On Some Elliptic Curves with Large Sha

Harvey E. Rose

CONTENTS

We consider a class of elliptic curves many of whose associated Shafarevich–Tate groups Ш are relatively large, and give examples of curves with o(Ш) = k^2 for all $k \leq 100$.

1. INTRODUCTION

Let p be a prime satisfying $p \equiv 1 \pmod 8$ throughout, and let $C(n)$ denote the elliptic curve

$$C(n) : y^2 = x^3 + nx,$$

where $n \in \mathbb{Z}$. We shall mainly be concerned with the case $n = p^3$. Further, for the curve $C(n)$, let $r(C(n))$ denote the (Mordell–Weil) rank over $\mathbb{Q}$, and $st(C(n))$ denote the (analytic) order of the Shafarevich–Tate group $Ш_{C(n)}$. We shall assume that the full Birch and Swinnerton-Dyer conjecture holds for all curves under consideration; see [Silverman 1986] for further details. The conjecture has been established in the rank zero case, except possibly for the 2 component of the formula; see [Rubin 1991].

Whilst undertaking some general investigations on the elliptic curves $C(n)$ for various small n, we noted that in the cases when $n = p^3$ a surprising number of the curves had comparatively large values for $st(C(n))$; for instance $st(C(233^3)) = 64$ and $st(C(433^3)) = 81$. This phenomenon was also noted for the curves $C(2p^3)$ but to a lesser extent. After some further computations it became clear that the curves $C(p^3)$ regularly have large sha; and hence it was possible, and thought to be worthwhile, to produce a list of elliptic curves with $o(Ш) = k^2$ for *each* k in some typical range. We chose $k \leq 100$ as being attainable in a few weeks using a reasonably fast machine, although the last entry found, for $k = 98$, did extend this timetable somewhat (and so it is remarkable in this case that a second prime occurs so soon after the first; although there are a number of

Keywords: elliptic curve, rank
AMS Classification: Primary: 11G05, 11D28; Secondary: 14H52

1058-6458/2000 $0.50 per page

similar instances, for example when $k = 6$ or 35). See Table 2.

Cassels [1964] showed that there are elliptic curves with arbitrarily large Shafarevich–Tate groups Ш by considering quadratic twists by many different primes. Recently de Weger [1998] has given some specific examples of curves with large sha, his largest satisfies $o(\text{Ш}) = 224^2$. He also discusses the Goldfeld–Szpiro Conjecture, first considered in [Goldfeld and Szpiro 1995], relating the size of Ш to the conductor; see Section 4E.

A prime p is called a *G-prime* if it can be expressed in the form $p = x^2 + 64y^2$ (or, equivalently, if 2 is a quartic residue modulo p). A easy extension of this gives: p^3 can be expressed in the form

$$p^3 = x_1^2 + 64y_1^2 \quad \text{with} \quad (x_1, y_1) = 1$$

if and only if p is a G-prime. Repeating the argument given in [Silverman 1986, Chapter 10] for the curves $C(p)$, we see that $C(p^3)$ has rank zero or two provided we assume, as we are doing, that the Birch and Swinnerton-Dyer Conjecture holds. (Note. The curve $C(p^3)$ is a quadratic twist of $C(p)$.) In [Rose 1995] we showed, using elementary methods, that $r(C(p)) = 0$ if p is not a G-prime (and so the conjecture is not needed in this case); an exactly similar argument shows that $r(C(p^3)) = 0$ when p is not a G-prime, and again the conjecture is only needed in the G-prime case.

2. METHOD

For $p \equiv 1 \pmod 8$ consider the elliptic curve $C(p^3)$. Note first that, whilst the discriminant of this curve is $64p^9$, its conductor is $64p^2$, and so it is as easy to calculate the value of $L(s)$-function at $s = 1$ for the curve $C(p^3)$ as it is for $C(p)$ (as these curves have the same conductor). The calculations were undertaken using the method given in [Buhler et al. 1985] and the computer package Pari/GP 1.39.

