MATHEMATICS OF COMPUTATION
Volume 73, Number 245, Pages 323–331
S 0025-5718(03)01547-3
Article electronically published on May 30, 2003

HIGH RANK ELLIPTIC CURVES WITH TORSION GROUP $\mathbb{Z}/(2\mathbb{Z})$

JULIÁN AGUIRRE, FERNANDO CASTAÑEDA, AND JUAN CARLOS PERAL

ABSTRACT. We develop an algorithm for bounding the rank of elliptic curves in the family $y^2 = x^3 - B\,x$, all of them with torsion group $\mathbb{Z}/(2\,\mathbb{Z})$ and modular invariant $j = 1728$. We use it to look for curves of high rank in this family and present four such curves of rank 13 and 22 of rank 12.

1. INTRODUCTION

Let $\mathcal{E}$ be an elliptic curve and let $\mathcal{E}(\mathbb{Q})$ be the group of rational points of $\mathcal{E}$. By Mordell's theorem $\mathcal{E}(\mathbb{Q}) = \mathcal{E}(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^r$, where the nonnegative integer $r = \text{rank}(\mathcal{E})$ is known as the rank of $\mathcal{E}$. The problem of determining the rank is a difficult one, and no general algorithm is known to solve it. It is a widely accepted conjecture that there is no upper bound for the rank of elliptic curves, although no curve (over $\mathbb{Q}$) of rank greater than 24 is known. An example of a curve of rank at least 24 was given by R. Martin and W. McMillen in May 2000. Current records are available at `www.math.hr/~duje/tors/tors.html` (last visited March 2002).

Curves with a torsion point of order two are usually represented as

$$y^2 = x^3 + a\,x^2 + b\,x, \qquad a, b \in \mathbb{Z}, \quad a^2 - 4\,b \neq 0, \tag{1}$$

and show a tendency to have lower ranks. Fermigier ([3], [4]) constructed an infinite family of such curves with rank greater than or equal to 8 and exhibited one with rank exactly 14. A. Dujella gave an example in April 2001 of such a curve with rank exactly 15.

We study the special family of curves

$$y^2 = x^3 - B\,x, \quad B \in \mathbb{Z}, \quad B \text{ not a square}, \tag{$\mathcal{E}_B$}$$

obtained from the one considered by Fermigier by setting $a = 0$ and $b = -B$. All of them have torsion group $\mathbb{Z}/(2\,\mathbb{Z})$ and modular invariant $j = 1728$. Nagao constructed in [6] a polynomial $P(t) \in \mathbb{Q}(t)$ such that $y^2 = x^3 + P(t)\,x$ has four independent points over $\mathbb{Q}(t)$. By specializing t to rational numbers, he found infinitely many curves of rank at least 4 and two of rank at least 6. Curves $(\mathcal{E}_B)$ with B a perfect square have been studied recently in [7].

In [1], the authors exhibited seven values of B for which the corresponding curve has rank at least 8. Since then we have improved our algorithms and found 4 curves

Received by the editor November 28, 2000 and, in revised form, July 5, 2002.
2000 *Mathematics Subject Classification.* Primary 11Y50.
The second and third authors were supported by a grant from the University of the Basque Country.

of rank 13 and 22 of rank 12, as well as a large number of curves whose rank is between 9 and 11. The construction of the curves rests on two pillars:

(1) A strategy to search for curves with high rank, which is a modification of the method described by Fermigier in [4].
(2) Algorithms to obtain lower and upper bounds on the rank, based on the two descent method and the computation of the 2-Selmer group, which are particularly simple for curves of the form $(\mathcal{E}_B)$.

For curves with a torsion point of order two, a theorem of Tate ([11], [10]) reduces the problem of determining their rank to the solvability of a set of diophantine equations, called the homogeneous spaces associated with the curve. The curves $(\mathcal{E}_B)$ are a subset of those to which Tate's Theorem applies, and our algorithm for determining their rank is based on it.

