BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 44, Number 2, April 2007, Pages 233–254
S 0273-0979(07)01138-X
Article electronically published on February 15, 2007

AVERAGE RANKS OF ELLIPTIC CURVES: TENSION BETWEEN DATA AND CONJECTURE

BAUR BEKTEMIROV, BARRY MAZUR, WILLIAM STEIN, AND MARK WATKINS

Abstract. Rational points on elliptic curves are the gems of arithmetic: they are, to diophantine geometry, what units in rings of integers are to algebraic number theory, what algebraic cycles are to algebraic geometry. A rational point in just the right context, at one place in the theory, can inhibit and control—thanks to ideas of Kolyvagin—the existence of rational points and other mathematical structures elsewhere. Despite all that we know about these objects, the initial mystery and excitement that drew mathematicians to this arena in the first place remains in full force today.

We have a network of heuristics and conjectures regarding rational points, and we have massive data accumulated to exhibit instances of the phenomena. Generally, we would expect that our data support our conjectures, and if not, we lose faith in our conjectures. But here there is a somewhat more surprising interrelation between data and conjecture: they are not exactly in open conflict one with the other, but they are no great comfort to each other either. We discuss various aspects of this story, including recent heuristics and data that attempt to resolve this mystery. We shall try to convince the reader that, despite seeming discrepancy, data and conjecture are, in fact, in harmony.

1. Introduction

Suppose you are given an algebraic curve C defined, let us say, as the locus of zeroes of a polynomial $f(x, y)$ in two variables with rational coefficients. Suppose you are told that C has at least one rational point; i.e., there is a pair of rational numbers (a, b) such that $f(a, b) = 0$. How likely is it that C will have infinitely many rational points?

Such a question, on the one hand, clearly touches on a fundamental issue in diophantine geometry and, on the other, is somewhat meaningless until it is made more precise and appropriately organized. The question we have just asked has distinctly different features when considered for each of the three basic "types" of algebraic curves: curves of (geometric) genus 0, 1, and > 1. Curves of genus 0 possessing a rational point *always* have infinitely many rational points (an easy fact—indeed, even known to the ancient Greeks—since our curve can be written as a conic in this case); curves of genus > 1 never do (a hard fact—indeed a theorem of Faltings [Fal86], for which he received the Fields Medal).

This leaves curves of genus 1 as the unresolved, and thus most interesting, case of the problem we posed, since some elliptic curves, like

$$x^3 + y^3 = 1,$$

Received by the editors January 1, 2006.
2000 *Mathematics Subject Classification.* Primary 11-02, 11D25, 11Y35, 11Y40.

have only finitely many rational points (two, in this instance) and others, like

$$y^2 + y = x^3 - x,$$

have infinitely many, starting with $(0,0)$, $(1,0)$, $(-1,-1)$, $(2,-3)$, $(1/4,-5/8)$, $(6,14)$, $(-5/9,8/27)$, $(21/25,-69/125)$, $(-20/49,-435/343),\ldots$.

If we are to try to extract an actual number between 0 and 1 that will describe "the" probability that a curve of genus 1 possessing at least one rational point has infinitely many, we have to be precise about exactly which curves we want to count and how we propose to "sort" them. Let us agree then (with details later):

- to deal only with the smooth projective models of the curves of genus 1 possessing a rational point (these being precisely the *elliptic curves* defined over $\mathbb{Q}$),
- to count their isomorphism classes over $\mathbb{Q}$, and
- to list them in order of increasing conductor, banking on the theorem that tells us that there are only finitely many isomorphism classes of elliptic curves over $\mathbb{Q}$ with any given conductor.

We can now pose our question. Does

$$P(X) = \frac{\#\{\text{elliptic curves of conductor} \le X \text{ with infinitely many rational points}\}}{\#\{\text{elliptic curves of conductor} \le X\}}$$

converge as X tends to infinity, and if so, what is the limit

$$P = \lim_{X\to\infty} P(X)?$$

In this way we have made our initial question precise:

What is the probability P that an elliptic curve has infinitely many rational points?

It is extraordinary how much vacillation there has been in the past three decades in the various guesses about the answer to this—clearly basic—question. The subject of this paper is to discuss aspects of this drama. Its see-saw history, involving a network of heuristics and conjectures and massive data that seemed not to offer much comfort to the conjecturers, comes in four parts.

(1) **The minimalist conjecture.** The "classical" Birch and Swinnerton-Dyer conjecture (see Section 2) suggests that the probability P described by our question is at least $1/2$. The reason for this is the (heuristic) phenomenon of *parity*: elliptic curves can be sorted into two classes: those of **even parity**, where the "sign in the functional equation of the L-function" is $+1$, and those of **odd parity**, where the "sign" is -1. The (conjectural) probability that an elliptic curve is of even parity is $1/2$, and the same, of course, for odd parity. A consequence of the Birch and Swinnerton-Dyer conjecture is that *all* elliptic curves of odd parity have infinitely many rational points. This is why no one doubts that the probability P described above is $\ge 1/2$.

It has long been a folk conjecture that P is *exactly* $1/2$—let us call this the **minimalist conjecture**. Given the Birch and Swinnerton-Dyer conjecture and the Parity Principle, we have an equivalent, and cleaner, way of stating it as follows:

Conjecture 1.1. *An elliptic curve of even parity has probability zero of having infinitely many rational points.*

This minimalist conjecture might seem appealing purely on the grounds that rational points of elliptic curves are accidental gems of mathematics, and it is hard to imagine that there could be bulk occurrence of these precious accidents—or at least substantially more bulk than is already predicted.

It seems that one could not find such a minimalist conjecture explicitly in the literature until very recently (see [Wat06] and Conjecture 3.4). Nevertheless, for some particular families of elliptic curves (the "quadratic twist" families; see Section 3.3 below) the conjecture is much older. Over a quarter of a century ago, Dorian Goldfeld conjectured that for any elliptic curve E, the probability

$$G(D) = \frac{\#\{\text{quadratic twists up to } D \text{ of } E \text{ with infinitely many rational points}\}}{\#\{\text{quadratic twists up to } D \text{ of } E\}}$$

has $G = 1/2$ as its limit as $D \to \infty$.

(2) **Contrary numerical data.** The next phase of our story involves the accumulation of numerical data regarding this probability P taken over the entirety of elliptic curves and also over various selected families of elliptic curves. The short description of this data (but see the detailed discussion in the body of our article) is the following. Over every data set accumulated so far, about 2/3 (or sometimes more) of the curves in the families being considered have had infinitely many rational points and rather flatly so over the range of conductors involved in the computations; these now include a large set (over 100 million curves) of elliptic curves of conductor $< 10^8$.

(3) **A gross heuristic for special families.** To get the most precise results we change the data set and restrict attention to the probability that a member of even parity of a *quadratic twist family* of elliptic curves has infinitely many rational points. As a refinement to Goldfeld's conjecture, Peter Sarnak gave a heuristic that predicts that among the first D members of such a quadratic twist family (essentially arranged in order of increasing conductor) the number of those with even parity and infinitely many rational points is caught between $D^{3/4-\epsilon}$ and $D^{3/4+\epsilon}$ for any positive ϵ and D sufficiently large. This guess, based on consideration of the size of Fourier coefficients of modular forms of half-integral weight, revived the minimalist conjecture: if Sarnak's estimate is correct, we would indeed have $G = 1/2$ in Goldfeld's conjecture, and even-parity members of a quadratic twist family would have probability zero of having infinitely many rational points.

At this point in our story, there is decided friction between accumulated data which suggests something like 2/3 as the probability for the general member to have infinitely many rational points and a reasoned theoretical expectation, which suggests exactly 1/2 for that probability. Generally, the least we would expect of our data is that they either support our conjectures or overthrow them. Here there was a somewhat more surprising interrelation between data and conjecture, a kind of truce between them: we believed our guesses, we believed the data, and we acknowledged the apparent gap between them.

