mathbf{Q})$ is finite". The case $\mathrm{rank}_{\mathrm{an}}(E)\geq 2$, except for isolated examples, remains completely open.

There are elliptic curves that can be proved to have analytic ranks 0, 1, 2, and 3 (see [20]). There is no elliptic curve that has been proved to have analytic rank greater than 3.

**Example 5.9.** If $E$ is the curve $y^2=x^3-x$ of Example 1.1, then

$$L(E,1)=0.655514388573029 95\ldots \neq 0.$$

Thus Theorem 5.8(i) shows that (as Fermat said) $E(\mathbf{Q})$ is finite.

The sign $w_E$ in the functional equation (Theorem 5.4) for $L(E,s)$ determines the parity of $\mathrm{rank}_{\mathrm{an}}(E)$:

$$\mathrm{rank}_{\mathrm{an}}(E) \text{ is } \begin{cases} \text{even} & \text{if } w_E=+1, \\ \text{odd} & \text{if } w_E=-1. \end{cases}$$

The Birch and Swinnerton-Dyer Conjecture predicts in particular that $\mathrm{rank}(E)$ and $\mathrm{rank}_{\mathrm{an}}(E)$ have the same parity, so the following is a consequence of the Birch and Swinnerton-Dyer Conjecture.

**Conjecture 5.10** (Parity Conjecture).

$$\mathrm{rank}(E) \textit{ is } \begin{cases} \textit{even} & \textit{if } w_E=+1, \\ \textit{odd} & \textit{if } w_E=-1. \end{cases}$$

To describe recent progress concerning the Parity Conjecture, we need to introduce the Tate-Shafarevich group and the Selmer group. For definitions see pp. 238–239 of [8] or Definitions 4.6.8 and 4.8.1 of [66]. The Tate-Shafarevich group $Ш_E$ is a torsion group that measures the failure of the Hasse Principle for curves that are principal homogeneous spaces for $E$.

**Conjecture 5.11.** (Tate-Shafarevich Conjecture).[2] $Ш_E$ *is finite.*

[2] In his article in the proceedings of the 1962 ICM ([8], pp. 239–240), Cassels writes, "Indeed Tate and Šafarevič have, I believe, independently conjectured that Ш itself is always finite, although, so far as I know, it has not been completely determined in any individual case." In a footnote he adds, "In his lecture Tate denied paternity but adopted the conjecture. In conversation during the Congress Šafarevič expressed strong doubts."

The proof of Theorem 5.8 also proves the following theorem.

**Theorem 5.12** ([31], [32], [20]). *If* $\operatorname{rank}_{\mathrm{an}}(E) \leq 1$*, then* $\text{Ш}_E$ *is finite.*

There is no example known of an elliptic curve with $\operatorname{rank}_{\mathrm{an}}(E) > 1$ for which $\text{Ш}_E$ has been proved to be finite.

Although there is no known general algorithm guaranteed to determine $E(\mathbf{Q})$ or $\text{Ш}_E$, there are effectively computable groups, known as Selmer groups, which combine information about both $E(\mathbf{Q})$ and $\text{Ш}_E$. More precisely, for every natural number $m$, the $m$-Selmer group $S_m(E)$ is a finite group of exponent dividing $m$ that sits in an exact sequence

$$0 \to E(\mathbf{Q})/mE(\mathbf{Q}) \to S_m(E) \to \underset{E}{\text{Ш}}[m] \to 0 \tag{8}$$

where $X[m]$ denotes the kernel of multiplication by $m$ in an abelian group $X$. Thus the Tate-Shafarevich group can also be viewed as an obstruction to effectively computing the rank of $E$: if $p$ is a prime, then (8) and Theorem 1.3 show that

$$\dim_{\mathbf{F}_p} S_p(E) = \operatorname{rank}(E) + \dim_{\mathbf{F}_p} E(\mathbf{Q})[p] + \dim_{\mathbf{F}_p} \underset{E}{\text{Ш}}[p]. \tag{9}$$

In practice the only way to prove upper bounds for the rank of $E$ has been to prove upper bounds for $\#S_m(E)$. For example, Theorems 5.8 and 5.12 follow from the statements

(i) $\operatorname{rank}_{\mathrm{an}}(E) \leq 1 \Rightarrow \operatorname{rank}(E) \geq \operatorname{rank}_{\mathrm{an}}(E)$;
(ii) $\operatorname{rank}_{\mathrm{an}}(E) \leq 1 \Rightarrow \#S_m(E) \leq Cm^{\operatorname{rank}_{\mathrm{an}}(E)}$, with a constant C independent of $m$.

The first assertion is trivial if $\operatorname{rank}_{\mathrm{an}}(E) = 0$ and was proved by Gross and Zagier [20] when $\operatorname{rank}_{\mathrm{an}}(E) = 1$ by constructing a point of infinite order (a Heegner point). The second assertion uses Kolyvagin's method of Euler systems and an infinite family of Heegner points. Combining these two statements with (8) proves that if $\operatorname{rank}_{\mathrm{an}}(E) \leq 1$, then $\operatorname{rank}(E) = \operatorname{rank}_{\mathrm{an}}(E)$ and $\# \text{Ш}_E \leq C$.

**Theorem 5.13** (Nekovář [55]). *If* $\text{Ш}_E$ *is finite, then the Parity Conjecture holds for* $E$.

What Nekovář proved (using recent results of Vatsal [74] and Cornut [10]) is that if $p$ is a prime not dividing $\#E(\mathbf{Q})_{\mathrm{tors}}$, and if $E$ has good ordinary reduction at $p$ (see Chapters V and VII of [68]), then $\dim_{\mathbf{F}_p} S_p(E)$ and $\operatorname{rank}_{\mathrm{an}}(E)$ have the same parity. But if $\text{Ш}_E$ is finite, then the Cassels pairing [7] is a nondegenerate skew-symmetric pairing on $\text{Ш}_E$, and it follows that $\dim_{\mathbf{F}_p} \text{Ш}_E$ is even. Hence by (9), $\operatorname{rank}(E)$ and $\dim_{\mathbf{F}_p} S_p(E)$ have the same parity. Every elliptic curve has infinitely many primes of good ordinary reduction, so the Parity Conjecture for $E$ follows.