An obvious change of variable shows that without loss of generality, the integer B in $(\mathcal{E}_B)$ can be taken free of fourth powers. Thus, we consider nonzero integers

$$B = \pm p_1^{\alpha_1} \cdots p_N^{\alpha_N},$$

where p_i are (positive) primes and $1 \le \alpha_i \le 3$ for $1 \le i \le N$.

Let $\mathcal{D}(B)$ be the set of squarefree divisors (both positive and negative) of B. Endowed with multiplication modulo $\mathbb{Q}^{*2}$, $\mathcal{D}(B)$ becomes a finite group. An independent set of generators is $\{-1, p_1, \ldots, p_N\}$, so that $\mathcal{D}(B)$ is of order 2^{N+1} and is isomorphic to the direct product of $N+1$ copies of $\mathbb{Z}/(2\,\mathbb{Z})$.

Definition. Let d be a divisor of B. We say that a triple (U, V, Z) of positive integers isolates d if $\gcd(U, V) = 1$ and

$$(\mathcal{C}_d) \qquad d\,U^4 - \frac{B}{d}\,V^4 = Z^2.$$

The diophantine equations $(\mathcal{C}_d)$ are called homogeneous spaces.

Remark 1. Let $d = \hat{d}\,q^2$, with $\hat{d}$ squarefree, be a divisor of B and suppose that (U, V, Z) isolates d. If $r = (q, V)$, then $(q\,U/r, V/r, q\,Z/r^2)$ isolates $\hat{d}$. Thus, there is no loss of generality in considering only squarefree divisors of B.

The set

$$\{d \in \mathcal{D}(B) : d \text{ can be isolated}\} \cup \{1, -\hat{B}\},$$

where $\hat{B}$ is the squarefree part of B, generates a subgroup of $\mathcal{D}(B)$, that we denote by $\mathcal{T}(B)$. Since the order of $\mathcal{D}(B)$ is a power of 2, the order of $\mathcal{T}(B)$ is $2^{r(B)}$ for some nonnegative integer $r(B)$. If $B < 0$, then negative divisors of B cannot be isolated, and we get the following upper bound on the value of $r(B)$:

$$(2) \qquad r(B) \le \begin{cases} N+1 & \text{if } B > 0, \\ N & \text{if } B < 0. \end{cases}$$

We are now ready to restate Tate's Theorem as it applies to curves in the special family $(\mathcal{E}_B)$.

Theorem 1 (Tate)**.**

$$\operatorname{rank}(\mathcal{E}_B) = r(B) + r(-4\,B) - 2.$$

Tate's Theorem and inequality (2) provide an upper bound for $\operatorname{rank}(\mathcal{E}_B)$ in terms of the prime factorization of B, in general much larger than the true value of the rank. A better estimate is obtained from the 2-Selmer group. To get a lower bound on $\operatorname{rank}(\mathcal{E}_B)$, explicit solutions of the homogeneous spaces are exhibited. When these bounds coincide, the exact rank of the curve has been found.

2. Bounds for $\operatorname{rank}(\mathcal{E}_B)$

2.1. **Upper bounds for $r(B)$: the 2-Selmer group.** The 2-Selmer group $S_2(B)$ is defined as the set of all $d \in \mathcal{D}(B)$ such that the homogeneous space $(\mathcal{C}_d)$ is solvable in $\mathbb{Q}_p$ for all primes p (including $\mathbb{Q}_\infty = \mathbb{R}$). For finite primes, we may restrict ourselves to the *bad* primes: $p = 2$ and p odd dividing B. It is clear that $\mathcal{T}(B) \subset S_2(B) \subset \mathcal{D}(B)$. The order of $S_2(B)$ is $2^{s(B)}$ for a nonnegative integer $s(B)$. The 2-Selmer rank of $(\mathcal{E}_B)$ is defined as

$$\mathrm{s}_2\mathrm{rank}(\mathcal{E}_B) = s(B) + s(-4\,B).$$

The criteria for local solvability of the homogeneous spaces associated with the curves $(\mathcal{E}_B)$ are simple, making the computation of $s(B)$ an easy task. We give some of the details for odd primes $p \parallel B$.

