BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 23, Number 2, October 1990

THE BEHAVIOR OF THE MORDELL-WEIL GROUP OF ELLIPTIC CURVES

ARMAND BRUMER AND OISÍN McGUINNESS

1. Introduction

Suppose that E is an elliptic curve defined over $\mathbf{Q}$ given by the equation

$$(1) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where we assume that $a_i \in \mathbf{Z}$. The set $E(\mathbf{Q})$ of solutions (x, y) with x, $y \in \mathbf{Q}$, together with the point at infinity, forms a finitely-generated abelian group, the *Mordell-Weil group* of E. It is isomorphic to $\mathbf{Z}^r \oplus F$, where F is finite and where r is the *rank* of E. The possibilities for the finite group F are completely known [9]. The important question then is to understand the behavior of the rank as E varies over elliptic curves. It is still unknown whether r is unbounded or not. In fact, one opinion is 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 [8]. We present evidence that this may not be the case.

Published examples [2, 10] of curves of rank ≥ 2 might suggest that such curves are sparsely distributed.[1] Mestre and Oesterlé found the 436 modular elliptic curves of prime conductor up to 13100, using [11]. There were 80 rank 2 curves among the 233 curves of even rank. This proportion of rank 2 curves seemed too large to conform to the conventional wisdom just stated (see also [18, pages 254–255]). We decided to investigate the ranks of elliptic curves in a systematic way, over a significantly larger range.

Received by the editors October 30, 1989 and, in revised form, March 1, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G40; Secondary 11D25, 11G05, 11-04, 14K15.

Key words and phrases. Elliptic curve, Mordell-Weil group, rank, Birch-Swinnerton-Dyer conjecture, Hasse-Weil L-series, discriminant, period.

[1] This situation is not unrelated to the ranks of ideal class groups of quadratic fields, where similar phenomena occur [13].

Curves of *prime* conductor only were considered for practical and theoretical reasons. This collection of curves appears to be a typical sample of the set of *all* curves (see §5 for some evidence).

We studied 310,716 elliptic curves of prime conductor less than 10^8. There were 155,658 curves with odd rank, and 155,058 curves with even rank. We found that 20.06% of *all* our curves have even rank at least 2, or about 40% of all the even rank curves. Even more striking is the behavior of the average rank, as discussed in §3. An incidental aspect of our computations is a massive corroboration of the standard conjectures on elliptic curves, recalled in §2.

Recent related work is described in [6] and [8]. Contrasts with our results are given in §3.

We expect to publish a fuller account, including the behavior of other invariants of interest. This announcement reports mainly on ranks. The computations were carried out on Macintosh II computers at Fordham University, with the partial support of a National Science Foundation grant. We would like to thank our colleagues R. Lewis, I. Morrison, and W. Singer for the use of their machines.

2. Definitions

We recall standard notations and definitions [15]. Associated with equation (1) is the *discriminant* Δ, which we will assume to be *minimal* among all models (1) of E. The fundamental property of the discriminant is that $p \mid \Delta$ if and only if equation (1) is singular modulo p, and the *conductor* N of E is a subtler invariant that has the same property.

The Hasse-Weil L-series of E is defined for $\Re(s) > 3/2$ by

$$L(E, s) = \prod_{p \mid N} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1},$$

where for $p \mid N$, $a_p \in \{-1, 0, 1\}$ and for $p \nmid N$, $a_p = p + 1 - |E(\mathbf{F}_p)|$. We shall assume that E is a *modular* curve, so E is a factor[2] of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ of level N. (That is, the Taniyama-Weil conjecture for E is true.) Hence, $L(E, s)$ can be continued to an entire function on $\mathbf{C}$, satisfying a functional equation when $s \mapsto 2 - s$, with a

[2] Note that Mestre-Oesterlé found their curves by determining the 1-dimensional factors of $J_0(N)$. Needless to say, we have the same curves in their range.