(4) **A refined heuristic for special families.** More recently, another twist to this story has developed. The work of Katz and Sarnak [KaSa99] regarding symmetry groups of the analogous families of curves over function

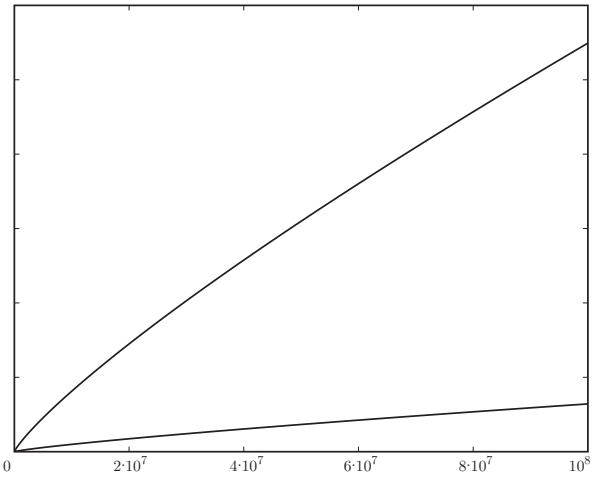

FIGURE 1. Plots of $D^{3/4}\log(D)^{11/8}$ (Upper) and $\Delta^{19/24}(\log\Delta)^{3/8}$ (Lower) up to 10^8

fields[1] gave impetus to the random matrix theory calculations of Keating and Snaith [KeSn00] regarding moments of L-functions and their value distribution. This was then combined with a discretization process by Conrey, Keating, Rubinstein, and Snaith in [CKRS02] to give a more precise guess for the (asymptotic) number of even parity curves with infinitely many rational points in a given quadratic twist family. For example, for the quadratic twist family $y^2 = x^3 - d^2x$, the prediction is that among the first D members of this family, the number of those with even parity and infinitely many rational points is asymptotic to

$$F(D) = c \cdot D^{3/4}\log(D)^{11/8} \tag{1}$$

for some (positive) constant c.

On the one hand, this is a sharpening of the prior heuristic, for $F(D)$ is comfortably sandwiched between $D^{3/4\pm\epsilon}$. On the other hand, we may be in for a surprise when we actually plot the graph of the function $F(D)$. See Figure 1. The striking aspect of the graph in Figure 1 is how "linear" it looks. Indeed, if $F(D)$ were replaced by a linear function with roughly the slope that appears in Figure 1, it would predict something closer to $2/3$ than $1/2$ for the proportion of curves in the family with infinitely many rational points.

Similarly—cf. Section 3.5 below—if we order all elliptic curves by discriminant, one of us (see [Wat06]) has conjectured that the number of even parity elliptic curves with infinitely many rational points and absolute discriminant less than X is asymptotically given by

$$\Phi(X) \;=\; cX^{19/24}(\log X)^{3/8}.$$

See Figure 1.

[1]More recently, Kowalski [KowB] has used monodromy results of Katz to prove upper bounds for average ranks in the function field analogues.

Here, roughly speaking, is where the story is at present, as we will explain in detail in the body of this article. The curious last phase of it, focussing on *special families*, makes it seem now that (a) data for these families are more closely adhering to the refined guess than one might expect, even for relatively small values of the conductor, and (b) a refined guess predicts an asymptotic behavior that is far from linear but within the currently attainable range, which is so close to linear that the numerical evidence elucidating these phenomena (even the very large data sets that computers have amassed) seem indecisive when it comes to distinguishing convincingly between such gross questions as: is the probability closer to 1/2 or to 2/3?

It may very well be that until we actually prove our conjectures, no data that we can accumulate, however massive it may appear, will give even lukewarm comfort to the conjecturers.[2] This conflict raises the question of whether we as mathematicians may, at times, face a situation where the substance we study has one shape asymptotically, and yet all computational evidence elucidating this substance—even up to the very large numbers that computers today, or in our lifetime, can compute—seems consistent with the possibility that the data have a different asymptotic shape.

But, of course, our story will continue. We would hope for

- a refined heuristic that covers the full set of elliptic curves, and not just quadratic twist families;
- an extension of the numerical computation to conductors $< 10^{10}$, which is a range where we may begin to see some significant differences between the graph of $F(D)$ and a linear function;
- a conceptual understanding of how to obtain, by more unified means, this impressive bulk of rational points that we see occurring for even parity elliptic curves, at least for curves of "small" conductor.

We find it useful to compare our question *what is the probability that an elliptic curve has infinitely many points* with some of the other counting problems of current interest. Specifically, consider the problem of *counting quartic fields* and sorting them into classes corresponding to the isomorphy type of the Galois group of their Galois closure. We have to be exceedingly careful when choosing the coefficients of a degree 4 polynomial if we want a root of that polynomial to generate anything other than a field whose Galois group is S_4. Hilbert's irreducibility theorem provides corroboration of this with a proof that if you rank algebraic numbers of degree 4 by the size of the coefficients of their minimal polynomial (monic, over $\mathbb{Q}$), then 100% of them have Galois group S_4. But consider the problem of counting quartic fields (rather than the algebraic numbers that generate them) listed by the size (absolute value) of their discriminant. Counting field extensions of a given field whose Galois closure has its Galois group of a particular isomorphy type has been the subject of a number of precise conjectures (initially [CDO], and then successively refined in [Mal02, Mal04]). Bhargava's remarkable paper [Bha05], which is further

[2] We are reminded of the challenge of Shanks [Sha85, §69] regarding Carmichael numbers: with respect to the conjecture of Erdős that for every $\epsilon > 0$ there are, for sufficiently large X, at least $X^{1-\epsilon}$ Carmichael numbers up to X, Shanks (essentially) noted that the data for small X did not remotely conform to this and proposed giving an explicit X for which there were at least (say) $\sqrt{X}$ Carmichael numbers up to X, suspecting that exhibiting such an X would be much beyond the capabilities of computers.

evidence for these conjectures, proves that when we count quartic fields, nested by absolute discriminant, we do *not* get that 100% of them have Galois group S_4.

Bhargava regards the problem of counting quartic fields as a problem purely in the Geometry of Numbers and *proves* the following theorem:

Theorem 1.2 (Bhargava)**.** *When ordered by absolute discriminant,* a positive proportion *(approximately* 0.17111*) of quartic fields has associated Galois group D_4 (the dihedral group). The remaining approximately* 0.82889 *of quartic fields has Galois group S_4, and the other three transitive subgroups occur with probability* 0 *asymptotically.*

It should be noted that these are Bhargava's percentages when counting fields up to isomorphism; when working in a fixed algebraic closure of the rationals, the percentages are not the same.

We would be more than delighted to see unconditional results of this precision established for questions such as the one motivating this survey article.

Acknowledgment. We thank Armand Brumer, Frank Calegari, Noam Elkies and Oisin McGuinness for stimulating conversations. We used PARI [ABCRZ] and SAGE [SJ05] to compute and analyze the data, and matplotlib [Mpl05] to draw the graphs. We thank Bob Guralnik for references to work about distributions of Galois groups. Similar surveys to this are those of Rubin and Silverberg [RS02] and Kowalski [KowA], the latter of which also relates random matrix theory to the theory of elliptic curves and then discusses questions related to the inability of reconciling experimental data with theoretical asymptotics, particularly with respect to the work of Heath-Brown [HB93] on the 2-Selmer rank of the congruent number curves.

2. Elliptic curves

An *elliptic curve* E over $\mathbb{Q}$ is a projective nonsingular curve defined as the projective closure of the zero locus of an equation of the form

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

with the a_i in $\mathbb{Q}$. The set $E(\mathbb{Q})$ of rational points on E is equipped with an abelian group structure (see [Sil92]).

Via completing the square in the y-variable, translating to eliminate the quadratic x-term, and then re-scaling, we find that the equation (2) is rationally equivalent to exactly one of the form

$$y^2 = x^3 - 27c_4x - 54c_6, \tag{3}$$

with $c_4, c_6, \Delta = (c_4^3 - c_6^2)/1728 \in \mathbb{Z}$ and for which there is no prime p with $p^4 \mid c_4$ and $p^{12} \mid \Delta$. We call Δ the *minimal discriminant* of E. (For example, the minimal discriminant of the curve $y^2 + y = x^3 - x$ mentioned in Section 1 is $\Delta = 37$; also $c_4 = 48$ and $c_6 = -216$ for this curve.)

The *conductor* of an elliptic curve E over $\mathbb{Q}$ is a positive integer $N = N_E$ that is a measure of the nature of the reduction of the elliptic curve modulo the prime divisors of Δ. For example, a prime $p \geq 5$ divides the conductor N only if there is no way of finding another defining equation (2) of E so that when reduced modulo p we obtain an equation over the field $\mathbb{F}_p$ without multiple roots; the maximal power of such a prime p dividing N is 2 and whether it is 1 or 2 is determined by the nature

of the *best* reduction of E modulo p, i.e., whether its defining cubic polynomial has a double or a triple root modulo p. There is a slightly more involved, but elementary, recipe to give the power of the primes 2 and 3 dividing the conductor (see [Tat75]).