Let $\mathcal{P} = \{\, p : p \text{ is an odd prime and } p \parallel B \,\}$. For any $p \in \mathcal{P}$ and $d \in \mathcal{D}(B)$ we have:

- If p does not divide d, then $(\mathcal{C}_d)$ is locally solvable in $\mathbb{Q}_p$ if and only if d is a quadratic residue modulo p.
- If p divides d, then $(\mathcal{C}_d)$ is locally solvable in $\mathbb{Q}_p$ if and only if $-B/d$ is a quadratic residue modulo p.

Define $\mathcal{D}(B,p) = \{\, d \in \mathcal{D}(B) : (\mathcal{C}_d) \text{ is solvable in } \mathbb{Q}_p \,\}$ and

$$S_2(B,\mathcal{P}) = \{\, d \in \mathcal{D}(B) : (\mathcal{C}_d) \text{ is solvable in } \mathbb{Q}_p \text{ for all } p \in \mathcal{P} \,\} = \bigcap_{p\in\mathcal{P}} \mathcal{D}(B,p).$$

It is easy to see that $\mathcal{T}(B) \subset S_2(B) \subset S_2(B,\mathcal{P}) \subset \mathcal{D}(B)$, where the inclusions also hold in the sense of subgroups. The order of $S_2(B,\mathcal{P})$ is $2^{s(B,\mathcal{P})}$ for some nonnegative integer $s(B,\mathcal{P})$, and

$$r(B) \le s(B) \le s(B,\mathcal{P}) \le N+1. \tag{3}$$

Through the identification of $\mathcal{D}(B)$ with $\big(\mathbb{Z}/(2\,\mathbb{Z})\big)^{N+1}$, conditions for local solvability modulo p can be rewritten as linear equations modulo 2, and $S_2(B,\mathcal{P})$ can then be efficiently computed by linear algebra methods. In practice, for each $p \in \mathcal{P}$, we compute a basis of $\mathcal{D}^+(B,p) = \{\, d \in \mathcal{D}(B,\mathcal{P}) : d > 0 \,\}$.

The procedure is essentially the same for odd primes p such that $p^3 \parallel B$ and somewhat more involved for odd primes p such that $p^2 \parallel B$ and for $p = 2$. However, these last computations are carried out only for those B's with $s(B,\mathcal{P})$ large, which are a small fraction of the total.

2.2. **A lower bound for $r(B)$.** As a first step, we choose a family $\mathcal{H}$ of pairs of relatively prime integers (U,V), representing the set of homogeneous spaces to be solved. The larger the $\mathcal{H}$, the more precise is the bound on $r(B)$, but the longer the calculation. Once $\mathcal{H}$ is chosen, carry out the following computations.

(1) Construct $S_2^+(B) = \{\, d \in S_2(B) : d > 0 \,\}$ as described above.

(2) Determine the set of those $d \in S_2^+(B)$ for which there exist $(U,V) \in \mathcal{H}$ such that

$$d\,U^4 - \frac{B}{d}\,V^4 \quad \text{is a perfect square.}$$

(3) Compute the order of the subgroup of $\mathcal{D}(B)$ generated by the divisors of B found in the previous step. This will be 2^r for some integer r. Then,

$$r(B) \geq r(B,\mathcal{H}) =_{\text{def}} \begin{cases} r+1 & \text{if } B>0, \\ r & \text{if } B<0. \end{cases}$$