0 at $s = 1$ of order ρ, the *analytic* rank of E. For squarefree conductor, the sign in the functional equation may be easily calculated from an equation of the curve, allowing a conjectural prediction of the parity of the analytic rank [1]. We also assume that the conjecture of Birch and Swinnerton-Dyer holds, so that the analytic rank equals the rank, $\rho = r$, and the leading term of $L(E, s)$ at $s = 1$ is given by:

$$\lim_{s\to 1}\frac{L(E, s)}{(s-1)^r} = \Omega\frac{|\text{Ш}|\det\left(\langle P_i, P_j\rangle\right)}{[E(\mathbf{Q}) : E']^2}\prod_{p\mid\Delta} c_p. \tag{2}$$

Here Ω is the period $\int_{E(\mathbf{R})}|\omega|$, for ω a Néron differential on E, Ш denotes the conjecturally finite Tate-Shafarevich group of E, the P_i for $1 \le i \le r$ are an independent set of points in $E(\mathbf{Q})$ generating the subgroup E', and $\langle P_i, P_j\rangle$ denotes the height pairing. The fudge factors c_p are all 1 for the curves we consider. Recent work of Rubin [14] confirms the conjecture of Birch and Swinnerton-Dyer in many cases of rank $r \le 1$.

Examples illustrating (2) for the curves of ranks 4 and 5 of least known conductor are given in §4.

3. Rank results

Elliptic curves of prime conductor N were conjectured to have prime discriminant, except for the Setzer-Neumann curves and for five other small conductor curves; see [2, Appendix]. This is now known for *modular* curves by Theorem 2 of [12]. We therefore searched for curves of prime discriminant, by looking for integral solutions to the equation

$$c_4^3 - c_6^2 = 1728\Delta, \tag{3}$$

where c_4 and c_6 are the usual invariants attached to equation (1), or more precisely, by fixing a_4, and searching for a_6 for which (3) has a solution with Δ prime and less than 10^8. This produced 311, 243 curves, including the 869 expected curves with nontrivial torsion and rank 0. The set of 310, 716 curves that we studied is most simply described by

$$\{E : |\Delta| \le 10^8, |a_6| \le 2^{31} - 1\},$$

with $|\Delta|$ *prime.*

We will not describe here all the details of the several thousand hours of computations, but just say that imitating Mazur's description [17] of "infinite descent," we searched for points by night, and calculated L-series derivatives or regulators by day. We may use the infinite series formulas of [3] for the derivatives of the L-series at $s = 1$, since E is assumed modular. Then an upper bound for the analytic rank is found by estimating the order of vanishing of $L(E, s)$ at $s = 1$. Using 2000 or 4000 terms of these series provided sufficient accuracy for our purposes, since the values are either 0 to several places or else are far from 0 in most cases. The period Ω is easily calculated using the arithmetic-geometric mean algorithm of Gauss [7], and the height regulator $R = \det\left(\langle P_i, P_j\rangle\right)$ is computed by using the method of Tate, as modified by Silverman [16], once points have been found by a search.

The rank predictions are based on a combination of three calculations: the rank parity, the analytic rank or order of vanishing of the L-series, and the number of independent points found which is a lower bound for the algebraic rank r. When the ranks coincide, as they should, we get a prediction from (2) of $|Ш|$, which should be an integer square. The largest $|Ш|$ we found was 289, for a curve of rank 0.

For each curve, we keep its discriminant, parity, period, rank, the appropriate L-derivative value, a list of x-coordinates of the independent points found, and the regulator of these points.

Of the curves analyzed, 113,969 had positive discriminant, and 196,747 had negative discriminant.[3] An interesting phenomenon was the systematic influence of the discriminant sign on all aspects of the arithmetic of the curve. The rank distribution is given in the following table:

Rank	0	1	2	3	4	5
$\Delta > 0$	31748	51871	24706	5267	377	0
$\Delta < 0$	61589	91321	36811	6594	427	5
Totals	93337	143192	61517	11861	804	5
Percents	30.04	46.08	19.80	3.82	0.26	

Thus, 20.06% of the curves have even rank at least 2. Note that the *positive* discriminant curves give an even higher percentage!

Define $N(r, X)$ to be the proportion of curves with conductor at most X, and with rank at least r. Our data show that these functions are *increasing* functions of X for $r \geq 3$ and $X \leq 10^8$. In contrast [6], dealing with quadratic twists of elliptic curves suggests a decrease for the analogous functions.

[3] The quotient is about 1.726, near $\sqrt{3}$. See §5 for an explanation.

Denote the *average rank* among the curves with discriminant sign ϵ and conductor at most X by $r_\epsilon(X)$. In our data, the functions $r_\epsilon(X)$ for $X < 10^8$ are quite steadily climbing to the numbers 1.04 for $\Delta > 0$, and to 0.94 for $\Delta < 0$. In particular, the average rank of our curves is *not* 0.5, as is expected to be the case for twists [5, 8].

In most cases, the predicted analytic rank matches with the rank of points found, and the predicted Ш is close to a nonzero integral square. More precisely, this is so for all the curves of rank at least 3, and for 95% of the rank 2 curves. There is a very small number of rank 2 curves for which the prediction of rank 2 is based solely on the vanishing of L-series. Note that in [8], a numerical study of one family of cubic twists, only the analytic rank is estimated. For many rank 1 curves (i.e., curves whose rank is predicted to be odd for which $L'(E, 1)$ does not vanish), we have found no points by point searches over moderate ranges, and do not expect to find any small points.

4. Examples

In the literature, one finds very few verifications of the conjecture of Birch and Swinnerton-Dyer for ranks ≥ 2. The paper [3] on the curve of conductor 5077, found in [2], works out the only rank 3 case that we know of. It is perhaps not without interest to report the details for the curves[4] of smallest known conductor of rank 4 and of rank 5.

The first rank 4 curve is:

$$y^2 + y = x^3 + x^2 - 72x + 210, \qquad \Delta = 501029.$$

For this curve, the predicted parity is even, the period $\Omega = 2.952580$, the value and second derivative of the L-series vanish to several places, and $L^{(4)}(E, 1)/4! = 9.357978$. The points with x-coordinates $5, 4, 3, 6$, in order of increasing height, form a basis. The regulator is $R = 3.169424$, which matches the quotient of $L^{(4)}(E, 1)/4!$ and Ω, so $|Ш|$ appears to be 1. There are 21×2 integral points with $|x| < 10^6$, while the second curve of rank 4 has 28×2.

The first rank 5 curve is:

$$y^2 + y = x^3 - 79x + 342, \qquad \Delta = -19047851.$$

[4] These curves are new. The curves of rank 4 reported in [2] and [10] are respectively the fifth, seventh, and second curves of rank 4 in our list.

The previously found curves of rank 5 have conductors about ten times larger [2, 10].

The predicted parity is odd, the period $\Omega = 2.047641$, and then the first and third L-series derivatives are 0 to several places, and $L^{(5)}(E, 1)/5! = 30.285711$. Dividing by Ω gives 14.790539. There are 38×2 integral points with $|x| < 10^6$. Those with $x = 5, 4, 3, 7, 0$ form a basis for $E(\mathbf{Q})$ with height regulator $R = 14.790528$. So Ш is predicted to be trivial. There are four other curves of rank 5 with conductor less than 100 million. The next one has discriminant $-64, 921, 931$. All turn out to have trivial Ш , if we believe the conjectures.

Some of the curves found by the search give rise to rather spectacular cancellations. A particular example is the curve of rank 0

$$y^2+xy+y = x^3+x^2-12632622x-17287039382, \qquad \Delta = 38593.$$

Here $c_4 = 606, 365, 857$, and $c_6 = 14, 931, 454, 281, 967$, and the equation $1728\Delta = c_4^3-c_6^2$ involves the difference of two 27 digit numbers!