Mordell proved in 1922 (see [Mor22]) that the *Mordell-Weil group* $E(\mathbb{Q})$ of rational points on E is a finitely generated abelian group, so $E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$. The integer r is the *rank* of E and is the main statistic that we will discuss below. In contrast, the torsion group is rather well-understood and is thus of less interest.

Let Δ be the minimal discriminant of E. The *L-function* $L(E,s)$ of E is a Dirichlet series given by a simple recipe in terms of the number of points N_p of the reduction of E over $\mathbb{F}_p$ for all primes p. Specifically,

(4)
$$L(E,s) = \prod_{p\nmid\Delta} \frac{1}{1-(1+p-N_p)p^{-s}+p^{1-2s}} \cdot \prod_{p|\Delta} \frac{1}{1-(1+p-N_p)p^{-s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

The integers a_n are defined by expanding the Euler product; e.g., $a_p = p+1-N_p$ and $a_{p^2} = a_p^2 - p$ when $p \nmid \Delta$, etc. As an example, if E is $y^2+y = x^3-x$, then

$$L(E,s) = 1 - \frac{2}{2^s} - \frac{3}{3^s} + \frac{2}{4^s} - \frac{2}{5^s} + \frac{6}{6^s} - \frac{1}{7^s} + \frac{6}{9^s} + \frac{4}{10^s} - \frac{5}{11^s} + \cdots.$$

For any elliptic curve E, the celebrated papers of Wiles [Wil95] and others [BCDT01] imply that $L(E,s)$ extends to an entire analytic function on the complex plane. Moreover these results imply that the completed L-function $\Lambda(E,s) = N^{s/2}\cdot(2\pi)^{-s}\cdot\Gamma(s)\cdot L(E,s)$ satisfies the functional equation

$$\Lambda(E,s) = u_E \cdot \Lambda(E, 2-s),$$

where u_E is either -1 or 1, and is called the *sign in the functional equation for* E. Note that $u_E = 1$ if and only if $L(E,s)$ vanishes to even order at $s=1$.

The classical Birch and Swinnerton-Dyer Conjecture [BSD] asserts that the order of vanishing of $\Lambda(E,s)$ at the point $s=1$ is equal to the rank of the Mordell-Weil group $E(\mathbf{Q})$. In the data regarding *rank* that we will be reporting below, at times the Mordell-Weil rank r has been computed directly by finding r rational points of E that are linearly independent and span a subgroup of finite index in $E(\mathbf{Q})$, and we will refer to this r as the *arithmetic rank* of E. At times, however, what is computed is the apparent order of vanishing of $L(E,s)$ at $s=1$; we refer to this order of vanishing as the *analytic rank* of E. The BSD conjecture asserts that the ranks are in fact equal. We say a curve has *even parity* if the analytic rank is even and *odd parity* if it is odd.

We now state the refined BSD conjecture for curves of rank 0. When E is given by (3), the real period Ω_{re} is, up to easily determined factors of 2 and 3, equal to the integral $\int_{E(\mathbb{R})} dx/y$. For a prime p, the Tamagawa number Ω_p is the index in $E(\mathbb{Q}_p)$ of the subgroup of p-adic points that reduce to a nonsingular point in $E(\mathbb{F}_p)$.

Conjecture 2.1 (Birch and Swinnerton-Dyer)**.** *If* $L(E,1) \neq 0$*, then*

$$L(E,1) = \frac{\Omega(E)\cdot \#Ш(E)}{\#E(\mathbb{Q})_{\text{tor}}^2}, \tag{5}$$

where $Ш(E)$*, the* Shafarevich-Tate group *of* E*, is a certain (mysterious) group associated to* E *(it measures the failure of a local-global principle), and*

$$\Omega(E) = \Omega_{\text{re}} \cdot \prod_p \Omega_p.$$

Since $L(E,1) \neq 0$, the group Ш(E) is known to be finite [Kol88] of order a perfect square [Cas62].

For any $r = 0, 1, 2, \ldots$ the question we now may ask is: what percentage of elliptic curves (nested according to size of conductor) have rank r? More correctly, we should ask: do these percentages exist, and if so what are they?

3. Conjectures

One fairly firm anchor in the study of elliptic curves is a principle that goes under the heading of parity. This principle is still only conjectural but is amply confirmed numerically in our accumulated data, and we also have theoretical reasons to believe it.[3] The parity principle is that 50% of the members of any of the sets of elliptic curves we will be considering have even parity and 50% have odd parity (under reasonable orderings). So by BSD, 50% should have even rank and 50% should have odd rank.

In general terms, the minimalist principle proclaims that from the rough viewpoint of percentages, there are as few rational points on elliptic curves as is possible, given the constraint of the parity principle. That is, 50% of the members of any of the families of elliptic curves we will be considering have rank $r = 0$, and 50% have rank $r = 1$, and the remaining ranks $r \geq 2$ account for 0% of the family.

As one thing or another comes to light in the subject, the minimalist position is sometimes favored and sometimes not. For certain special families of elliptic curves, this minimalist conjecture has long been in print and has had a wild ride in terms of its being believed and doubted.

3.1. **The form of the conjectures.** There are two types of asymptotic conjectures that we encounter in discussions regarding rank statistics. The first we might call a *rough conjecture* where it is asserted, or conjectured, for a certain collection $\mathcal{F}(x)$ of items indexed by a variable x that there is an *exponent* a and a function $x(\epsilon)$ such that the cardinality of $\mathcal{F}(x)$ is bounded above by $x^{a+\epsilon}$ and below by $x^{a-\epsilon}$ for any positive ϵ and any $x \geq x(\epsilon)$.

We also will be discussing *fine conjectures* where such collections $\mathcal{F}(x)$ will be conjectured to have asymptotic estimates of the form

$$\#\mathcal{F}(x) \sim x^a \cdot (\log x)^b \cdot c,$$

for constants a, b, c; the delicacy, of course, of these constants is inversely related to their alphabetical order.

What seems to be a pattern is that the exponent a, appearing in both rough and fine versions in specific contexts under discussion, can usually be guessed by more old-fashioned heuristics. But—at present, at least—the on-going work regarding random matrix eigenvalues is the only source of heuristics that leads us to formulate specific "fine conjectures" regarding ranks, and specifically for guesses regarding the exponent b of the $\log x$ term. The fact that the graphs of some of the specific concoctions of the form $x^a \cdot (\log x)^b \cdot c$ predicted by random matrix statistics can look deceivingly like x^1 even though $a < 1$ (and for a significant range of the variable x) is one of the curiosities of our story.

[3] In particular, the sign of the functional equation is a product of local signs for primes $p|\Delta$, each of which is ± 1 with equal proportion. See the work of Helfgott [Hel04] for the latest results.

3.2. **Random matrix statistics.** Originally developed in mathematical physics, random matrix theory [Meh04] has now found many applications in number theory, the first being the oft-told story [Gr] of Dyson's remark to Montgomery regarding the pair-correlation of zeros of the Riemann ζ-function. Based on substantial numerical evidence, random matrix theory appears to give reasonable models for the distribution of L-values in families, though the issue of what constitutes a proper "family" can be delicate. The work of Katz and Sarnak [KaSa99] regarding families of curves over function fields implies that for quadratic twists of even parity, we should expect orthogonal symmetry with even parity. Though we have no function field analogue when considering all curves of even parity, we still brazenly assume (largely from looking at the sign in the functional equation) that the symmetry is orthogonal with even parity. What this means is that we want to model properties of the L-function via random matrices taken from $\mathrm{SO}(2M)$ with respect to Haar measure for an appropriate value of M.[4] We suspect that the L-value distribution is approximately given by the distribution of the evaluations at 1 of the characteristic polynomials of our random matrices. In the large, this distribution is determined entirely by the symmetry type, while finer considerations are distinguished via arithmetic considerations.

Via the moment conjectures [KeSn00] of random matrix theory and then using Mellin inversion, we expect that (for some constant $c > 0$)

$$\text{Prob}[L(E,1) < t] \sim ct^{1/2}(\log N)^{3/8} \qquad \text{as} \qquad t \to 0, \tag{6}$$

when the curves E are taken from a suitable family.

3.3. **Conjectures about twist families.** Let E be an elliptic curve over $\mathbb{Q}$ defined by an equation $y^2 = x^3 + ax + b$. The *quadratic twist* E_d of E by a nonzero integer d is the elliptic curve defined by $y^2 = x^3 + ad^2x + bd^3$. The twist E_d is isomorphic to E over the field $\mathbb{Q}(\sqrt{d})$, and (when d is a fundamental discriminant relatively prime to N_E) the conductor of E_d is $d^2 \cdot N_E$.