3. The search strategy

We implement a variation of the method used by Fermigier in [4]. He starts with a monic, even polynomial $p(x) = \prod_{i=1}^{8}(x^2 - a_i^2)$ of degree 16, $a_i \in \mathbb{N}$, and then lets

$$p(x) = \big(q(x)\big)^2 - r(x),$$

where q is is an even polynomial of degree 8 and $r(x) = r_6x^6 + r_4x^4 + r_2x^2 + r_0$. The curve $y^2 = r(x)$ has at least the 32 rational points $(\pm a_i, \pm q(a_i))$, $1 \leq i \leq 8$. For it to have genus 1, $r(x)$ must be of degree 4 and must be irreducible, hence $r_6 = 0$. A sufficient condition for this is

$$a_1^2 + a_2^2 = a_3^2 + a_4^2 = a_5^2 + a_6^2 = a_7^2 + a_8^2.$$

The quartic $y^2 = r_4x^4 + r_2x^2 + r_0$ is interpreted as a homogeneous space for the curve whose cubic model is (1) with a and b given by $a = -r_2/2$ and $b = (a^2 - r_0r_4)/4$. Fermigier goes on to get explicit expressions for a and b in terms of the a_i. It turns out that b is always a multiple of a, so that if $a = 0$, then also $b = 0$ and the curve is singular.

Since we want $a = 0$ and $b \neq 0$, some changes in the above procedure are necessary. We begin with a monic, even polynomial of degree 8

$$p(x) = \prod_{i=1}^{4}(x^2 - a_i^2) = x^8 - s_1x^6 + s_2x^4 - s_3x^2 + s_4,$$

where s_i is the ith elementary symmetric polynomial in 4 variables, $1 \leq i \leq 4$, evaluated at $(a_1^2, a_2^2, a_3^2, a_4^2)$. Then $p = q^2 - r$ with

$$q(x) = x^4 - \frac{s_1}{2}\,x^2 + \frac{s_3}{s_1} \quad \text{and} \quad r(x) = \Big(\frac{s_1^2}{4} + \frac{2\,s_3}{s_1} - s_2\Big)x^4 + \frac{s_3^2}{s_1^2} - s_4.$$

The associated cubic model for the quartic $y^2 = r(x)$ is a curve $(\mathcal{E}_B)$ with

$$B = -\Big(\frac{s_1^2}{4} + \frac{2\,s_3}{s_1} - s_2\Big)\Big(\frac{s_3^2}{s_1^2} - s_4\Big). \tag{4}$$

It has at least the eight rational points $(r_4\,a_i^2, \pm r_4\,a_i\,q(a_i))$, where r_4 is the coefficient of x^4 in r. The right-hand side of (4) is homogeneous of degree 12 in the a_i. Given a quadruple of positive integers (a_1, a_2, a_3, a_4) (which without loss of generality can be taken to be relatively prime), we can find a positive integer multiplier λ such that the quadruple $\lambda(a_1, a_2, a_3, a_4)$, when inserted in (4), produces an integer. In

fact, we can take $\lambda = 2(a_1^2 + a_2^2 + a_3^2 + a_4^2)$. Carrying out the computations and factoring out fourth powers, we get

$$\begin{aligned} B = {} & 4(a_1a_2 + a_3a_4)(a_1a_2 - a_3a_4)(a_1a_3 + a_2a_4)(a_1a_3 - a_2a_4) \\ & \times (a_1a_4 + a_2a_3)(a_1a_4 - a_2a_3)(a_1^2 + a_2^2 - a_3^2 - a_4^2) \\ & \times (a_1^2 - a_2^2 + a_3^2 - a_4^2)(a_1^2 - a_2^2 - a_3^2 + a_4^2)(a_1^2 + a_2^2 + a_3^2 + a_4^2). \end{aligned} \tag{5}$$

For specific values of the quadruple (a_1, a_2, a_3, a_4), the value of B given by the above formula is in general not free of fourth powers, so that a further reduction modulo $\mathbb{Q}^{*4}$ may be necessary. Moreover, if $B < 0$, then we multiply it by -4, and, if necessary, divide it by 16; we denote the result by $B(a_1, a_2, a_3, a_4)$.

