Rank Computations for the Congruent Number Elliptic Curves

Nicholas F. Rogers

CONTENTS

In a companion paper, Rubin and Silverberg relate the question of unboundedness of rank in families of quadratic twists of elliptic curves to the convergence or divergence of certain series. Here we give a computational application of their ideas on counting the rational points in such families; namely, to find curves of high rank in families of quadratic twists. We also observe that the algorithm seems to find as many curves of positive even rank as it does curves of odd rank. Results are given in the case of the congruent number elliptic curves, which are the quadratic twists of the curve $y^2 = x^3 - x$; for this family, the highest rank found is 6.

1. MAIN ALGORITHM

Rubin and Silverberg [2000] have studied the question of unboundedness of rank in families of quadratic twists, and have rephrased it in terms of the asymptotic behavior of certain arithmetically defined series. Fix a family of twists $E^{(D)} : Dy^2 = f(x)$, where D is square-free. Then the starting point of their argument is the observation of Gouvêa and Mazur [1991] that, for any nonzero rational number $x = u/v$, x is the x-coordinate of a rational point on exactly one of the curves $E^{(D)}$, namely when $D = s(f(u/v))$. Here $s(u/v)$ will denote the square-free part of a rational number u/v; that is, the unique square-free integer such that $s(u/v) \cdot v/u$ is the square of a rational number.

This observation suggested to Rubin and Silverberg the following sieving process to look for curves of high rank in a given family of twists. For each rational number u/v up to some fixed height, compute the D for which $(u/v, y)$ is a rational point on the curve $E^{(D)}$. Keep track of which D's were attained most often in this way; these are the D's for which there are many rational points of small (naive) height. Since the logarithmic (naive) height

1058-6458/2000 $0.50 per page

is approximately a quadratic form on the group of rational points, a curve with many points found in this way would tend to have higher rank. The last step is most easily accomplished by computing the rank of the best D's directly, using one of the available rank computation programs such as mwrank [Cremona 1998] or apecs [Connell n.d.]. In practice, of course, curves of high rank are quite rare, and it requires the consideration of many rational numbers u/v to distinguish between curves of high rank and large regulator and those of moderate rank but small regulator.

2. THE CONGRUENT NUMBER ELLIPTIC CURVES

We have actually implemented and run this algorithm in the case of the so-called congruent number elliptic curves, which are the quadratic twists $E^{(D)} : Dy^2 = x^3 - x$. The literature seems to be lacking in concrete examples of curves in this family with even moderately high rank. Nemenzo [1998], extending results from [Noda and Wada 1993; Kramarz 1986], computes the ranks of all of the curves $E^{(D)}$ for $D \le 40000$; the highest rank encountered in this range is 4.

For the congruent number elliptic curves, the computations can be simplified considerably. First of all, we need only consider one representative of each element in the quotient group $E^{(D)}(\mathbb{Q})/E^{(D)}_{tors}(\mathbb{Q})$. In this case, $E^{(D)}_{tors}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and it is easy to check that in each orbit of a point of infinite order in the natural additive action of the torsion subgroup, there are two points with positive x-coordinate. Furthermore, exactly one of these two x-coordinates is written in lowest terms as the quotient of an odd number and an even number. It is obvious that there are no points with x-coordinate less than one, so in the algorithm it suffices to consider only rational numbers $u/v > 1$, with u and v not both odd. Equivalently, we could consider only those rational numbers u/v with u and v both odd, but then it is easy to see that we must consider numbers up to a greater height, which is disadvantageous for reasons described below.

In practice, the most difficult computation in the algorithm is the determination of $s(f(u/v))$, which in the general case seems to be about as difficult as factoring $f(u/v)$. However, in this special case we have $f(u/v) = (1/v^4)(u^3v - uv^3)$, so

$$s(f(u/v)) = s(u^3v - uv^3) = s\big(uv(u-v)(u+v)\big).$$

Now, since u and v are relatively prime and not both odd, the four numbers u, v, $u-v$, and $u+v$ are all pairwise relatively prime, and we may write $s\big(uv(u-v)(u+v)\big) = s(u)s(v)s(u-v)s(u+v)$. In the algorithm, we consider rational numbers up to some fixed height H, so certainly $u, v \le H$ and $u + v < 2H$. Thus it suffices to precompute the square-free parts of all integers up to $2H$, and the computation of $s(f(u/v))$ is reduced to a few multiplications.

The remaining question is how to keep track of the score of each D as the algorithm progresses. In our implementation, we used a hash table keyed on the integer D. Also, we enforced a maximum table size (simply constrained by memory limitations), and so any D discovered after the table was full was ignored. We chose the number of hash buckets to be a prime number p near the maximum table size, to minimize key collisions, and then the hash function is simply reduction modulo p.

The constraint of the table size is quite a troublesome one, since the table tends to fill rather quickly. There are on the order of h^2 rational numbers of height less than h, and so if repetitions are rare (as they are in practice), the table will be full after considering numbers up to height on the order of the square root of the table size. There are, however, numerous ways to improve one's chances of finding a curve of high rank. For example, one could demand that for a number D to be entered into the table, it must have some minimum number of prime factors (since the Selmer group must be large; see [Silverman 1986, X.6]), or that each prime factor must be less than some arbitrary upper bound. Also, the Conjecture of Birch and Swinnerton-Dyer predicts that $E^{(D)}$ has even rank if $D \equiv 1, 2, 3 \pmod 8$ and odd rank if $D \equiv 5, 6, 7 \pmod 8$. So, if one is interested in a particular rank, it is easy to eliminate curves whose rank is the opposite parity. Another option is to "clean out" the table every time it gets full, by removing all of the D's that have only appeared once. This is a tremendous savings of space, but it takes a lot of time, and the table must be emptied so often that there are undoubtedly many unlucky curves of high rank that never manage to get more than one entry before the next cleaning.

Results of running this algorithm with most of the improvements just mentioned are given below. For each rank, the first curve found by the algorithm is given, which is a curve of that rank distinguished by having several rational points of relatively small height. The specifications for this particular running of the algorithm are as follows: the maximum table size was 3000000, and the upper bound H on u and v was 100000. These particular examples can be produced in a relatively short time, perhaps between four and six hours on a Sparc machine with 64-bit integers. In fact, the more time-consuming portion of the algorithm was running a rank computation program on the high-scoring D's to see which actually have high rank.

Rank 1:	D = 6
Rank 2:	D = 210
Rank 3:	D = 1254
Rank 4:	D = 29274
Rank 5:	D = 4132814070
Rank 6:	D = 61471349610

Note that for most ranks, the first curve found is not the curve with the smallest D. For example, $E^{(5)}$ has rank 1 and $E^{(34)}$ has rank 2. In fact, for each given rank except 6, I know of smaller D's than those given above. It is a much more difficult problem to produce the minimum D for which $E^{(D)}$ has a given rank r, since it may have large regulator. For this problem, there does not seem to be a significantly better approach than trying to compute directly the rank of each $E^{(D)}$ in succession, which is hopelessly slow.

3. TUNNELL'S THEOREM AND THE EFFECTIVENESS OF THE ALGORITHM

To analyze the effectiveness of this algorithm, one must consider how quickly the algorithm tends to find curves of a given rank. In this section, we consider the simplest case, and look at how well the algorithm finds curves of rank 2 as compared to how well it finds curves of rank 1.

Tunnell's theorem (see [Tunnell 1983] or [Koblitz 1984, IV.4]), which hypothesizes the weak Birch and Swinnerton-Dyer conjecture, characterizes in a computationally effective way all of the congruent number elliptic curves of nonzero rank. Furthermore, the reduction of D modulo 8 conjecturally gives us the parity of the rank. Combining these, we can compute fairly easily which curves $E^{(D)}$ have odd rank, and which have nonzero even rank. If we assume that most of the odd rank curves have rank 1, and that most of the nonzero even rank curves have rank 2 (reasonable assumptions given experimental data), we can address the above question in this special case.

The results of this computation are given in Table 1. For this computation, the upper bound H on u and v is 500000. The first column of the table is the range of square-free integers D. The next three columns show data for the curves which conjecturally have odd rank; that is, where $D \equiv 5, 6, 7 \pmod 8$. The first of these three is the number of curves of nonzero rank, which is all of them in the odd rank case. That is, this first column is just the number of squarefree integers D in the specified range. The next shows the number found by the algorithm, and the third is the percentage found. The final three columns give analogous data for the even rank case, i.e., when $D \equiv 1, 2, 3 \pmod 8$. In this case Tunnell's theorem is used to compute which curves have nonzero rank, and so the weak Birch and Swinnerton-Dyer conjecture is hypothesized.

As the computations show, it seems to be just as easy to find curves of nonzero even rank as curves of odd rank. In fact, the number of positive even rank curves found is practically equal to the number of odd rank curves. This is rather surprising given the relative rarity of nonzero even rank curves.

ACKNOWLEDGMENTS

I thank Karl Rubin for suggesting this project to me, and for his advice and guidance.

REFERENCES

[Connell n.d.] I. Connell, "APECS: Arithmetic of Plane Elliptic Curves", See ftp.math.mcgill.ca/pub/apecs/. Requires Maple.

[Cremona 1998] J. E. Cremona, "mwrank, a program for 2-descent on elliptic curves over $\mathbb{Q}$", last major update 1998. See http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs.

range		#odd	found		#even	found	
from	to		#	%		#	%
1	1000000	303979	12832	4.221	28733	11190	38.945
1000001	2000000	303972	6656	2.190	23875	6247	26.165
2000001	3000000	303933	5308	1.746	22181	4970	22.407
3000001	4000000	304003	4526	1.489	21416	4469	20.868
4000001	5000000	303945	4146	1.364	20459	3963	19.370
5000001	6000000	303944	3854	1.268	20208	3640	18.013
6000001	7000000	303977	3485	1.146	19609	3406	17.370
7000001	8000000	303971	3241	1.066	19523	3211	16.447
8000001	9000000	303962	3035	0.998	18755	2970	15.836
9000001	10000000	303962	2959	0.973	18559	2867	15.448
10000001	11000000	303983	2758	0.907	18118	2733	15.084
11000001	12000000	303953	2739	0.901	18191	2719	14.947
12000001	13000000	303965	2620	0.862	18025	2625	14.563
13000001	14000000	303955	2445	0.804	17674	2596	14.688
14000001	15000000	303953	2517	0.828	17220	2343	13.606
15000001	16000000	303973	2319	0.763	17174	2428	14.138
16000001	17000000	303938	2304	0.758	16803	2167	12.897
17000001	18000000	303969	2266	0.745	17026	2192	12.874
18000001	19000000	303991	2122	0.698	16879	2180	12.915
19000001	20000000	303963	2095	0.689	16751	2121	12.662

TABLE 1. Expected number of nonzero rank curves with D up to 20 million, grouped by the conjectural parity of the rank. The computations use Tunnell's theorem, and therefore hypothesize the weak Birch and Swinnerton-Dyer conjecture. The table also shows what fraction of these D's were encountered in running the algorithm described in this paper with $H < 100000$; that is, the D's for which $E^{(D)}$ has a rational point whose x-coordinate has height less than 100000.

[Gouvêa and Mazur 1991] F. Gouvêa and B. Mazur, "The square-free sieve and the rank of elliptic curves", *J. Amer. Math. Soc.* **4**:1 (1991), 1–23.

[Koblitz 1984] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math. **97**, Springer, New York, 1984. Second edition, 1993.

[Kramarz 1986] G. Kramarz, "All congruent numbers less than 2000", *Math. Ann.* **273**:2 (1986), 337–340.

[Nemenzo 1998] F. R. Nemenzo, "All congruent numbers less than 40000", *Proc. Japan Acad. Ser. A Math. Sci.* **74**:1 (1998), 29–31.

[Noda and Wada 1993] K. Noda and H. Wada, "All congruent numbers less than 10 000", *Proc. Japan Acad. Ser. A Math. Sci.* **69**:6 (1993), 175–178.

[Rubin and Silverberg 2000] K. Rubin and A. Silverberg, "Ranks of elliptic curves in families of quadratic twists", *Experiment. Math.* **9**:4 (2000), 583–590.

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

[Tunnell 1983] J. B. Tunnell, "A classical Diophantine problem and modular forms of weight 3/2", *Invent. Math.* **72**:2 (1983), 323–334.

Nicholas F. Rogers, Department of Mathematics, Harvard University, Cambridge, MA 02138, United States (nfrogers@math.harvard.edu)

Received December 12, 1999; accepted March 6, 2000