Conjecture 3.1 (Goldfeld, [Gol79])**.** *The average rank of the curves E_d is $\frac{1}{2}$, in the sense that*

$$\lim_{D\to\infty} \frac{\sum_{|d|<D} \text{rank}(E_d)}{\#\{d : |d| < D\}} = \frac{1}{2}.$$

(Here the integers d are fundamental discriminants.)

There are many conditional and unconditional results regarding Goldfeld's conjecture. For a survey, see the papers of Rubin and Silverberg [RS02, Sil01].

The values $L(E_d, 1)$ of quadratic twists E_d of a given curve E essentially appear in a single object as the coefficients (weighted by the real period and Tamagawa numbers) of an integral modular form g_E of weight 3/2 (this follows from work of Waldspurger; see [Wal81]). In particular, for many d, we have that $L(E_d, 1) = 0$ precisely when the dth (or $-d$th, depending on the case) coefficient of g_E is zero. This object g_E does not give us values of $L(E_d, 1)$ for all d but does provide a large proportion of them. The Ramunajan conjecture for modular forms implies that the coefficients of g_E should be bounded by about $|d|^{1/4}$, and so if we assume a coefficient distribution that is somewhat uniform, we approximate the count $F(D)$ of quadratic twists up to D with even parity that have $L(E_d, 1) = 0$ by $\sum_{|d|<D} 1/|d|^{1/4}$.

[4]Here we wish the mean density of zeros of the L-functions to match the mean density of eigenvalues of our matrices, and so, as in [KeSn00], we should take $2M \approx 2 \log N$.

Sarnak's rough heuristic asserts that this count lies between $D^{3/4-\varepsilon}$ and $D^{3/4+\varepsilon}$. Using random matrix theory, the paper [CKRS06] gets the refined heuristic that

$$F(D) \sim D^{3/4} \cdot (\log D)^b \cdot c,$$

where there are four possibilities for b (depending on the Galois group of the cubic polynomial $x^3 - 27c_4x - 54c_6$) and c is still mysterious.

In [CKRS06], Rubinstein used weight 3/2 forms to give data about $L(E_d, 1)$ for over 2000 elliptic curves E. For each of these he computed $L(E_d, 1)$ for a substantial subset of the quadratic twists by fundamental discriminants d with $|d| < 10^8$. (For example, for the curve E given by $y^2 + y = x^3 - x^2$ of conductor 11, the only twist E_{-d} of even parity with $L(E_{-d}, 1) = 0$ for $3 < d < 91$ is $d = 47$.) The data of Rubinstein agree fairly well with predictions such as (1).

It is possible, however, to ameliorate the effects of b and c (and the 3/4-exponent for that matter) via the ratio conjecture of [CKRS02]. Fix an elliptic curve E and a modulus q, prime for simplicity. Consider the d with $\gcd(q, d) = 1$ for which E_d has even parity and $L(E_d, 1) = 0$, and divide these into two classes depending on whether d is a square modulo q. The ratio conjecture asserts that the (asymptotic) ratio of the sizes of these two classes is $\left(\frac{q+1+a_q}{q+1-a_q}\right)^{-1/2}$, where the exponent $-1/2$ comes from the arguments leading to (6). In essence, the d's that are squares should give $c_S X^{3/4} (\log X)^{b_E}$, while those that are not should yield $c_N X^{3/4} (\log X)^{b_E}$, and [CKRS02] predicts c_S/c_N via a clever methodology. The data match this prediction fairly well,[5] especially for $a_q = 0$, when the convergence is quite rapid.

We can also consider other twist families. For example, Kramarz and Zagier [ZK87] considered cubic twists $x^3 + y^3 = m$ of the Fermat cubic[6] $x^3 + y^3 = 1$ and found in their data that 23.3% of the curves with even parity have rank at least 2 and 2.2% of those with odd parity have rank at least 3. One of the authors of the present article [Wat04] and independently Fermigier (unpublished) have followed up on these computations. Also, Patricia Quattrini (Universidad de Buenos Aires) as part of her thesis work (to appear in *Experimental Mathematics*) did some extensive calculations of the analytic rank for the curves $y^2 = x^3 - nx$. As in the Kramarz-Zagier case, the percentage of curves with analytic rank ≥ 2 was in the 20% range but did seem to be going down. Similar computations [DFK04] have also been undertaken for twists by other (complex) Dirichlet characters, which are related to ranks over number fields. Finally, Fermigier [Fer96] investigated specializations of various (about 100) elliptic curves defined over $\mathbb{Q}(t)$ and found that typically 10%-20% of the specializations had excess rank that could not be explained simply from parity.

3.4. **Conjectures when counting all elliptic curves.** Before we can count curves with even parity and infinitely many points, we might first take a step back and just try to count curves. Though before we ordered curves by conductor, when deriving heuristics it is often easier to sort by discriminant. Indeed, Brumer and McGuinness [BM90, §5] state a heuristic estimate for the number of minimal discriminants of elliptic curves up to a given bound:

[5] In [CPRW] a secondary term is computed, and the fit to the data becomes even better. The paper [Wat04] notes similar data for cubic twists, while [CRSW] analyses the data of Elkies for the congruent number curve in the odd parity case.

[6] Note that this is rationally isomorphic to the elliptic curve in the form (3) given by the equation $Y^2 = X^3 - 54 \cdot 5832$ via the map $(X, Y) = \big(108/(x+y), 972(y-x)/(y+x)\big)$.

Conjecture 3.2 (Brumer-McGuinness)**.** *We have the following estimates for the number of positive or negative minimal discriminants of elliptic curves of absolute value at most X (respectively):*

$$A_\pm(X) \sim \frac{\alpha_\pm}{\zeta(10)} X^{5/6}$$

where $\alpha_+ = 0.4206\ldots$ and $\alpha_- = \sqrt{3}\alpha_+ = 0.7285\ldots$ are given by

$$\alpha_\pm = \frac{\sqrt{3}}{10} \int_{\pm 1}^{\infty} \frac{du}{\sqrt{u^3 \mp 1}}.$$

Brumer and McGuinness say little about their derivation of this heuristic but remark that it suggests a heuristic for prime discriminants that matches very well with their data. We can derive their heuristic by counting lattice points in the (c_4, c_6)-plane, restricting to congruence classes modulo powers of 2 and 3 to ensure that Δ is integral. Because $\Delta = (c_4^3 - c_6^2)/1728$, we heuristically have that $A_+(X)$ is proportional to the area of the region $0 < c_4^3 - c_6^2 < 1728X$, and similarly with $A_-(X)$. This gives $\alpha_\pm X^{5/6}$; the extra factor of $\zeta(10)$ comes about since we need (for $p \geq 5$, and similarly for $p = 2, 3$) to eliminate (c_4, c_6) pairs with $p^4 | c_4$ and $p^6 | c_6$. For a more complete derivation of the value of $\alpha_\pm$ see [Wat06].

We expect that half of these curves have even parity. Now we wish to estimate how many of the curves with even parity have $L(E, 1) = 0$.

3.5. **Rank conjectures for all curves.** To make use of the heuristic (6), we introduce a discretization process. We want to connect $L(E, 1)$ with the *winding number* $W = W(E) = |L(E, 1)/\Omega_{\mathrm{re}}|$ (see [MSD74, §2.2])[7] and measure the likelihood that W is 0. Ignoring torsion (so that W is an integer) we are trying to estimate the probability that $L(E, 1) < \Omega(E)$. If we consider *only* elliptic curves for which $\Omega(E)$ lies in a fixed interval $c_1 < \Omega(E) < c_2$, then we get a neat estimate of this probability. So this line of reasoning leads one to try to deal with the statistics of the invariant $\Omega(E)$ for varying E.

Next, we simplify matters by restricting to curves with prime positive discriminant (and even parity). Three nice things about these curves are that (except for a sparse subset): all have trivial torsion, all have $\Omega_p = 1$ for all (finite) primes p, and all have that $N = \Delta$. The idea of our discretization is that W can take on only integral values (note that when $W \neq 0$, Conjecture 2.1 implies that $W = \#Ш(E)$, which is a perfect square, but we will not use this). Thus, in terms of our probability distribution of L-values, we get that $L(E, 1) < \Omega_{\mathrm{re}}$ if and only if $L(E, 1) = 0$; this is because

$$0 \leq W = \left| \frac{L(E, 1)}{\Omega_{\mathrm{re}}} \right| < 1$$

and W is an integer.