It had been proved earlier that if the Tate-Shafarevich Conjecture is true, then the Parity Conjecture holds for semistable elliptic curves (combining [33] and Theorem 5.8) and for the curves $y^2 = x^3 - d^2x$ (see Monsky's appendix to [24]).

## 6. Quadratic twists

Up until now, we have been considering ranks of arbitrary elliptic curves over $\mathbf{Q}$. To understand ranks, it is useful to consider special families of elliptic curves. Quadratic twists give perhaps the simplest such families, since even though their complex analysis is "constant" (i.e., they are isomorphic over $\mathbf{C}$), their arithmetic varies.

TABLE 2. Ranks $r_d$ in the family $E_d : dy^2 = x^3 - x$

| $d$ | $r_d$ | discovery | $x$-coordinates of independent points |
|---:|---|---|---|
| 1 | 0 | Fermat (∼1640) | |
| 5 | 1 | Billing [2] (1937) | 9 |
| 34 | 2 | Wiman [78] (1945) | $17, \frac{17}{8}$ |
| 1254 | 3 | Wiman [78] (1945) | $\frac{11}{8}, \frac{22}{3}, \frac{19}{8}$ |
| 29274 | 4 | Wiman [78] (1945) | $\frac{41}{34}, \frac{24}{17}, \frac{34}{7}, \frac{121}{2}$ |
| 205015206 | 5 | Rogers [61] (2000) | $\frac{649}{323}, \frac{1650}{1121}, \frac{326}{323}, \frac{19234}{8993}, \frac{5783298}{2468041}$ |
| 61471349610 | 6 | Rogers [61] (2000) | $\frac{779}{134}, \frac{52441}{31691}, \frac{228001}{931}, \frac{21033}{10658}, \frac{56416}{32761}, \frac{4427538}{2255}$ |

**Definition 6.1.** If $E$ is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Q}$, then the *quadratic twist* of $E$ by a nonzero rational number $d$ is the elliptic curve $y^2 = x^3 + ad^2x + bd^3$. It will be convenient to make the change of variables $(x, y) \mapsto (dx, d^2y)$, so that we can rewrite this curve in the equivalent (isomorphic) form

$$E_d : \quad dy^2 = x^3 + ax + b.$$

In this section we will study the behavior of $\mathrm{rank}(E_d)$ as $d$ varies. Clearly $E_{dt^2}$ is isomorphic to $E_d$ for every $t \in \mathbf{Q}^\times$, so we need only consider squarefree integers $d$.

6.1. **The curve $y^2 = x^3 - x$.** For the remainder of this section, let $E$ be the curve $y^2 = x^3 - x$. The family $E_d : dy^2 = x^3 - x$ of quadratic twists of $E$ has been studied extensively. This family is closely connected with the classical *congruent number problem*, which asks what integers are the areas of right triangles with three rational sides. The relationship between this problem and the above family of quadratic twists is the fact that there is a right triangle with rational sides and area $d$ if and only if $\mathrm{rank}(E_d) > 0$ (see for example [30], [63], [73]).

Note that $E_d$ is isomorphic to $E_{-d}$ by the change of variables $(x, y) \mapsto (-x, y)$, so we may restrict to $d > 0$.

The curve $E_{157}$ has rank one, but the simplest point of infinite order (see p. 5 of [30]) is

$$\left(-\frac{27748778732924463216912 1}{609760250665615167250729}, \frac{22826630568289716631287654159126420}{47614438250616355400538204422244906 7}\right).$$

For $r \leq 4$, Table 2 gives the smallest $|d|$ for which $E_d$ has rank $r$. For $r = 5, 6$ there are probably smaller examples of $d$ than the one listed in the table.

In [78], Wiman doubted whether any other $d$'s with $\mathrm{rank}(E_d) = 4$ could be found. Using the method of proof of Theorem 8.2(vii) below and modern computers, it is no longer difficult to find such examples. In [79], Wiman pointed out that he knew of no $d$ for which $\mathrm{rank}(E_d) > 4$ and said that if such exist, they would be almost insurmountably difficult to find.

If $d$ is squarefree, an upper bound on the rank of $E_d$ is given by twice the number of odd prime divisors of $d$ (see [78]), and there is an absolute constant $C$ such that

$$\mathrm{rank}(E_d) \leq C \frac{\log |d|}{\log \log |d|}$$

for all squarefree $d$ with $|d| > 2$ (see Exercise 3.4.11 of [66]). This is known as the "trivial bound" for the rank of $E_d$. It follows that for $E_d$ to have large rank,

$d$ must have many prime divisors. For example, the last $d$ in Table 2 has prime factorization

$$61471349610 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 19 \cdot 41 \cdot 43 \cdot 67 \cdot 83.$$

**Theorem 6.2** (Tunnell [73]). *If $E$ is $y^2 = x^3 - x$ and $d$ is a squarefree positive integer, then*

$$L(E_d, 1) \;=\; \frac{(n-2m)^2 a\Omega}{16\sqrt{d}}$$

*where*

$a = 1$ *if $d$ is odd,* $a = 2$ *if $d$ is even,*
$n = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 8z^2 = d/a\}$,
$m = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 32z^2 = d/a\}$,
$\Omega = \displaystyle\int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \approx 2.6220575542921198\ldots.$

*In particular,*

$$L(E_d, 1) = 0 \iff n = 2m.$$

For example, if $d = 1$, then $m = n = 2$ and $L(E,1) = \Omega/4$ as in Example 5.9.