4. The results

We have computed upper and lower bounds of the rank of curves $(\mathcal{E}_B)$ with $B = B(a_1, a_2, a_3, a_4)$ using $a_1^2 + a_2^2 + a_3^2 + a_4^2$ as a parameter. Given a positive integer σ, let

$$\mathcal{B}(\sigma) = \{\, B(a_1, a_2, a_3, a_4) : a_1^2 + a_2^2 + a_3^2 + a_4^2 = \sigma \,\}.$$

It can be seen that $\mathcal{B}(2\,\sigma) = \mathcal{B}(\sigma)$, so that it is enough to consider odd values of σ. We computed $\mathcal{B}(\sigma)$ for $1 < \sigma < 302000$. For values of σ between 1 and 20000, we looked for curves of rank at least 9, of which we found over one thousand. Of them, 135 were of rank 10, 19 of rank 11 and one of rank 12. For $\sigma > 20000$ we focused on finding curves of rank greater than or equal to 12, following a process that we describe next.

4.1. **The search algorithm.** We selected two families of homogeneous spaces:

$$\mathcal{H}_1 = \{\, (U, V) : 1 \le V \le U \le 33,\ \gcd(U, V) = 1 \,\},$$
$$\mathcal{H}_2 = \{\, (U, V) : 1 \le U \le 2001,\ 1 \le V \le \min(U, 128),\ \gcd(U, V) = 1 \,\}.$$

The first one has 344 elements and was used to select integers B for which $\operatorname{rank}(\mathcal{E}_B)$ is likely large. The second has 151387 elements and was used to calculate a better lower bound of $\operatorname{rank}(\mathcal{E}_B)$ for those B selected previously. For each $(a_1, a_2, a_3, a_4) \in \mathbb{N}^4$ such that $1 \le a_1 < a_2 < a_3 < a_4$, $\gcd(a_1, a_2, a_3, a_4) = 1$ and $20000 < a_1^2 + a_2^2 + a_3^2 + a_4^2 \le 302000$, we proceed as follows:

(1) Compute $B = B(a_1, a_2, a_3, a_4)$. If B is a perfect square, then reject it.
(2) Compute $s(B, \mathcal{P})$. If $s(B, \mathcal{P}) < 6$, then reject B. Otherwise, go to the next step.
(3) Compute $s(-4\,B, \mathcal{P})$. If $s(B, \mathcal{P}) + s(-4\,B, \mathcal{P}) < 14$, then reject B. Otherwise, go to the next step.
(4) Compute $\mathrm{s}_2\mathrm{rank}(\mathcal{E}_B)$. If $\mathrm{s}_2\mathrm{rank}(\mathcal{E}_B) < 14$, then reject B. Otherwise, go to the next step.
(5) Compute $r(B, \mathcal{H}_1)$. If $r(B, \mathcal{H}_1) < 5$, then reject B. Otherwise, go to the next step.
(6) Compute $R = r(B, \mathcal{H}_2) + r(-4\,B, \mathcal{H}_2)$.

If $R = \mathrm{s}_2\mathrm{rank}(\mathcal{E}_B)$, then $\operatorname{rank}(\mathcal{E}_B) = \mathrm{s}_2\mathrm{rank}(\mathcal{E}_B) - 2$, while if $R < \mathrm{s}_2\mathrm{rank}(\mathcal{E}_B)$, then we only have the inequalities $R - 2 \le \operatorname{rank}(\mathcal{E}_B) \le \mathrm{s}_2\mathrm{rank}(\mathcal{E}_B) - 2$. There are two reasons why this could happen:

(1) Not all $d \in \mathcal{D}(B)$ for which equation $(\mathcal{C}_d)$ has a rational solution have been found.