5. Heuristics

While its connection with the Taniyama-Weil conjecture makes the conductor a natural invariant, the discriminant has turned out to be more useful in our heuristics. The idea is to arrange the curves in order by discriminant size, and then replace lattice-point counting problems by area computations. This works well, for instance, to count curves.

Heuristic Estimate. *We have the following estimates for the number of positive and negative discriminants of absolute value at most* N,

$$A_+(N) \sim \frac{\alpha_+}{\zeta(10)} N^{5/6},$$
$$A_-(N) \sim \frac{\alpha_-}{\zeta(10)} N^{5/6}.$$

The $\zeta(10)$ factor arises from taking into account the nonminimal discriminants. Here $\alpha_+ = 0.4206$ and $\alpha_- = 0.7285$ are given by the elliptic integrals

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

which arise from parameterizing suitably the integrals that replace the lattice-point counts. A well-known identity of Legendre, related to complex multiplication, is $\alpha_- = \sqrt{3}\alpha_+$.

Remark. One should compare this estimate with the results of [4]. While the number of elliptic curves grows like $N^{5/6}$, the number of cubic fields grows like N.

Assuming the distribution of *prime* discriminants among discriminants is that of prime numbers among all integers, the number of prime discriminants of sign ϵ and of size less than N is then $\alpha_\epsilon \operatorname{Li}(N^{5/6})$, where $\operatorname{Li}(x)$ is the logarithmic integral. The expected number of curves with prime $|\Delta| < 10^8$ is then $311, 586$, comparing rather well with the number $311, 243$ found.

Similar heuristic arguments have been applied to other invariants. For instance, the *average period of a curve with positive discriminant is* $\sqrt{3/2}$ *times the average period of a curve with negative discriminant.* This is also confirmed by the data. The fits with the experimental data are so good that one could hope for proofs in the near future.

We have not as yet been able to provide heuristics for the growth of the functions $N(r, X)$. 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.

References

1. B. Birch and W. Kuyk, editors, *Modular functions of one variable* IV, Lecture Notes in Math., vol. 476, Springer-Verlag, New York, 1975.
2. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.
3. J. Buhler, B. H. Gross and D. B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3, Math. Comp. **44** (1985), 473–481.
4. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields* (II), Proc. Royal Soc. London Ser. (A) **322** (1971), 405–420.
5. D. M. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory Carbondale 1979, Lecture Notes in Math., vol. 751, Springer-Verlag, New York, 1979, pp. 108–118.
6. F. Gouvea and B. Mazur, *The square-free sieve and the rank of Mordell-Weil*, preprint, April 1989.
7. D. Grayson, *The arithogeometric mean*, Arch. Math. **52** (1989), 507–512.
8. G. Kramarz and D. B. Zagier, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51–60, (Ramanujan Centenary volume).
9. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.

10. J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Comp. Math. **58** (1986), 209–232.

11. J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Class Numbers and Units of Number Fields, Katata conference, Nagoya University, Nagoya, Japan, 1986, pp. 217–242, (unpublished tables).

12. J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance* m*-ième*, J. Reine Angew. Math. **400** (1989), 173–184.

13. J. Quer, *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de rang* 12, C. R. Acad. Sci. Paris Ser. 1 **305** (1987), 215–218.

14. K. Rubin, *The work of Kolyvagin on the arithmetic of elliptic curves*, Arithmetic of Complex Manifolds (W. P. Barth and H. Lange, eds.), Lecture Notes in Math., vol. 1399, Springer-Verlag, New York, 1989, pp. 128–136.

15. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. vol. 106, Springer-Verlag, New York, 1986.

16. J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.

17. J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

18. L. C. Washington, *Number fields and elliptic curves*, NATO Adv. Study Inst. on Number Theory, Banff 1988, Kluwer, Netherlands, 1989, pp. 245–278.

Mathematics Department, Fordham University, Bronx, New York 10458