## 7. Variation of the rank in families of quadratic twists

Fix for this section an elliptic curve $E$ over $\mathbf{Q}$. We will study how the ranks of quadratic twists are distributed.

**Definition 7.1.** Let

$$S(X) = \{\text{squarefree } d \in \mathbf{Z} : |d| \le X\}.$$

Define the *average rank* $\mathrm{A}(E)$ to be

$$\mathrm{A}(E) = \lim_{X\to\infty} \frac{\sum_{d\in S(X)} \operatorname{rank}(E_d)}{\#S(X)} \tag{10}$$

if this limit exists, and in general define the upper and lower average ranks, $\overline{\mathrm{A}}(E)$ and $\underline{\mathrm{A}}(E)$, to be, respectively, the corresponding lim sup and lim inf.

Define

$$N_*(X) = \#\{d \in S(X) : \operatorname{rank}(E_d) \text{ is } *\}$$

where $*$ can be any property that makes sense, such as "1", "$\ge 2$", "even", etc. We write simply $N(X) = N_{\ge 0}(X) = \#S(X)$.

Let

$$\mathrm{D}_*(E) = \lim_{X\to\infty} \frac{N_*(X)}{N(X)}$$

if this limit exists, and in general let $\overline{\mathrm{D}}_*(E)$ and $\underline{\mathrm{D}}_*(E)$ be the corresponding lim sup and lim inf.

The next theorem, which is well-known (see for example the corollary to Proposition 10 of [62]), describes how the sign in the functional equation of the $L$-function changes under quadratic twist. If $t$ is a squarefree integer, let $\chi_t$ be the quadratic Dirichlet character attached to the extension $\mathbf{Q}(\sqrt{t})/\mathbf{Q}$. Concretely, $\chi_t$ is the unique

Dirichlet character modulo $t$ (if $t \equiv 1 \pmod 4$) or $4t$ (if $t \equiv 2, 3 \pmod 4$) with the property that for all odd primes $p$ not dividing $t$,

$$\chi_t(p) = \begin{cases} +1 & \text{if } t \text{ is a square modulo } p, \\ -1 & \text{if } t \text{ is not a square modulo } p. \end{cases}$$

Recall that the conductor of an elliptic curve is defined on p. 196 of [70].

**Theorem 7.2.** *Suppose that $d$ is a squarefree integer, and let $\mathcal{N}_d$ be the conductor of $E_d$. If $t \equiv 1 \pmod 4$ is a squarefree integer relatively prime to $d\mathcal{N}_1$, then*

$$w_{E_{td}}/w_{E_d} = \chi_t(-\mathcal{N}_d).$$

**Example 7.3.** Let $E$ be the curve $y^2 = x^3 - x$. It follows from Theorem 6.2 that $L(E, 1) \neq 0$ and $L(E_2, 1) \neq 0$, so $w_E = w_{E_2} = 1$. Combining this with Theorem 7.2 and the fact that the conductors of $E$ and $E_2$ are 32 and 64, respectively, one can show that the sign in the functional equation of $L(E_d, 1)$ for $d > 0$ is given by

$$w_{E_d} = \begin{cases} +1 & \text{if } d \equiv 1, 2, \text{ or } 3 \pmod 8, \\ -1 & \text{if } d \equiv 5, 6, \text{ or } 7 \pmod 8. \end{cases}$$

(Since $d$ is squarefree, it is not 0 or 4 $\pmod 8$.) In particular, if $d > 0$ and $d \equiv 5, 6$, or 7 $\pmod 8$, then the Parity Conjecture predicts that $\mathrm{rank}(E_d)$ is odd. Elkies [11], [12] has verified that $\mathrm{rank}(E_d) \geq 1$ for all positive squarefree $d \equiv 5, 6,$ or $7 \pmod 8$ less than $10^6$. Note that for $d \equiv 5, 6,$ or $7 \pmod 8$ one can also use Theorem 6.2 to show that $L(E_d, 1) = 0$, since $n = m = 0$ in those cases.

**Corollary 7.4.** *Suppose that the Parity Conjecture holds. Then*

$$\mathrm{D}_{\mathrm{even}}(E) = \mathrm{D}_{\mathrm{odd}}(E) = 1/2 \quad \textit{and} \quad \underline{\mathrm{A}}(E) \geq 1/2.$$

*Proof.* This follows from Theorem 7.2 applied to the curves $E_d$ for (positive or negative) $d$ dividing twice the conductor of $E$. □

**Conjecture 7.5** (Goldfeld [15])**.** $\mathrm{A}(E) = 1/2$.

In other words, Goldfeld's conjecture predicts that the average rank is as small as the Parity Conjecture allows. The following conjecture is an easy consequence of Goldfeld's conjecture combined with the Parity Conjecture and Corollary 7.4.

**Conjecture 7.6** (Density Conjecture)**.** $\mathrm{D}_0(E) = \mathrm{D}_1(E) = 1/2$ *and* $\mathrm{D}_{\geq 2}(E) = 0$.

Note that $N(X) \sim \frac{2}{\zeta(2)} X = \frac{12}{\pi^2} X$. The Density Conjecture would imply that

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

Given the Birch and Swinnerton-Dyer Conjecture, the Density Conjecture can be interpreted as saying that the set where the $L$-function has "extra vanishing", that is, the set of $d$ for which the value of $\mathrm{rank}_{\mathrm{an}}(E_d)$ is larger than the functional equation forces it to be, has density zero. For some recent motivation for the Density Conjecture from this point of view, see §5 of [26].