TABLE 1. Curves of rank 12

B	$(r,\bar{r})$	σ	(a_1,a_2,a_3,a_4)
454 719 638 875 058 296 871 292	(7, 7)	60695	(47, 129, 138, 151)
715 970 874 943 386 994 467 852	(7, 7)	235331	(103, 172, 213, 387)
1 214 095 827 971 924 150 174 460	(8, 6)	245375	(53, 203, 294, 339)
1 645 077 324 548 360 946 504 525	(7, 7)	111035	(21, 47, 184, 273)
5 169 170 820 204 434 510 666 892	(8, 6)	18809	(54, 57, 70, 88)
58 821 272 836 753 123 416 329 100	(8, 6)	204085	(121, 152, 206, 352)
75 678 650 779 410 795 595 704 225	(8, 6)	115045	(62, 152, 176, 239)
15 011 634 178 110 530 936 913 092 525	(7, 7)	134705	(29, 120, 230, 258)
28 135 643 357 680 741 625 006 358 497	(7, 7)	72495	(26, 117, 139, 197)
116 336 368 496 576 127 302 236 525 692	(7, 7)	164775	(37, 198, 239, 259)
172 792 290 506 501 154 725 844 507 900	(7, 7)	112669	(4, 26, 229, 244)
566 685 291 293 488 600 339 545 971 532	(7, 7)	146371	(87, 173, 213, 252)
783 009 180 239 218 955 118 450 366 012	(8, 6)	268279	(154, 181, 211, 409)
2 308 516 307 675 706 889 377 609 045 900	(8, 6)	46995	(17, 33, 44, 209)
3 577 257 554 785 727 695 575 721 968 225	(7, 7)	180449	(5, 30, 210, 368)
9 669 224 911 726 890 971 188 351 254 540	(8, 6)	269875	(161, 253, 283, 316)
365 270 130 088 647 753 858 238 745 495 100	(7, 7)	274365	(72, 74, 251, 448)
634 069 893 288 350 019 987 584 209 395 900	(8, 6)	231613	(58, 125, 320, 332)
14 712 331 120 225 575 885 203 830 147 929 357	(7, 7)	110925	(17, 18, 214, 254)
59 265 540 998 867 979 915 642 579 193 217 100	(8, 6)	110385	(66, 104, 163, 262)
179 951 925 306 622 698 660 887 676 991 871 100	(8, 6)	149017	(6, 16, 90, 375)
368 992 705 100 019 698 676 996 450 186 445 692	(8, 6)	247871	(65, 78, 291, 391)

TABLE 2. Curves of rank 13

B	$(r,\bar{r})$	σ	(a_1,a_2,a_3,a_4)
1 525 990 877 673 927 911 985 309 090	(8, 7)	269125	(72, 186, 329, 348)
2 827 529 113 871 322 622 866 959 217	(8, 7)	31213	(19, 86, 100, 116)
93 922 872 848 724 146 729 053 666 257	(7, 8)	59737	(14, 26, 167, 176)
19 348 006 334 886 975 416 600 173 605 900	(8, 7)	298595	(96, 183, 233, 449)

(2) Equation $(\mathcal{C}_d)$ is solvable in $\mathbb{Q}_p$ for all primes p but has no rational solution. This implies in particular that the Tate-Shafarevich group $Ш_{\mathcal{E}_B}$ is nontrivial.

We found 22 curves of rank 12 and 4 of rank 13. They are listed in Tables 1 and 2, respectively. The first column is the number B; the second is $(r,\bar{r}) = (r(B), r(-4\,B))$; the third column is σ; and the last one is the corresponding quadruple.

4.2. **Rational points on the curves.** From the solutions of the equations

$$d\,U^4 - \frac{B}{d}\,V^4 = Z^2, \quad d \in \mathcal{D}(B), \qquad \bar{d}\,\bar{U}^4 + 4\,\frac{B}{\bar{d}}\,\bar{V}^4 = \bar{Z}^2, \quad \bar{d} \in \mathcal{D}(-4\,B),$$

we obtain rational points of infinite order on the curve $(\mathcal{E}_B)$:

$$\Big(\frac{d\,U^2}{V^2}, \frac{d\,Z\,U}{V^3}\Big), \qquad \Big(\frac{\bar{Z}\,\bar{V}}{4\,\bar{d}\,\bar{U}}, \frac{\bar{Z}\,\bar{V}(\bar{d}\,\bar{U}^2 - 4\,B\,\bar{V}^2)}{8\,\bar{d}\,\bar{U}^3}\Big).$$