Putting $t = \Omega_{\mathrm{re}}$ and $N = \Delta$ in (6) we get:

Heuristic 3.3. *A curve with positive prime discriminant and even parity has infinitely many points with probability $c\Omega_{\mathrm{re}}^{1/2}(\log \Delta)^{3/8}$.*

Using the above, the number $B(X)$ of such curves up to X with even parity and infinitely many points is estimated by integrating $\int\int c\Omega_{\mathrm{re}}^{1/2}(\log \Delta)^{3/8-1} du_4 du_6$ over

[7] We could relate W to the Birch and Swinnerton-Dyer conjecture, but the (topological) winding number interpretation is rigorous and sufficient for our needs.

the region $|u_4^3 - u_6^2| < 1728X$, where the "-1" in the exponent of $\log \Delta$ comes about from the prime number theorem. Also, the integral makes sense because Ω_{re} and Δ are smooth functions of c_4 and c_6; that is, we can define Ω_{re} and Δ for c_4 and c_6 that are not necessarily integral (or even rational). So, similar to the above discussion of the Brumer-McGuinness heuristic, we have replaced a (weighted) lattice-point problem with the area of a region in a plane, weighted by a factor depending on the real period and the discriminant (and congruence restrictions as before).

We expect that the typical size[8] of the real period Ω_{re} is $1/|\Delta|^{1/12}$, and so, from the above heuristic,[9] we thus get a crude estimate that $B(X)$ is of size $X^{19/24}$.

The preprint [Wat06] handles more of the details and considers all curves, not only those with prime discriminant. Indeed, if $F(X)$ is the number of elliptic curves E with even parity and $L(E,1) = 0$ and $|\Delta| \le X$, then [Wat06] predicts

$$F(X) \sim c_1 X^{19/24} (\log X)^{3/8},$$

with a computable[10] positive constant c_1.

In any case, since we expect $cX^{5/6}$ curves with $|\Delta| \le X$, this heuristic says that 100% of the even parity curves have rank 0.

The best known results (conditional on a Generalized Riemann Hypothesis and a Parity Principle analogue) on nonvanishing of even parity L-functions appear in the work of Young [YouB], and results about average (analytic) ranks and their relation to random matrix theory appear in [YouA].

3.6. **Ordering by conductor.** The predictions become more difficult to derive when we order by conductor instead of discriminant, as this introduces arithmetic considerations related to the ABC-conjecture (see [GT02]) in the accounting. Even giving a heuristic for the number $C(X)$ of curves of conductor less than X is nontrivial. The preprint [Wat06] asserts heuristic asymptotics of $c_2 X^{5/6}$ for $C(X)$ and similarly $c_3 X^{19/24} (\log X)^{3/8}$ for the number of rank 2 curves with conductor less than X. However, Cremona's data (see below) might suggest linear growth for $C(X)$. In any event, in all cases we expect that 100% of the even parity curves have rank 0. Despite our lack of numerical confirmation, we label these guesses as "conjectures":

Conjecture 3.4. *The number of even parity elliptic curves with infinitely many rational points and absolute discriminant less than X is asymptotically given by $c_1 X^{19/24} (\log X)^{3/8}$ for some positive computable constant c_1 as $X \to \infty$. If we replace "absolute discriminant" by "conductor", we get an asymptotic of $c_3 X^{19/24} (\log X)^{3/8}$. In particular, asymptotically almost all elliptic curves with even parity have finitely many rational points.*

See [Wat06] for more details.

[8] This is also an upper bound; the ABC conjecture says Ω_{re} is never much smaller than $1/|\Delta|^{1/2}$.

[9] Note that random matrix theory is largely used to determine the power of logarithm in this heuristic. The cruder estimate of $X^{19/24}$ can alternatively be obtained by assuming that the winding number is a random square integer of size up to $1/\Omega_{\mathrm{re}}$ (this is similar to Sarnak's heuristic); indeed this was probably known to Brumer and McGuinness, as they conclude their paper with

> *While our data may seem massive, $N = 10^8$ is not sufficient to distinguish growth laws of $\log\log N$, $N^{1/12}$ or $N^{1/24}$ from constants. So we have to be cautious in formulating conjectures based on the numerical evidence.*

[10] Our imprecise discretization might make the computed value of c_1 not too relevant.

4. Data

> The opinion had been expressed that, in general, an elliptic curve might tend to have the smallest possible rank, namely 0 or 1, compatible with the rank parity predictions of Birch and Swinnerton-Dyer. We present evidence that this may not be the case. [...] This proportion of rank 2 curves seemed too large to conform to the conventional wisdom. – Brumer and McGuinness [BM90]

In [BM90], Brumer and McGuinness considered over 310,000 curves of prime conductor $\leq 10^8$. In this section we discuss extensions of their data and answer in the affirmative that there is a similar large proportion of rank 2 curves for composite conductor $\leq 10^8$ and for prime conductor $\leq 10^{10}$. More precisely, we consider 136,832,795 curves of all conductors $\leq 10^8$ and 11,378,911 curves of prime conductor $\leq 10^{10}$. The results of the rank computation we describe are similar to those of Brumer and McGuinness, which appear to suggest that if one orders all elliptic curves over $\mathbb{Q}$ by conductor, then the average rank is bigger than 0.5. However, as discussed above, we conjecture that the average rank is 0.5.

4.1. **Brumer-McGuinness.** In [BM90], Brumer and McGuinness found, by thousands of hours of computer search, 311,219 curves of prime conductor $\leq 10^8$. For 310,716 of these curves they computed the probable rank by a combination of point searches and computation of apparent order of vanishing of L-functions. Table 1 (expanded from [BM90]) summarizes the rank distribution that they found.[11]

Table 1. Brumer-McGuinness Rank Distribution

Rank	0	1	2	3	4	5
$\Delta > 0$	31748	51871	24706	5267	377	0
$\Delta < 0$	61589	91321	36811	6594	427	5
Total # Curves	93337	143192	61517	11861	804	5
Proportion	0.300	0.461	0.198	0.038	0.0026	0.00002
Proportion $\Delta > 0$	0.279	0.455	0.217	0.046	0.0033	0.00000
Proportion $\Delta < 0$	0.313	0.464	0.187	0.034	0.0022	0.00003

In Table 1, note that curves with $\Delta > 0$ are more likely to have large rank. Let $r_\varepsilon(X)$ be the average rank of elliptic curves in [BM90] with conductor at most X and discriminant sign ε. They observe that in their data, r_+ climbs to 1.04 and r_- climbs to 0.94, and they remark that *"An interesting phenomenon was the systematic influence of the discriminant sign on all aspects of the arithmetic of the curve."* The more extensive computations do *not* always find this to be the case; see, in particular, Figure 3, where the graphs split by discriminant cross.

4.2. **The Stein-Watkins database.** Brumer and McGuinness fixed the a_1, a_2, a_3 invariants (12 total possibilities, as (2) can be modified first to be integral, and then to ensure that $a_1, a_3 \in \{0, 1\}$ and $|a_2| \leq 1$) and then searched for a_4 and a_6 that made $|\Delta|$ small. Stein and Watkins [SW02] broke the c_4 and c_6 invariants into

[11] Some of their counts were computed incorrectly (for instance, they used only 4,000 terms of the L-series and thus misidentified 11 curves of rank 0 as having rank 2), but this has little influence on the overall statistics.

congruence classes and then found small solutions to $c_4^3 - c_6^2 = 1728\Delta$, with c_4, c_6 minimal in the sense of (3). There is little theoretical advantage in this approach; more computing power and disk space were the main advances in [SW02]. Stein and Watkins searched for curves with prime conductor up to 10^{10}, and for composite conductor chose $|\Delta| < 10^{12}$ and $N \leq 10^8$ as search bounds, and then included isogenous curves and twists (with $N \leq 10^8$) of the curves they found.

4.3. **Completeness of the databases.** Note that neither the method of Brumer-McGuinness nor Stein-Watkins is guaranteed to find all curves of prime (absolute) discriminant up to a given bound (indeed, it is more likely that they miss a few curves), but we think that their data sets are reasonable surrogates and should exhibit validity when compared to the predictions of the theoretical model.