In [Rose 1997] we conjecture that the probability for the curve $C(p)$ to have rank 2 is $O(p^{-1/8})$ (this is backed up with some numerical evidence and the implied constant is close to 3/2). The computations undertaken for this paper suggest that a similar estimate applies for the curves $C(p^3)$; that is, the probability of the rank of $C(p^3)$ equalling two is $O(p^{-3/8})$. The data given in Table 1 provides some evidence for the validity of this estimate. It is perhaps also of interest to note that there is *no* close correspondence between the ranks of $C(p)$ and $C(p^3)$ for fixed p — for many primes p, $C(p)$ has rank 2 and $C(p^3)$ has rank 0, whilst those p marked with an asterisk in Table 1 satisfy the opposite: namely, $r(C(p)) = 0$ and $r(C(p^3)) = 2$. In the remaining cases in this table both curves have rank 2. Note also that, for all the asterisked primes p in the table, we have $st(C(p)) = 64$ using data given in [Rose 1997]; for larger p this equation will probably need to be replaced by the condition $64 \mid st(C(p))$. Note that $st(C(p))$ need not be a power of two even in the rank 2 case, for example $st(C(51137)) = 9$ as noted in [Rose 1997].

89	6529	26249	41177	52673	67057	83089
601	8969	26417	43441	54401	67129	83177*
937	12697*	26497*	43721	54497	70921	84857
1889	13913	27449	45281	57073	71233	86161
2969	14249	29569	47057	57529	71761	87641
3257	16633	32009	47609	57697	73417*	88873
3529	17881	32377	47713	60089	75289	91873
3673	25057*	35449	49681	65729	77249	96001
4289	25409	40577	52489	66569	79537	96137

TABLE 1. Primes $p \equiv 1 \pmod 8$ less than 10^5 for which the curve $C(p^3)$ has rank 2. The asterisk means that $r(C(p)) = 0$.

We have confirmed that these curves have rank 2 (by finding two independent generators) for the first three primes only, although one generator is known in 20 cases. In the remaining cases we are relying on the Birch and Swinnerton-Dyer conjecture, and the fact that our calculated estimate for the value of the $L(s)$-function at $s = 1$ equals zero to an accuracy of at least four places. It would be a major undertaking to find the generators for the remaining curves; in no case will elementary (that is, quadratic) arguments help.

3. RANK-ZERO CURVES

We consider now the elliptic curves $C(p^3)$ with rank zero; note that in this case the Birch–Swinnerton-Dyer conjecture has been established except for the power of 2 in their formula; see [Rubin 1991]. We have calculated the values of the $L(s)$-functions of these curves at $s = 1$ for all primes congruent to

1 modulo 8 up to 150000, and up to 230000 for G-primes congruent to 1 or 33 modulo 40 only; a summary of the results is given in Table 2. We curtailed the calculations once we had found at least one entry in every line of Table 2, further details are available from the author via e-mail. We also calculated these L-function values in two higher, randomly chosen, ranges: 1200000 to 1205000, and 4100100 to 4105100. All calculations were performed to an accuracy of at least three decimal places; this was sufficient to give, using the Birch and Swinnerton-Dyer conjecture, the value of $st(C(p^3))$ as this number is a square integer k^2 whose parity can be determined in advance, see Section 4C below. Also we found that the larger the value of $st(C(p^3))$ the better was the accuracy of the calculation. Typical examples of actual calculated values are:

$$st(C(229321^3)) = 8464.0733 \approx 8464 = 92^2,$$
$$st(C(219361^3)) = 2.8927 \approx 4$$

(here 219361 is a G-prime, so the st value is an even square).

4. OBSERVATIONS ABOUT THE CALCULATIONS

4A. The Spread of Values of k

All values of k occur and, generally speaking, they occur with a similar frequency. It seems reasonable to assume that for all k there are infinitely many primes p such that

$$st(C(p^3)) = k^2,$$

although the frequency of these occurrences probably drops considerably as p increases. For example the values $k = 1, 2$ or 3 do not occur in the range $1200000 < p < 1205000$, the smallest value of $st(C(p^3))$ for rank zero curves in this range is 16.

Further the first prime p for which the displayed equation above holds increases relatively smoothly with k, except that there is a slight tendency for this prime to be larger than ‘normal’ when k has the form $k = 2n$ and n is odd. Examples are when $k = 6, 26, 50$ and 98. This is probably not significant; for instance, although the smallest prime p with $st(C(p^3)) = 2500$ is $p = 79769$, there are at least eleven further primes with this property less then 200000. Finally note that there is also a tendency for the ‘first’ prime to be congruent to 3 mod 5 (or, to a lesser extent, congruent to 1 mod 5); this is also probably not significant but explains the choice of primes between 150001 and 230000 above.