TABLE 3. Rational points on $y^2 = x^3 - 152599087767392791198530909 0\,x$

x-coordinate	Height
39413976156831	21.473
40502815695250	17.612
50289827997240	18.948
91403564224440	22.617
94820358842040	22.689
188018729972415	20.454
898132328130375	19.943
$313976463023161/2^2$	33.491
$1838016872665801/6^2$	35.378
$5597088660298249/8^2$	36.438
$10708120954962601/12^2$	37.114
$2041823852075112361/38^2$	42.179
$181177719039357121/42^2$	39.892

TABLE 4. Rational points on $y^2 = x^3 - 28275291138713226228669592 17\,x$

x-coordinate	Height
57802481969281	20.601
2463952792028124	18.874
2659109867774031	18.817
10194232424354319	21.741
53366153545551	21.688
56075012802831	21.916
3193703671713159	20.097
$1362706667330449/2^2$	34.916
$1008541918487401/2^2$	34.637
$2120724718460929/4^2$	35.452
$38895157647413809/10^2$	38.259
$17814532666614649/12^2$	37.590
$19593697986655081/14^2$	37.720

All such points are of the form $P = (a/c^2, b/c^3)$, where a, b and c are integers with $\gcd(a, c) = \gcd(b, c) = 1$. The naïve height of such a point is defined as $h(P) = \log(\max(|a|, |c|^2))$, and the canonical height as $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P)$, where $2\,P$ is the double of the point P. For each of the curves of rank 13, Tables 3 through 6 give the x-coordinate of 13 independent points of infinite order of the Mordell-Weil group of the curve, together with its height. The points have been chosen to have as small a denominator as possible.

4.3. **Final observations.** We finish with some comments and observations coming from the results obtained along our investigations.

(1) The integers B produced by formula (5) have in general many prime factors, which in view of inequality (2) is a somewhat necessary condition for the curve $(\mathcal{E}_B)$ to have high rank. Moreover, the prime factors are in general small, in fact they are bounded by σ. An extreme case is

TABLE 5. Rational points on $y^2 = x^3 - 939228728487241467290536662 57\,x$

x-coordinate	Height
306470225435625	19.897
339591992999857	16.702
1001302871976927	18.148
10361196200475081	18.149
16411319158318513	18.330
$3810572356653064431/7^2$	24.343
743162066478001	34.061
15102001501820401	36.916
574324244593969	33.844
126920957456144329	39.037
1077912054328041	33.287
$27972519349516641/7^2$	36.633
$24848678782121769/2^2$	36.675

TABLE 6. Rational points on $y^2 = x^3 - 193480063348869754166600173605900\,x$

x-coordinate	Height
4399936592496676	24.134
4428422453912205	22.752
7395170181651525	21.061
14431675270763520	21.796
50390034811827670	17.597
66814197937168080	24.292
67885400694630645	19.701
5776295187771364	35.878
133546225497652900	37.145
$17882826281089225/2^2$	36.155
$185226264400224100/3^2$	37.549
$553402906401302500/3^2$	38.584
$113356886513589353881/10^2$	46.179

$B = 10356583068229284172$, for which $\mathrm{rank}(\mathcal{E}_B) = 9$ and

$$B = 2^2 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 31 \cdot 37^2 \cdot 43 \cdot 53 \cdot 59 \cdot 67 \cdot 71.$$

(2) The curves $(\mathcal{C}_d)$ are constructed with four integer points, so that one expects them to have rank greater than or equal to 4. This is true on average for low values of σ: the average of the computed lower estimate of the rank for the curves with $\sigma < 16000$ is slightly above 4. However, as σ grows, this average decreases.