For curves of composite conductor, the Stein-Watkins database is much more likely to miss curves. Here the comparison is to the data set of Cremona [Cre], who used the algorithms of [Cre97] and the modularity theorem of [BCDT01] to find *every* elliptic curve of conductor up to 120000. Cremona found 782, 493 curves up to conductor 120000. In the Stein-Watkins computation, they found 614, 442 curves of conductor up to 120000, so they found over 78.5% of the curves. The first case in which Cremona has a curve and Stein-Watkins do not is the curve $y^2 + xy + y = x^3 - 7705x + 1226492$ of conductor 174, which has discriminant $-621261297432576 = -2^{11} \cdot 3^{21} \cdot 29$, whose absolute value is substantially larger than 10^{12}. The conductors up to 500 where they miss curves are

$$174, 222, 273, 291, 330, 354, 357, 390, 420, 442, 462, 493.$$

Figure 2 shows the proportion of the number of curves in the Stein-Watkins database to the number of curves in Cremona's database, as a function of the conductor. The rank distribution of Cremona's curves is given in Table 2. The average rank for Cremona's curves is about 0.688. This is smaller than the average rank in other data sets we consider (and is probably explainable via the real period considerations of the last section), but we prefer to highlight the results from other data sets.

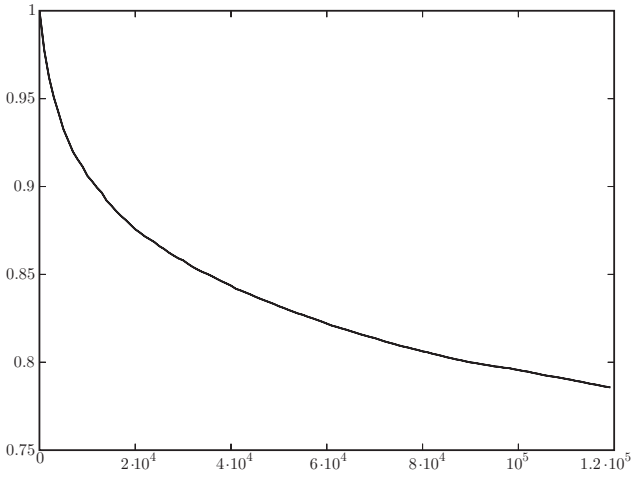

FIGURE 2. Proportion of Cremona's Curves Obtained by Stein and Watkins for $N \leq 120000$

TABLE 2. Rank Distribution of All Curves of Conductor ≤ 120000

Rank	0	1	2	3
Proportion	0.404	0.505	0.090	0.001
Proportion $\Delta > 0$	0.408	0.503	0.087	0.001
Proportion $\Delta < 0$	0.401	0.506	0.092	0.001

As noted above, when ordering by conductor there is presently no consensus guesstimate for the number of curves up to X. Cremona has commented that there is approximately linear growth in the number of curves of conductor less than 120000, and extrapolating this gives a prediction close to 650 million for the number of curves with $N \leq 10^8$.

D. J. Bernstein suggested that we try to quantify the completeness of the Stein-Watkins database by considering what percentage of Cremona's curves would be obtained by using their search methods with a smaller discriminant bound. That is, for a parameter B, if we find all curves with $N \leq B^2$, $|\Delta| \leq B^3$, and $c_4 \leq 100 \cdot (12B)^2$, and then take all isogenous curves and twists of these with conductor less than B^2, what percentage of Cremona's curves do we obtain? With $B = 300$, we get 246,532 curves, while Cremona has 592,519 curves of conductor $\leq 90000 = 300^2$, so we get about 42%. Applying this percentage to the Stein-Watkins database with $B = 10^4$ suggests that there are about 325 million elliptic curves with conductor less than 10^8. So the two guesses differ by a factor of two, exemplifying our ignorance on so basic an issue.

5. Average ranks: graphs of data

This section contains graphs that at a glance suggest that the minimalist principle is contradicted by the data for curves of conductor $\leq 10^8$; indeed, particularly in Figure 3, we see that *the average rank is increasing!* However, for prime conductor $\leq 10^{10}$ the average rank drops, though only slightly from 0.978 to 0.964. With some imagination, the distribution of rank for prime conductors might appear to support the minimalist conjecture that the average rank is 0.5. Table 3 gives the average rank for various collections of curves that are described in more detail elsewhere in this paper and section.

TABLE 3. Average Ranks

Cremona's curves of conductor ≤ 120000	0.688
All Stein-Watkins curves of conductor $\leq 10^8$	0.865
Brumer-McGuinness curves of prime conductor $\leq 10^8$	0.982
Stein-Watkins curves of prime conductor $\leq 10^{10}$	0.964
Selected curves of prime conductor near 10^{14} with $\Delta < 0$	0.869
Selected curves of prime conductor near 10^{14} with $\Delta > 0$	0.938

In this section when we write elliptic curves with property P, we mean elliptic curves in the Stein-Watkins database with property P.

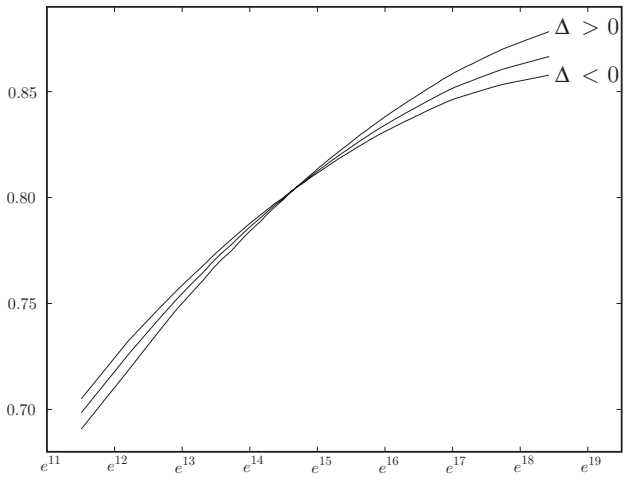

FIGURE 3. Average Rank of Stein-Watkins Curves of Conductor $\leq 10^8$

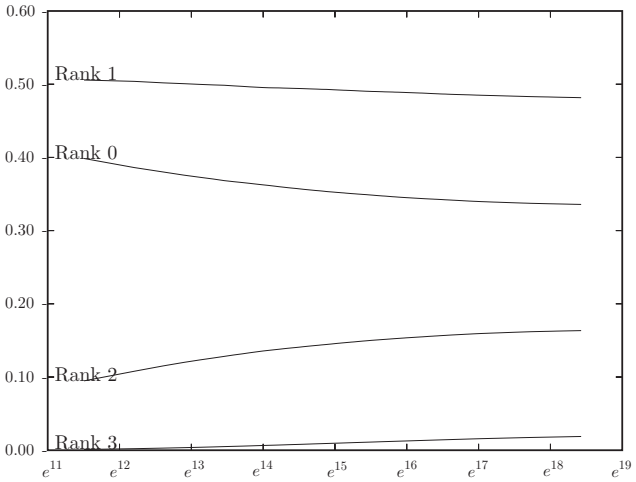

FIGURE 4. Rank Distribution of Stein-Watkins Curves with $N \leq 10^8$

5.1. **Curves ordered by conductor.** The average rank of all Stein-Watkins curves with conductor $\leq 10^8$ is about 0.87. Figure 3 gives the average rank as a function of log of the conductor and also the average rank for curves of positive and negative discriminant. We created this graph by computing the average rank of curves of conductor up to $n \cdot 10^5$ for $1 \leq n \leq 1000$. Figure 4 graphs the proportion of curves with each rank 0, 1, 2, and 3 as a function of log of the conductor, all on a single graph. The overall rank proportions are in Table 4.

5.2. **Prime conductor curves.** The average rank for the curves of prime conductor $\leq 10^{10}$ is about 0.964; see Table 5 for the rank distribution. Figure 5 plots the average rank of curves of prime conductor $\leq 10^{10}$ as a function of log of the conductor. Note that here the average ranks are decreasing, unlike in Figure 3.