4B. The Size of Values k

Compared with some previously published tables, for example Cremona [1997], the sizes of the Shafarevich–Tate groups for the curves under consideration are relatively large. We have if $p < 50000$ the largest value for $st(C(p^3))$ is 7744, for the prime 46681; if $p < 10^5$ the largest value is 11025, for the prime 99233; if $p < 150000$ the largest value is $28561 = 169^2$, for the prime 137873.

Further in the range $1200000 < p < 1205000$ the largest st value is $111556 = 334^2$ for the prime 1200833, and in the range $4100100 < p < 4105100$ we found the values

$$st(C(4102393^3)) = 391^2,$$
$$st(C(4103353^3)) = 474^2,$$
$$st(C(4105033^3)) = 635^2 = 403225,$$

which is the largest explicitly calculated value of sha for any elliptic curve known to the author.

4C. G and Non-G Primes

For the curves $C(p^3)$,

$st(C(p^3))$ is even if and only if p is a G-prime.

We used this to complete the table below by considering only G-primes between 150000 and 230000. Note that, for the curves $C(p)$, we have $4 \mid st(C(p))$ for all p and

$$16 \mid st(C(p)) \text{ if and only if } p \text{ is a } G\text{-prime;}$$

see [Rose 1995]. Also note that although $C(p^3)$ is a quadratic twist of $C(p)$ there is no precise relationship between their corresponding ‘shas’. For example $st(C(56081)) = 6^2$ whilst $st(C(56081^3)) = 55^2$.

4D. Relationship Between $C(p^3)$ and $C(p)$ for G-Primes p

There is some connection between the 2-component of $st(C(p^3))$ and the rank of $C(p)$. Using the data given in [Rose 1995; 1997], the following properties hold for $p < 10^5$ for the curves under consideration:

(a) If $4 \,||\, st(C(p^3))$ then $r(C(p)) = 0$.
(b) If $16 \mid st(C(p^3))$ then either $r(C(p)) = 2$, or $r(C(p)) = 0$ and $64 \mid st(C(p))$.

k	n	p_1	p_2	k	n	p_1	p_2	k	n	p_1	p_2	k	n	p_1	p_2	k	n	p_1	p_2
1	96	17	41	22	43	3761	7841	43	16	31081	41513	64	5	51913	59473	85	5	49433	74873
2	68	257	577	23	33	2753	5641	44	15	20353	27073	65	4	70393	71633	86	0	134593	163481
3	116	137	241	24	45	3313	5113	45	16	31481	41953	66	2	57793	70321	87	2	48073	78713
4	126	73	113	25	46	2953	4561	46	5	23761	67049	67	3	29873	38113	88	1	46681	142193
5	123	313	401	26	25	19433	26297	47	7	32441	52433	68	7	16553	25633	89	2	64153	86353
6	72	2833	2857	27	27	7681	11369	48	13	27953	41233	69	1	81353	109001	90	0	159833	224881
7	82	641	2417	28	34	11633	14633	49	8	20233	30593	70	3	82073	89273	91	2	72353	96233
8	98	233	1153	29	22	5273	5953	50	4	79769	83737	71	4	82913	84761	92	0	123593	133033
9	92	433	673	30	32	9281	13921	51	7	11353	45121	72	3	50833	80273	93	2	67153	95233
10	60	1721	2441	31	19	12401	14081	52	13	14713	18433	73	2	28793	76873	94	0	145513	179801
11	63	953	2713	32	31	7993	12073	53	7	15233	31193	74	1	94273	103049	95	0	128873	141041
12	91	1753	1801	33	20	8513	16561	54	1	48593	113489	75	2	44953	48761	96	3	69833	71473
13	70	1321	5009	34	7	21961	30697	55	3	56081	63281	76	3	66593	78233	97	2	66713	90313
14	50	4001	5737	35	25	11393	11593	56	5	43313	51241	77	2	36473	73681	98	0	222193	224993
15	70	9049	11489	36	32	18481	24281	57	8	45673	52153	78	4	58073	62761	99	0	106321	139201
16	60	1193	3833	37	19	15473	17713	58	4	60601	70913	79	1	43913	146273	100	1	50153	103553
17	49	3881	8521	38	10	28001	29137	59	2	67961	79633	80	3	56713	57601	101	1	92033	
18	36	7817	12497	39	17	17401	19753	60	10	23633	25673	81	2	82193	94033	102	0	114073	201673
19	42	3793	6473	40	14	24953	31649	61	3	82793	89513	82	1	87281	123953	103	0	117193	
20	60	2273	3361	41	13	7193	12113	62	2	48953	78569	83	4	23593	45641	104	0	109433	117881
21	37	4793	6329	42	12	25913	32993	63	5	35593	49033	84	1	68713	109313	105	1	99233	

TABLE 2. For each $k \leq 105$, the second column gives the number n of primes $p < 10^5$ for which $st(C(p^3)) = k^2$. The columns headed p_1 and p_2 give the two smallest primes p for which $st(C(p^3)) = k^2$; only one such prime is known for $k = 101$, 103 and 105.

In this final case, divisibility cannot be replaced by equality: for example if $p = 50177$, we have $r(C(p)) = 0$ whilst $st(C(p)) = 256$.

4E. The Goldfeld–Szpiro Conjecture

In [Goldfeld and Szpiro 1995] it was conjectured that elliptic curves defined over $\mathbb{Q}$ with Shafarevich–Tate group Ш, conductor N, and $\varepsilon > 0$, satisfy

$$o(\text{Ш}) \ll N^{1/2+\varepsilon}.$$

Let GS denote the ratio $o(\text{Ш})/\sqrt{N}$, and dW denote the ratio $o(\text{Ш})/\Delta^{1/12}$ where Δ is the discriminant of the curve in question. In [de Weger 1998] there are several examples of elliptic curves with GS larger than 1, the largest value being 6.893 for the curve mentioned in the introduction. In the same article de Weger proves, assuming the validity of the Birch and Swinnerton-Dyer Conjecture in the rank zero case, that there are many elliptic curves with dW larger than unity (the precise statement is: for all $\varepsilon > 0$, there exist infinitely many elliptic curves E defined over $\mathbb{Q}$ with the property $o(\text{Ш}_E) \gg \Delta^{1/12-\varepsilon}$). For the curves discussed in this paper all values of GS are less than 0.040 but some satisfy dW > 1. The six curves $C(p^3)$ with the largest values of GS are:

p	GS	dW	$st(C(p^3))$
23593	0.0365	2.559	6889
16553	0.0349	2.241	4624
233	0.0343	0.759	64
7193	0.0292	1.522	1681
11353	0.0286	1.672	2601
73	0.0274	0.453	16

Incidently, the elliptic curve $C(4105033^3)$, having the largest sha we have found to date (see Section 4B above), has GS = 0.01228 and dW = 3.1264.

REFERENCES

[Buhler et al. 1985] J. P. 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**:170 (1985), 473–481.

[Cassels 1964] J. W. S. Cassels, "Arithmetic on curves of genus 1, VI: The Tate-Šafarevič group can be arbitrarily large", *J. Reine Angew. Math.* **214/215** (1964), 65–70.

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[Goldfeld and Szpiro 1995] D. Goldfeld and L. Szpiro, "Bounds for the order of the Tate-Shafarevich group", *Compositio Math.* **97**:1-2 (1995), 71–87. Special issue in honour of Frans Oort.

[Rose 1995] H. E. Rose, "On a class of elliptic curves with rank at most two", *Math. Comp.* **64**:211 (1995), 1251–1265, S27–S34.

[Rose 1997] H. E. Rose, "On some classes of elliptic curves with rank two or three", preprint, 1997.

[Rubin 1991] K. Rubin, "The "main conjectures" of Iwasawa theory for imaginary quadratic fields", *Invent. Math.* **103**:1 (1991), 25–68.

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

[de Weger 1998] B. M. M. de Weger, "$A+B=C$ and big Ш's", *Quart. J. Math. Oxford Ser.* (2) **49**:193 (1998), 105–128.

Harvey E. Rose, Department of Mathematics, University Walk, Bristol, BS8 1TW, United Kingdom (h.e.rose@bris.ac.uk)

Received May 26, 1998; accepted in revised form March 8, 1999