When $r \geq 2$ the Density Conjecture predicts that $N_r(X) = o(X)$, and one can ask for a more precise description of the rate of growth of $N_r(X)$. Numerical evidence suggests that $N_{\geq 2,\mathrm{even}}(X)$ and $N_{\geq 3,\mathrm{odd}}(X)$ grow roughly like $X^{3/4}$ (see Figure 2 of [9] and see [12], respectively). The following conjecture, based on connections between $L$-functions and random matrix theory, makes this more precise.

**Conjecture 7.7** (Conjecture 1 and (7) of [9]). *There are constants $b_E$ and $e_E$, with $b_E \neq 0$, such that*

$$\lim_{X\to\infty} \frac{N_{\geq 2,\mathrm{even}}(X)}{X^{3/4}\log(X)^{e_E}} = b_E.$$

See §8 for some lower bounds for $N_{\geq r}(X)$.

Heath-Brown showed that if $E$ is $y^2 = x^3 - x$ and one restricts to twists by odd integers $d$, then the density of twists with rank at least $r$ goes to zero at least exponentially with $r$. From this one can deduce an upper bound for the average rank and lower bounds for the densities $\underline{\mathrm{D}}_r(E)$ for small values of $r$. Let $S^{\mathrm{odd}}(X) = \{\text{odd squarefree } d \in \mathbf{Z}^+ : d \leq X\}$, define $\mathrm{A}^{\mathrm{odd}}(E)$ as in (10) but with $S^{\mathrm{odd}}(X)$ in place of $S(X)$, and similarly write $\mathrm{D}_*^{\mathrm{odd}}(E)$ for the corresponding density restricted to odd $d$.

**Theorem 7.8** (Heath-Brown [24]). *Let $E$ be the curve $y^2 = x^3 - x$. Then:*

(i) $\overline{\mathrm{A}}^{\mathrm{odd}}(E) \leq 1.2645$*;*
(ii) *for every* $r \geq 0$, $\overline{\mathrm{D}}_{\geq r}^{\mathrm{odd}}(E) \leq 1.7313 \cdot 2^{-(r^2-r)/2}$*;*
(iii) $\underline{\mathrm{D}}_0(E) > .044$*;*
(iv) *if the Parity Conjecture holds, then* $\underline{\mathrm{D}}_1(E) > .26$.

*Proof.* Assertions (i) and (ii) are Corollaries 4 and 3 of [24], respectively. In fact, Heath-Brown proves more. As before, we may restrict to $d > 0$. Let $s_2(d) = \dim_{\mathbf{F}_2} S_2(E_d)$ (recall the 2-Selmer group $S_2$ from §5). Since $E_d(\mathbf{Q})_{\mathrm{tors}}$ contains $(\mathbf{Z}/2\mathbf{Z})^2$, (9) shows that

$$s_2(d) \geq \mathrm{rank}(E_d) + 2. \tag{11}$$

Monsky proved in an appendix to [24] that

$$s_2(d) \equiv \begin{cases} 0 \pmod 2 & \text{if } d \equiv 1 \text{ or } 3 \pmod 8, \\ 1 \pmod 2 & \text{if } d \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{12}$$

Let $\overline{SD}_*(h)$ (resp., $\underline{SD}_*(h)$) denote the upper (resp., lower) density of $d \equiv h \pmod 8$ such that $s_2(d) - 2$ is $*$. Corollary 3 of [24] proves that

$$\overline{SD}_{\geq r}(h) \leq 1.7313 \cdot 2^{-(r^2-r)/2}$$

for every $r$ and every odd $h$. Taking $r = 2$ and $h = 1$ or $3$, one finds that $\underline{SD}_{\leq 1}(1) \geq .134$ and $\underline{SD}_{\leq 1}(3) \geq .134$. But (11) and (12) show that if $d \equiv 1$ or $3 \pmod 8$ and $s_2(d) \leq 3$, then $s_2(d) = 2$ and $\mathrm{rank}(E_d) = 0$. Thus $\underline{\mathrm{D}}_0(E) \geq .044$, which proves (iii). The proof of (iv) is similar, taking $r = 3$ and $h = 5$ or $7$. In this case (11) and (12) show that if $d \equiv 5$ or $7 \pmod 8$ and $s_2(d) \leq 4$, then $s_2(d) = 3$ and $\mathrm{rank}(E_d) \leq 1$. If the Parity Conjecture holds, then $\mathrm{rank}(E_d)$ is odd, so $\mathrm{rank}(E_d) = 1$, and (iv) follows. □

In 1960, Honda stated a controversial conjecture that would imply:

**Conjecture 7.9** (Honda [25]). *Suppose $E$ is an elliptic curve over $\mathbf{Q}$. Then there is a constant $C_E$ depending only on $E$ such that for all $d$,*

$$\mathrm{rank}(E_d(\mathbf{Q})) \leq C_E.$$

*In other words, for all sufficiently large $r$, $N_r(X) = 0$ for all $X$.*

Instead of looking at elliptic curves over $\mathbf{Q}$ and twisting by elements of $\mathbf{Q}$, one could consider an elliptic curve over a field $K$ and twist by elements of $K$. In [71], Shafarevich and Tate constructed a family of quadratic twists with unbounded rank for an elliptic curve over the function field $\mathbf{F}_q(t)$, where $\mathbf{F}_q$ is the field with $q$ elements. Their result led many to believe that a similar phenomenon should hold for elliptic curves over $\mathbf{Q}$, i.e., that Honda's conjecture should be false.

## 8. Lower bounds for $N_{\geq r}(X)$

In this section we show how to obtain lower bounds for the number of quadratic twists with rank at least $r$, for small values of $r$.

**Definition 8.1.** For every $t \in \mathbf{Q}^\times$, there is a unique squarefree integer $\mathrm{sf}(t)$ such that $t = \mathrm{sf}(t)y^2$ with $y \in \mathbf{Q}^\times$. (If $t = \pm \prod p^{n_p}$ is the prime factorization of $t$, then $\mathrm{sf}(t) = \pm \prod_{n_p \text{ odd}} p$.)

The following theorem is a combination of results of Gouvêa and Mazur [19], Stewart and Top [69], and the authors [65] (see also [46] for related results). (In this theorem, $E$ is always an elliptic curve over $\mathbf{Q}$, and $A(X) \gg B(X)$ means that there exists a constant $C$ depending only on $E$ such that $A(X) \geq CB(X)$ for all sufficiently large $X$.)

**Theorem 8.2.** (i) $N_{\geq 1}(X) \gg X^{1/2}$.

(ii) *If $E$ is $y^2 = x^3 + ax + b$ and $ab \neq 0$, then $N_{\geq 2}(X) \gg X^{1/7}/\log^2(X)$.*

(iii) *If $E$ is $y^2 = x^3 + ax + b$, and $x^3 + ax + b$ has a nonzero rational root, then $N_{\geq 2}(X) \gg X^{1/3}$.*

(iv) *If $E$ is $y^2 = x(x-f)(x-c^2 f)$ or $y^2 = x(x-f)(x+2c^2 f)$ with $c, f \in \mathbf{Q}$, or $E$ is $y^2 = x^3 - x$, then $N_{\geq 3}(X) \gg X^{1/6}$.*

*Suppose now that the Parity Conjecture holds for all the quadratic twists of $E$.*

(v) $N_{\geq 2}(X) \gg X^{1/2}$.

(vi) *If $E$ is $y^2 = x^3 + ax + b$ where $x^3 + ax + b$ has three real roots and either the largest or smallest of these roots is rational, then $N_{\geq 3}(X) \gg X^{1/3}$.*

(vii) *If $E$ is $y^2 = x(x-f)(x-c^2 f)$ with $c, f \in \mathbf{Q}$, or $E$ is $y^2 = x^3 - x$, then $N_{\geq 4}(X) \gg X^{1/6}$.*

*Sketch of proof.* Write $E : y^2 = f(x)$ with a cubic polynomial $f(x) \in \mathbf{Q}[x]$. Suppose that $g(t) \in \mathbf{Q}[t]$ is a squarefree polynomial, and consider

$$E_{g(t)} : g(t)y^2 = f(x).$$

This is an elliptic curve defined over the rational function field $\mathbf{Q}(t)$. Let $r = \mathrm{rank}(E_{g(t)})$, the rank of the finitely generated abelian group $E_{g(t)}(\mathbf{Q}(t))$, and let $P_1(t), \ldots, P_r(t)$ be $r$ independent points in $E_{g(t)}(\mathbf{Q}(t))$.

If $t_0 \in \mathbf{Q}$ is not a root of $g(t)$, nor of the denominators of the coordinates of the $P_i(t)$, then $E_{g(t_0)}$ is a quadratic twist of $E$ defined over $\mathbf{Q}$ and $P_1(t_0), \ldots, P_r(t_0) \in E_{g(t_0)}(\mathbf{Q})$. Theorem C of [67] shows that these points are independent for all $t_0$ outside a finite exceptional set $\Sigma$. Since $E_{g(t_0)} \cong E_{\mathrm{sf}(g(t_0))}$, we conclude that $\mathrm{rank}(E_{\mathrm{sf}(g(t_0))}) \geq r$ for all $t_0 \in \mathbf{Q} - \Sigma$. In other words, $N_{\geq r}(X) \geq \#M(X)$, where

$$M(X) := \{d \in S(X) : d = \mathrm{sf}(g(t_0)) \text{ for some } t_0 \in \mathbf{Q} - \Sigma\}.$$

Results of Gouvêa and Mazur [19], improved by Stewart and Top [69], give a lower bound for $\#M(X)$. (The smaller the degree of $g(t)$, the larger the lower bound.)

For example, when $g(t) = f(t)$, $\operatorname{rank}(E_{g(t)}) = 1$ (we can take $P_1(t) = (t, 1)$). The above argument, applied to this example, was used by Gouvêa and Mazur [19] to prove a slightly weaker form of (i). (As stated here, (i) uses improved bounds of Stewart and Top.) Assertion (ii) was proved by Stewart and Top using a polynomial $g(t)$ of degree 14 constructed by Mestre [45]. Assertions (iii) and (iv) are proved in [65] by finding ways to construct suitable polynomials $g(t)$.

For example, if $E$ is $y^2 = x^3 - x$, and $g(t) = 6(t^3 - 33t^2 - 33t + 1)$, then

$$\operatorname{rank}(E_{g(t)}) = 1, \quad \operatorname{rank}(E_{g(t^2)}) = 2, \quad \operatorname{rank}(E_{g(t^4)}) = 3.$$

Three independent points of infinite order on $E_{g(t^4)}$ are

$$P_1(t) = \left(-\frac{t^4 - 6t^2 + 1}{3(t^2+1)^2}, \frac{2}{9(t^2+1)^3}\right), \quad P_2(t) = \left(-\frac{t^4 + 6t^2 + 1}{3(t^2-1)^2}, \frac{2}{9(t^2-1)^3}\right),$$
$$P_3(t) = \left(\frac{t^4+1}{6t^2}, \frac{1}{36t^3}\right).$$

Let

$$M'(X) = \{d \in M(X) : w_{E_d} = (-1)^{r+1}\}.$$

If $d \in M'(X)$, then $\operatorname{rank}(E_d) \geq r$. But assuming the Parity Conjecture, $\operatorname{rank}(E_d) \equiv r + 1 \pmod 2$, so $\operatorname{rank}(E_d) \geq r + 1$ and $N_{\geq r+1}(X) \geq \#M'(X)$. Under additional conditions on $g(t)$, one can obtain a lower bound for $\#M'(X)$. This idea was used by Gouvêa and Mazur [19] to prove a slightly weaker version of (v). Applying this idea to some of the polynomials used to prove (i), (iii), and (iv) gives (v), (vi), and (vii). □

See [65] for additional families of curves for which the conclusions of (iv) and (vii) of Theorem 8.2 hold.