TABLE 4. Rank Distribution for Stein-Watkins Curves with $N \leq 10^8$

Rank	0	1	2	3	≥ 4
Proportion	0.336	0.482	0.163	0.019	0.000
Proportion $\Delta > 0$	0.331	0.480	0.168	0.020	0.000
Proportion $\Delta < 0$	0.339	0.482	0.160	0.018	0.000

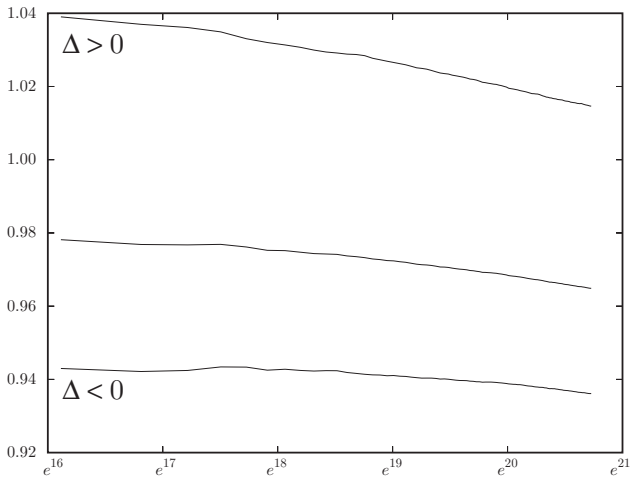

FIGURE 5. Average Rank of Curves with Prime $N \leq 10^{10}$

TABLE 5. Rank Distribution for Prime Conductor $\leq 10^{10}$

Rank	0	1	2	3	≥ 4
Proportion	0.309	0.462	0.188	0.037	0.004
Proportion $\Delta > 0$	0.291	0.457	0.204	0.044	0.004
Proportion $\Delta < 0$	0.320	0.465	0.179	0.033	0.003

Figure 6 graphs the proportion of curves with prime conductor with each rank 0, 1, 2, and 3 as a function of log of the conductor.

5.2.1. *An experiment.* The data of [BM90] and [SW02] for curves of prime conductor up to 10^8 and 10^{10} show very little drop in the observed average rank. To investigate the possibility that the average rank might not decrease much below 0.964, we chose a selection of curves with prime conductor of size 10^{14}. It is nontrivial to get a good data set, since we must take congruence conditions on the elliptic curve coefficients and the variation of the size of the real period into account; see [Wat06] for more details on how to account for this.

Our data sets contained 89,913 curves of positive prime discriminant and 89,749 similar curves with negative discriminant, with $|\Delta|$ near 10^{14} for all the curves. It then took a few months to compute the analytic rank for these curves. We found that for positive discriminant the average analytic rank is approximately 0.937 and for negative discriminant it is approximately 0.869 (see Table 6 for more details). Note that this is significantly less than the average rank found in [BM90]

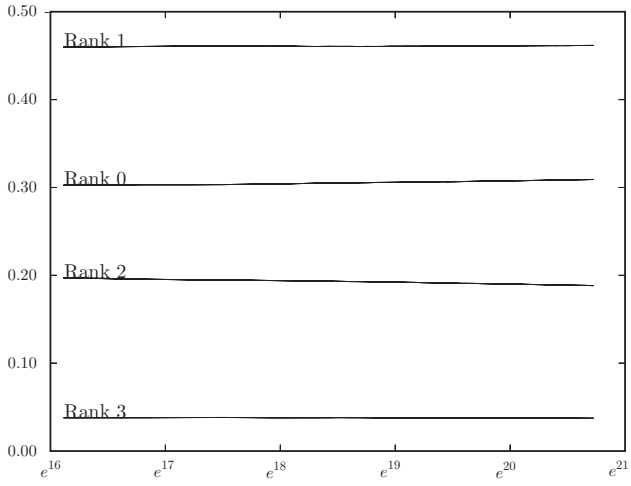

FIGURE 6. Rank Distribution of Curves with Prime $N \leq 10^{10}$

and [SW02]. It could be said that this is the strongest numerical evidence yet for the Minimalist Conjecture, though it is still very weak. Incidentally, the largest rank found in any of these data sets is 6.

TABLE 6. Rank Distribution for a Selection of Curves with Prime Conductor near 10^{14}

Rank	0	1	2	3	≥ 4
Proportion $\Delta > 0$	0.319	0.467	0.176	0.034	0.004
Proportion $\Delta < 0$	0.343	0.475	0.154	0.025	0.002

Let $f(\Delta)$ be the "probability" that $L(E,1) = 0$ for an even parity curve of discriminant near Δ for Δ positive. For example, Tables 5 and 6 suggest that

$$f(10^{10}) \sim \frac{0.204 + 0.004}{0.291 + 0.204 + 0.004} = 0.417\ldots$$
$$f(10^{14}) \sim \frac{0.176 + 0.004}{0.319 + 0.176 + 0.004} = 0.361\ldots.$$

(Note that we approximated $f(10^{10})$ using data for all $|\Delta| < 10^{10}$.) Motivated by the discussion in Section 3, we might heuristically approximate this probability function by $\hat{f}(\Delta) = c \cdot (\log \Delta)^{3/8}/\Delta^{1/24}$, where $\Delta^{1/24}$ comes about as the square root of the "typical" real period. The value of $\hat{f}(10^{10})/\hat{f}(10^{14})$ is about 1.29, which is not ridiculously far from the observed ratio of

$$\frac{f(10^{10})}{f(10^{14})} \sim \frac{0.417}{0.361} \sim 1.16.$$

5.3. **Variants.** We also carried out computations similar to the ones described above when counting isogeny classes instead of isomorphism classes of curves (isogeny is a coarser equivalence relation than isomorphism, grouping together curves between which there is a finite degree morphism). In our data the average size of isogeny classes for all curves of conductor up to X converges reasonably

quickly to 1 (Duke has shown [Duk97] that this is indeed the case under a different ordering). Thus the data and graphs look almost identical to those presented above. Table 7 gives rank data for other subsets of the Stein-Watkins database of curves of conductor $\leq 10^8$. In the table, "has CM" refers to curves that have complex multiplication, i.e., whose endomorphism ring (over $\mathbb{C}$) is bigger than $\mathbb{Z}$.

TABLE 7. Distribution of Rank in Various Subsets of the Stein-Watkins Database with Conductor $N < 10^8$

Description	**Number**	**Rank 0**	**Rank 1**	**Rank 2**	**Rank ≥ 3**
All curves	136832795	0.336	0.482	0.163	0.019
All isogeny classes	115821258	0.328	0.480	0.171	0.021
Has Isogeny	38599162	0.375	0.492	0.125	0.008
Has nontrivial torsion	35249448	0.373	0.492	0.127	0.008
N squarefree	21841534	0.296	0.467	0.202	0.034
Has full 2-torsion	1674285	0.392	0.496	0.107	0.005
N is square	538558	0.416	0.496	0.084	0.004
N is prime	312435	0.303	0.460	0.197	0.041
Has 3-torsion	184590	0.422	0.498	0.078	0.002
Has CM	135226	0.411	0.498	0.087	0.005
N is prime squared	517	0.439	0.480	0.072	0.010

6. How can we *systematically* account for the Mordell-Weil rank we have already computed?

Forget all questions of asymptotics. Consider only the curves of prime conductor up to 10^{10} in our data. Is there an argument other than just computing ranks for each of the elliptic curves in the databases—is there a pure thought heuristic—that explains why we are witnessing so much Mordell-Weil rank? In a sense, these rational points are both analogous, and not analogous, to the physicist's dark matter.[12] This large mass of rational points for elliptic curves of prime conductor $\leq 10^{10}$ is palpably there. We aren't in the dark about that. We are merely in the dark about how to give a satisfactory account of it being there, other than computing instances one after another.

We are, so to speak, just at the very beginning of this story.

About the authors

Baurzhan Bektemirov is a mathematics major at Harvard College in the class of 2008.

Barry Mazur is the Gerhard Gade University Professor at Harvard University.

William Stein is currently an associate professor at the University of Washington. He has held positions at Harvard and at San Diego.

Mark Watkins is a postdoctoral associate in the Mathematical Physics Group at the University of Bristol (UK). He previously worked at Penn State and frequently

[12] The original idea is due to Zwicky [Zwi33]; recent SDSS and WMAP data [Teg04] seem to confirm its existence, though there are still some doubters (such as [Bek04]).

visits the MAGMA computer algebra group in Sydney. He was an invited speaker at the 2004 Algorithmic Number Theory Symposium (ANTS-VI) in Burlington, VT.