(3) On the other hand, the average of $\mathrm{s}_2\mathrm{rank}(\mathcal{E}_B)$ remains above 5 for all the values of σ in the range of our experiments.

(4) It is relatively easy to find curves with large 2-Selmer rank but with low rank, meaning that they have a large Tate-Shafarevich group. Among the curves coming from $\sigma < 16000$, at least 23 percent of them are such that $\mathrm{rank}(B) = \mathrm{s}_2\mathrm{rank}(\mathcal{E}_B) - 2$, that is, $Ш_{\mathcal{E}_B}[2]$ is trivial. This percentage decreases as σ grows, in accordance with the previous observations.

(5) When solving the homogeneous spaces, we find that for most of the solutions the value of V (and $\bar{V}$) is quite small, in fact most of the time it is equal to 1. As a consequence, we are able to find rational points on the curves with small denominator.
(6) All the computations were done on a desktop computer using *Mathematica*®.

Acknowledgments

The authors are grateful to the anonymous referee, whose helpful comments lead us to write new, more efficient algorithms for the computation of the Selmer rank, allowing us to extend the search. The referee also informs us that recently N. Elkies came to the same parametrization by specializations of the families E_8 of Shioda ([8]) and $D_4 + \mathbb{Z}/(2\mathbb{Z})$ of Shioda and Usui ([9]) and that the search has been extended to $\sigma < 4 \cdot 10^6$. This search has produced a curve of rank 14, with $(a_1, a_2, a_3, a_4) = (744, 750, 1030, 1031)$ and $\sigma = 3239897$ (found by M. Watkins), and at least 12 new curves of rank 13. The one corresponding to $(a_1, a_2, a_3, a_4) = (304, 722, 1136, 1433)$ and $\sigma = 3957685$ yields a value of B smaller than those in Table 2.

References

[1] Aguirre, J., Castañeda, F. and Peral, J.C., *High rank elliptic curves of the form $y^2 = x^3 + B\,x$*, Revista. Mat. Compl., **XIII**, num. 1, (2000), 1–15. MR **2001i:**11065
[2] Cremona, J.E., *Algorithms for Modular Elliptic Curves*, Cambridge U. Press, Cambridge, (1992). MR **93m:**11053
[3] Fermigier, S., *Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possedant des points d'ordre* 2, C. R. Acad. Sci. Paris Ser. I Math., **322** (1996), 949–952. MR **97b:**11073
[4] Fermigier, S., *Construction of high-rank elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$ with nontrivial 2-torsion* (extended abstract), in Algorithmic Number Theory (Talence, 1996), Springer, Berlin, (1996). MR **97m:**11071
[5] Fermigier, S., *Une courbe elliptique definie sur $\mathbb{Q}$ de rang $\geq$ 22*, Acta Arith., **82** (1997), 359–363. MR **98j:**11041
[6] Nagao, K., *On the rank of the elliptic curves $y^2 = x^3 - k\,x$*, Kobe J. Math., **11** (1994), 205–210. MR **96c:**11060
[7] Rogers, N.F., *Rank Computations for the congruent number elliptic curves*, Experimental Mathematics, **9** (2000), 591–594. MR **2001k:**11104
[8] Shioda, T., *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan, **43** (1991), 673–719. MR **92i:**11059
[9] Shioda, T. and Usui, H., *Fundamental invariants of Weyl groups and excellent families of elliptic curves*, Comment. Math. Univ. St. Paul, **41** (1992), 169–217. MR **93m:**11047
[10] Silverman, J.H. and Tate, J., "Rational points on elliptic curves", UTM, Springer-Verlag, Berlin, 1992. MR **93g:**11003
[11] Tate, J., "Rational points on elliptic curves", Phillips Lectures, Haverford College, 1961.

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
E-mail address: mtpagesj@lg.ehu.es

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
E-mail address: mtpcabrf@lg.ehu.es

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
E-mail address: mtppealj@lg.ehu.es