*Remark* 8.3. Conjectures 7.6 and 7.7 and the numerical evidence in [9] and [12] suggest that $N_{\geq r}(X)$ should grow roughly like $X$, $X$, $X^{3/4}$, and $X^{3/4}$ for $r = 0$, 1, 2, and 3, respectively. The lower bounds of Theorem 8.2 are consistent with, but weaker than, these predictions.

## 9. Looking for large ranks

The standard method for finding elliptic curves of large rank is due to Mestre [41], [44]. We describe it here briefly.

Suppose $E^{(t)}$ is an elliptic curve over $\mathbf{Q}(t)$ with $r$ independent points. (See Table 3 for examples with large rank.) As in the proof of Theorem 8.2, specializing gives, for all but finitely many rational numbers $t_0$, elliptic curves $E^{(t_0)}$ over $\mathbf{Q}$ of rank at least $r$. One would now like to search among these specializations for some that have even larger rank.

Table 3. Rank records over $\mathbf{Q}(t)$

| **Rank over $\mathbf{Q}(t) \geq$** | **Year** | **Discoverers** |
|---|---|---|
| 11 | 1991 | Mestre [42] |
| 12 | 1991 | Mestre [43] |
| 13 | 1994 | Nagao [52] |
| 14 | 2000–1 | Mestre [47], Kihara [28] |

To do this, choose a pair of parameters $n, m \in \mathbf{Z}^+$. For positive integers $t_0 \leq n$, compute the Birch and Swinnerton-Dyer product $\pi_{E^{(t_0)}}(m)$ defined by (4). The Birch and Swinnerton-Dyer philosophy says that those $t_0$ for which this value is relatively large are good candidates for having "extra" rank, and one searches for points on those curves. Hopefully one finds (several) new points, independent of the $r$ specialized points. Modifications of this program (and more and more computing power) led to all the examples in Table 1 with rank at least 15.

We now describe a method for finding curves of large rank in a fixed family of quadratic twists, in the spirit of Theorem 8.2.

Fix an elliptic curve $E : y^2 = f(x)$ over $\mathbf{Q}$, and let $E_d$ denote its quadratic twist $dy^2 = f(x)$ for $d \in \mathbf{Q}^\times$, as in §6. In [19] (see the proof of Theorem 8.2), Gouvêa and Mazur count how many $d$'s occur as $\mathrm{sf}(f(t))$ for some rational $t$. Instead, we will count *how often* each $d$ occurs.

**Definition 9.1.** If $t \in \mathbf{Q}$, define the *height* of $t$

$$h(t) = \max\{\log|u|, \log|v|\}$$

where $t = u/v$ with relatively prime integers $u, v$.

For $B > 0$ let

$$M(d, B) = \#\{t \in \mathbf{Q} : h(t) < B,\ \mathrm{sf}(f(t)) = d\}.$$

The next proposition follows easily from basic facts about heights on elliptic curves (see for example the proposition in §2 of [80]).

**Proposition 9.2.** *For every squarefree integer $d$,*

$$\lim_{B\to\infty} \frac{M(d, B)}{B^{\mathrm{rank}(E_d)/2}}$$

*exists and is positive.*

In particular if $\mathrm{rank}(E_d) > \mathrm{rank}(E_{d'})$, then for all sufficiently large $B$ we have $M(d, B) > M(d', B)$.

This suggests a computational method for searching for curves $E_d$ with large rank:

- Let $t$ run through all rational numbers with $h(t) < B$ and make a table of the values $M(d, B)$.
- Pick out those $d$ for which $M(d, B)$ is large, and compute $\mathrm{rank}(E_d)$.

Rogers [61] implemented this method for the curve $E : y^2 = x^3 - x$ and found the large examples in Table 2: $\mathrm{rank}(E_{205015206}) = 5$, $\mathrm{rank}(E_{61471349610}) = 6$.

Proposition 9.2 also suggests a method for testing the entire family of curves $E_d$ at once for curves of large rank. Although the method works generally [64], to illustrate it we restrict to the curve $y^2 = x^3 - x$.

Define

$$S(j, k) \ = \sum_{x \in \mathbf{Q} - \{0, \pm 1\}} |\mathrm{sf}(x^3 - x)|^{-k} h(x)^{-j}.$$

If $a, b, c, d \in \mathbf{Z}^+$, let $\omega_{a,b,c,d} \in \mathbf{Z}^2$ be a shortest nonzero vector in the lattice

$$\{(u, v) \in \mathbf{Z}^2 : a^2 \mid u,\ b^2 \mid v,\ c^2 \mid (u + v),\ d^2 \mid (u - v)\}$$

and define

$$Q(j,k) \;=\; \sum_{a,b,c,d=1}^{\infty}{}' \qquad \frac{(abcd)^{2k}}{\|\omega_{a,b,c,d}\|^{4k} h(\omega_{a,b,c,d})^{j}}$$

where the sum is over $a,b,c,d$ such that, if $\omega_{a,b,c,d} = (u,v)$, then $u$ and $v$ are relatively prime and $uv(u+v)(u-v) \neq 0$.

**Theorem 9.3** ([64]). *If $j$ is a positive real number, then the following are equivalent:*

(i) $\operatorname{rank}(E_d) < 2j$ *for every* $d \in \mathbf{Z}^+$,
(ii) $S(j,k)$ *converges for some* $k \geq 1$,
(iii) $S(j,k)$ *converges for every* $k \geq 1$,
(iv) $Q(j,k)$ *converges for some* $k \geq 1$,
(v) $Q(j,k)$ *converges for every* $k \geq 1$.

*Idea of proof.* If $x \in \mathbf{Q} - \{0, \pm 1\}$ and $d = \operatorname{sf}(x^3 - x)$, then $(x, \pm\sqrt{(x^3-x)/d}) \in E_d(\mathbf{Q})$. Using this we can rewrite

$$S(j,k) = \frac{1}{2} \sum_{d \text{ squarefree}} |d|^{-k} \sum_{P \in E_d(\mathbf{Q})} h(x(P))^{-j},$$

where $x(P)$ denotes the $x$-coordinate of $P$. If $\operatorname{rank}(E_d) \geq 2j$ for some $d$, then it follows from Proposition 9.2 that the inner sum $\sum_{P \in E_d(\mathbf{Q})} h(x(P))^{-j}$ diverges, so $S(j,k)$ diverges.

But if $\operatorname{rank}(E_d) < 2j$ for every $d$, then $j > 1$ (see Table 2), and one can show that

$$\sum_{P \in E_d(\mathbf{Q})} h(x(P))^{-j} \ll \log(|d|)^{-j},$$

so $S(j,k)$ converges. It follows that (i), (ii), and (iii) are equivalent.

Further, one can compare $Q(j,k)$ and $S(j,k)$ directly to show that

$$Q(j,k) \text{ converges } \iff S(j,k) \text{ converges}$$

so (ii) is equivalent to (iv) and (iii) is equivalent to (v). □

By Theorem 9.3, unboundedness of ranks in the family of quadratic twists of $E$ is equivalent to the divergence of $S(j,k)$ (or $Q(j,k)$) for all $j > 0$ and $k \geq 1$. Our experimental evidence indicates that such divergence would be very slow.

## References


[1] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), no. 203, 29–68. MR **93m:**11136

[2] G. Billing, *Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlechte eins*, Nova Acta Reg. Soc. Sc. Upsaliensis (4) **11** (1937), No. 1.

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

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

[5] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR **2002d:**11058

[6] A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR **56:**15658

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

[8] ———, *Arithmetic on an elliptic curve*, in Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler (1963), 234–246. MR **31:**167

[9] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular $L$-functions*, preprint.

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

[11] N. Elkies, *Heegner point computations*, in Algorithmic Number Theory (ANTS-1), Lect. Notes in Comp. Sci. **877**, Springer-Verlag, Berlin (1994), 122–133. MR **96f:**11080

[12] ———, `http://www.math.harvard.edu/~elkies/compnt.html`.

[13] S. Fermigier, *Un exemple de courbe elliptique définie sur $\mathbf{Q}$ de rang* $\geq 19$, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 6, 719–722. MR **93i:**11067

[14] ———, *Une courbe elliptique définie sur $\mathbf{Q}$ de rang* $\geq 22$, Acta Arith. **82** (1997), no. 4, 359–363. MR **98j:**11041

[15] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), M. B. Nathanson, ed., Lect. Notes in Math. **751**, Springer-Verlag, Berlin (1979), 108–118. MR **81i:**12014

[16] ———, *Sur les produits partiels eulériens attachés aux courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 14, 471–474. MR **84d:**14031

[17] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified*, in Proc. 18th STOC (Berkeley, May 28–30, 1986), ACM, New York, 1986, 316–329.

[18] ———, *Primality testing using elliptic curves*, J. ACM **46** (1999), no. 4, 450–472. MR **2002e:**11182

[19] F. Gouvêa, B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23. MR **92b:**11039

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

[21] F. J. Grunewald, R. Zimmert, *Über einige rationale elliptische Kurven mit freiem Rang* $\geq 8$, J. Reine Angew. Math. **296** (1977), 100–107. MR **57:**6028

[22] H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen eliptischen Fällen. Vorläufige Mitteilung*, Nachr. Ges. Wiss. Göttingen I, Math.-phys. Kl. Fachgr. I Math. Nr. 42 (1933), 253–262 (# 38 in H. Hasse, Mathematische Abhandlungen, Band 2, Walter de Gruyter, Berlin-New York, 1975). MR **57:**5648b

[23] ———, *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpen*, Abh. Math. Sem. Univ. Hamburg. **10** (1934), 325–348 (# 40 in Helmut Hasse Mathematische Abhandlungen, Band 2, Walter de Gruyter, Berlin-New York, 1975). MR **57:**5648b

[24] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370. MR **95h:**11064

[25] T. Honda, *Isogenies, rational points and section points of group varieties*, Japan. J. Math., **30** (1960), 84–101. MR **27:**5762

[26] N. M. Katz, P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. **36** (1999), no. 1, 1–26. MR **2000f:**11114

[27] S. Kihara, *On an infinite family of elliptic curves with rank* $\geq 14$ *over* $\mathbf{Q}$, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), no. 2, 32. MR **98d:**11059

[28] ———, *On an elliptic curve over* $\mathbf{Q}(t)$ *of rank* $\geq 14$, Proc. Japan Acad. Ser. A Math. Sci. **77** (2001), no. 4, 50–51. MR **2002a:**11057

[29] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209. MR **88b:**94017

[30] ———, Introduction to elliptic curves and modular forms, 2nd edition, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1993. MR **94a:**11078

[31] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E,\mathbf{Q})$ 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). MR **89m:**11056

[32] ———, *Euler systems*, in The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., Prog. in Math. **87**, Birkhäuser, Boston (1990), 435–483. MR **92g:**11109

[33] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR **82g:**14028

[34] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33** (1976), no. 2, 193–237. MR **55:**7910

[35] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), no. 3, 649–673. MR **89g:**11125

[36] E. Lutz, *Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic*, J. Reine Angew. Math. **177** (1937), 238–247.

[37] R. Martin, W. McMillen, posting to Number Theory server, March 16, 1998.

[38] ———, posting to Number Theory server, May 2, 2000.

[39] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. math. IHES **47** (1977), 33–186. MR **80c:**14015

[40] J.-F. Mestre, *Construction d'une courbe elliptique de rang* $\geq 12$, C. R. Acad. Sci. Paris Sér. I Math. **295** (1982), no. 12, 643–644. MR **84b:**14019

[41] ———, *Formules explicites et minorations de conducteurs de variétés algébriques*, Comp. Math. **58** (1986), no. 2, 209–232. MR **87j:**11059

[42] ———, *Courbes elliptiques de rang* $\geq 11$ *sur* $\mathbf{Q}(t)$, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 3, 139–142. MR **92j:**11052

[43] ———, *Courbes elliptiques de rang* $\geq 12$ *sur* $\mathbf{Q}(t)$, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 4, 171–174. MR **92m:**11052

[44] ———, *Un exemple de courbe elliptique sur* $\mathbf{Q}$ *de rang* $\geq 15$, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 6, 453–455. MR **93b:**11071

[45] ———, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 12, 919–922. MR **93e:**11075

[46] ———, *Rang de certaines familles de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. **327** (1998), no. 8, 763–764. MR **99j:**11063

[47] ———, Berkeley Number Theory Seminar, September 15, 2000.

[48] V. S. Miller, *Use of elliptic curves in cryptography*, in Advances in cryptology—CRYPTO '85, Lect. Notes in Comp. Sci. **218**, Springer-Verlag, Berlin (1986), 417–426. MR **88b:**68040

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

[50] K. Nagao, *Examples of elliptic curves over* $\mathbf{Q}$ *with rank* $\geq 17$, Proc. Japan Acad. Ser. A Math. Sci. **68** (1992), no. 9, 287–289. MR **93m:**11046

[51] ———, *An example of elliptic curve over* $\mathbf{Q}$ *with rank* $\geq 20$, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 8, 291–293. MR **95a:**11052

[52] ———, *An example of elliptic curve over* $\mathbf{Q}(T)$ *with rank* $\geq 13$, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 5, 152–153. MR **95e:**11064

[53] K. Nagao, T. Kouya, *An example of elliptic curve over* $\mathbf{Q}$ *with rank* $\geq 21$, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 4, 104–105. MR **95e:**11063

[54] T. Nagell, *Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I (1935), No. 1, 1–25.

[55] J. Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104. MR **2002e:**11060

[56] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166. MR **15:**151a

[57] ———, *Propriétés arithmétiques de certaines familles de courbes algébriques*, Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III, pp. 481–488, Erven P. Noordhoff N.V., Groningen; North-Holland Publishing Co., Amsterdam, 1956. MR **19:**321b

[58] D. E. Penney, C. Pomerance, *A search for elliptic curves with large rank*, Math. Comp. **28** (1974), 851–853. MR **51:**12861

[59] ———, *Three elliptic curves with rank at least seven*, Math. Comp. **29** (1975), 965–967. MR **51:**12862

[60] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Math. Pures Appl., Ser. 5, vol. 7 (1901), 161–233.

[61] N. Rogers, *Rank computations for the congruent number elliptic curves*, Exper. Math. **9** (2000), no. 4, 591–594. MR **2001k:**11104

[62] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Comp. Math. **100** (1996), no. 3, 311–349. MR **97m:**11075

[63] K. Rubin, *Right triangles and elliptic curves*, to appear in Bay Area Math Adventures, D. F. Hayes, ed., MAA.

[64] K. Rubin, A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Exper. Math. **9** (2000), no. 4, 583–590. MR **2001k:**11105

[65] ———, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), no. 4, 559–569.

[66] A. Silverberg, *Open questions in arithmetic algebraic geometry*, in Arithmetic Algebraic Geometry (Park City, UT, 1999), IAS/Park City Mathematics Series **9**, AMS, Providence, RI (2001), 85–142.

[67] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211. MR **84k:**14033

[68] ———, The arithmetic of elliptic curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986. MR **87g:**11070

[69] C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), no. 4, 943–973. MR **95m:**11055

[70] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206. MR **54:**7380

[71] J. T. Tate, I. R. Safarevic, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), no. 4, 770–773 (= Soviet Math. Dokl. **8** (1967), no. 4, 917–920). MR **38:**5790

[72] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), no. 3, 553–572. MR **96d:**11072

[73] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), no. 2, 323–334. MR **85d:**11046

[74] V. Vatsal, *Special values of anticyclotomic L-functions*, preprint.

[75] A. Weil, Number theory, an approach through history, Birkhäuser, Boston, 1984. MR **85c:**01004

[76] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551. MR **96d:**11071

[77] A. Wiman, *Über den Rang von Kurven* $y^2 = x(x+a)(x+b)$, Acta Math. **76** (1945), 225–251. MR **7:**70g

[78] ———, *Über rationale Punkte auf Kurven* $y^2 = x(x^2 - c^2)$, Acta Math. **77** (1945), 281–320. MR **7:**323b

[79] ———, *Über rationale Punkte auf Kurven dritter Ordnung vom Geschlechte Eins*, Acta Math. **80** (1948), 223–257. MR **10:**472c

[80] D. Zagier, *The Birch-Swinnerton-Dyer conjecture from a naive point of view*, in Arithmetic Algebraic Geometry, G. van der Geer et al., eds., Prog. in Math. **89**, Birkhäuser, Boston (1991), 377–390. MR **92c:**11063

Department of Mathematics, Stanford University, Stanford, California 94305
*E-mail address*: `rubin@math.stanford.edu`
*URL*: `http://www.math.stanford.edu/~rubin/`

Department of Mathematics, Ohio State University, Columbus, Ohio 43210
*E-mail address*: `silver@math.ohio-state.edu`
*URL*: `http://www.math.ohio-state.edu/~silver/`