References

[ABCRZ] B. Allombert, K. Belabas, H. Cohen, X. Roblot, and I. Zakharevitch, `PARI/GP`, computer software, `pari.math.u-bordeaux.fr`

[Bek04] J. D. Bekenstein, *An alternative to the dark matter paradigm: relativistic MOND gravitation.* Invited talk at the 28th Johns Hopkins Workshop on Current Problems in Particle Theory, June 2004, Johns Hopkins University, Baltimore. Published online in JHEP Proceedings of Science, `arxiv.org/astro-ph/0412652`

[Bha05] M. Bhargava, *The density of discriminants of quartic rings and fields*, Annals of Mathematics **162** (2005), no. 2, 1031–1063. Can be obtained online: Project Euclid Identifier is `euclid.annm/1134163091`. MR2183288

[BSD] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I, II,* J. Reine Angew. **212** (1963), 7–25; **218** (1965), 79–108. MR0146143 (26:3669), MR0179168 (31:3419)

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). Online at `www.ams.org/journal-getitem?pii=S0894034701003708`. MR1839918 (2002d:11058)

[BM90] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382; data available from `oisinmc.com/math/310716`. MR1044170 (91b:11076)

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

[CDO] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Counting discriminants of number fields of degree up to four*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 269–283. MR1850611 (2002g:11148)

[CKRS02] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and 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), edited by M. A. Bennett, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand and W. Philipp; A K Peters, Natick, MA (2002), 301–315. Available online at `arxiv.org/math.NT/0012043`. MR1956231 (2003m:11141)

[CKRS06] ———, *Random matrix theory and the Fourier coefficients of half-integral weight forms*, Experimental Math. **15** (2006), no. 1. Online at `arxiv.org/math/0412083`. MR2229387

[CPRW] J. B. Conrey, A. Pokharel, M. O. Rubinstein, and M. Watkins, *Secondary terms in the number of vanishings of quadratic twists of elliptic curve L-functions* (2005); `arxiv.org/math.NT/0509059`

[CRSW] J. B. Conrey, M. O. Rubinstein, N. C. Snaith, and M. Watkins, *Discretisation for odd quadratic twists* (2006); `arxiv.org/math.NT/0509428`

[Cre] J. E. Cremona, *Elliptic curve tables*, `www.maths.nott.ac.uk/personal/jec/ftp/data`

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. Online at `www.maths.nott.ac.uk/personal/jec/book` MR1628193 (99e:11068)

[DFK04] C. David, J. Fearnley, and H. Kisilevsky, *On the vanishing of twisted L-functions of elliptic curves*, Experiment. Math. **13** (2004), no. 2, 185–198. Available online at `arxiv.org/math.NT/0406012`. MR2068892 (2005e:11082)

[Duk97] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. MR1485897 (99b:11059)

[Fal86] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic Geometry (Storrs, CT, 1984), Springer, New York, 1986; translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381] by Edward Shipz, pp. 9–27. MR0861971, MR0718935 (85g:11026a), MR0732554 (85g:11026b)

[Fer96] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur Q* (French) [Experimental study of the rank of families of elliptic curves over Q]. Experiment. Math. **5** (1996), no. 2, 119–130. Available online at `www.expmath.org/restricted/5/5.2/fermigier.ps`. MR1418959 (98g:11061)

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

[Gr] See, for instance, a book review of *Stalking the Riemann Hypothesis: The Quest to Find the Hidden Law of Prime Numbers* by Dan Rockmore, reviewed by S. W. Graham in the MAA Online book review column at `www.maa.org/reviews/stalkingrh.html`, where discrepancies in versions of the story are discussed.

[GT02] A. Granville and T. J. Tucker, *It's as easy as abc*, Notices Amer. Math. Soc. **49** (2002), no. 10, 1224–1231. Online at `www.ams.org/notices/200210/fea-granville.pdf`. MR1930670 (2003f:11044)

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. I. II.* Invent. Math. **111** (1993), no. 1, 171–195; **118** (1994), no. 2, 331–370. MR1193603 (93j:11038), MR1292115 (95h:11064)

[Hel04] H. A. Helfgott, *On the behaviour of root numbers in families of elliptic curves* (2004), submitted; `arxiv.org/math.NT/0408141`

[KaSa99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR1659828 (2000b:11070)

[KeSn00] J. P. Keating and N. C. Snaith, *Random matrix theory and* $\zeta(1/2+it)$, *Random matrix theory and L-functions at* $s = 1/2$. Comm. Math. Phys. **214** (2000), no. 1, 57–89, 91–110. Online from `www.maths.bris.ac.uk/~mancs/publications.html`. MR1794265 (2002c:11107), MR1794267 (2002c:11108)

[Kol88] 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. MR0954295 (89m:11056)

[KowA] E. Kowalski, *Elliptic curves, rank in families and random matrices*. To appear in the Proceedings of the Isaac Newton Institute workshop on random matrices and *L*-functions (July 2004). Also related to the author's lecture at the AIM/Princeton workshop on the Birch and Swinnerton-Dyer conjecture (November 2003). See `www.math.u-bordeaux1.fr/~kowalski/elliptic-curves-families.pdf`

[KowB] E. Kowalski, *On the rank of quadratic twists of elliptic curves over function fields*. To appear in International J. Number Theory. Online at `arxiv.org/math.NT/0503732`

[Mal02] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), no. 2, 315–329. Online from `www.mathematik.uni-kl.de/~malle/en/publications.html`. MR1884706 (2002k:12010)

[Mal04] ———, *On the distribution of Galois groups. II*, Experiment. Math. **13** (2004), no. 2, 129–135. Online from `www.expmath.org/expmath/volumes/13/13.2/Malle.pdf`. MR2068887 (2005g:11216)

[Mpl05] *Matplotlib*, computer software, `matplotlib.sourceforge.net`

[MSD74] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. MR0354674 (50:7152)

[Meh04] M. L. Mehta, *Random matrices*, Third edition, Pure and Applied Mathematics (Amsterdam), 142, Elsevier/Academic Press, Amsterdam, 2004, xviii+688 pp. MR2129906 (2006b:82001)

[Mor22] L. J. Mordell, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees*, Proc. Cambridge Philos. Soc. **21** (1922-23), 179–192.

[RS02] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 4, 455–474. Available online from the AMS website at `www.ams.org/bull/2002-39-04/S0273-0979-02-00952-7/home.html`. MR1920278 (2003f:11080)

[Sha85] D. Shanks, *Solved and Unsolved Problems in Number Theory*. Third edition, Chelsea, New York, 1985. MR0798284 (86j:11001)

[Sil01] A. Silverberg, *Open questions in arithmetic algebraic geometry*, Arithmetic Algebraic Geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 83–142. Can also be obtained online from `www.math.uci.edu/~asilverb/bibliography/pcmibook.ps`. MR1860041 (2002g:11073)

[Sil92] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1992, corrected reprint of the 1986 original. MR1329092 (95m:11054)

[SJ05] W. Stein and D. Joyner, *Sage: System for algebra and geometry experimentation*, Communications in Computer Algebra (SIGSAM Bulletin) (July 2005). Online at `sage.sourceforge.net`

[SW02] W. A. Stein and M. Watkins, *A database of elliptic curves—first report*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275. Online from `modular.ucsd.edu/papers/stein-watkins`

[Tat75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, pp. 33–52. MR0393039 (52:13850)

[Teg04] M. Tegmark et al., *Cosmological parameters from SDSS and WMAP,* Phys. Rev. D **69** (2004) 103501. Online at `arxiv.org/astro-ph/0310723`.

[Wal81] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier* (French) [On the Fourier coefficients of modular forms of half-integral weight], J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484. MR0646366 (83h:10061)

[Wat04] M. Watkins, *Rank distribution in a family of cubic twists*. To appear in Proceedings of the Issac Newton Institute Workshop on Elliptic Curves and Random Matrix Theory. Online at `arxiv.org/math.NT/0412427`

[Wat06] ———, *Some heuristics about elliptic curves*, Preprint (2006). To be submitted to Experimental Mathematics; currently online at `www.maths.bris.ac.uk/~mamjw/heur.ps`

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. Online: `www.jstor.org/view/0003486x/di976377/97p00631/0`. MR1333035 (96d:11071)

[YouA] M. P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. **19** (2006), no. 1, 205–250. Online from `dx.doi.org/10.1090/S0894-0347-05-00503-5`. MR2169047 (2006d:11072)

[YouB] M. P. Young, *On the nonvanishing of elliptic curve L-functions at the central point* (2005), to appear in Proc. London Math. Soc.; `arxiv.org/math.NT/0508185`, AIM preprint 2004-30.

[ZK87] D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. (N.S.) **52** (1987), 51–69 (1988). MR0989230 (90d:11072)

[Zwi33] F. Zwicky, *Die Rotverschiebung von extragalaktischen Nebeln* (German) [The red shift of extragalactic nebulae], Helvetica Phys. Acta, vol. 6 (1933), 110–127.

(B. Bektemirov) Harvard College, Cambridge, Massachusetts 02138

(B. Mazur) Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138

(W. Stein) Department of Mathematics, University of Washington, Seattle, Washington 98195

(M. Watkins) School of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW England