REVISTA MATEMÁTICA COMPLUTENSE
(2000) vol. XIII, num. 1, 17-31
http://dx.doi.org/10.5209/rev_REMA.2000.v13.n1.17088
ISNN 1139-1138

HIGH RANK ELLIPTIC CURVES OF THE FORM $y^2 = x^3 + B\,x$

J. AGUIRRE, F. CASTAÑEDA and J.C. PERAL

Abstract

Seven elliptic curves of the form

$$y^2 = x^3 + B\,x$$

and having rank at least 8 are presented. To find them we use the double descent method of Tate. In particular we prove that the curve with $B = -14752493461692$ has rank exactly 8.

1 Introduction

Let E be a non-singular elliptic curve over $\mathbb{Q}$. According to the Mordell-Weil theorem the set Γ of $\mathbb{Q}$-rational points of E is a finitely generated abelian group, the operation of the group being the classically named "chord and tangent" addition of points.

The structure theorem for abelian groups tells us that

$$\Gamma = T \oplus \mathbb{Z}^r,$$

T being the torsion part and $\mathbb{Z}^r$ the free part of the group. The number r is called the rank of the elliptic curve.

The structure of the finite group T is well-known due to a theorem of Mazur, ([MZ1] and [MZ2]), stating that the only possibilities for T are

$$T = \begin{cases} \mathbb{Z}/n, & 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2 \oplus \mathbb{Z}/(2k), & 1 \leq k \leq 4, \end{cases}$$

and that all these 15 possibilities occur. On the other hand, the theorem of Nagel and Lutz gives, in our case, a direct way for finding the points of finite order with a modest amount of computation.

1991 Mathematics Subject Classification: 11040.
Servicio de Publicaciones. Universidad Complutense. Madrid, 2000

The determination of the rank is more difficult: no algorithmic procedure is known, given a particular curve, for the determination of its rank or the generators of the group Γ.

As mentioned above, the maximum order that a torsion point can have is 12. A bound for the size of the rank it is not known. Even though a generally accepted conjecture states that there are elliptic curves of arbitrarily large rank, the largest ranks known until now are the Nagao example, ([N1]), where a curve with rank 21 is exhibited and a curve with rank 22 found by Fermigier ([F2]).

The following table shows how the largest known rank has increased in time:

1948	Wiman ([W1])	$r \geq 4$
1975	Penney, Pomerance ([PP1])	$r \geq 7$
1977	Grunewald, Zimmert ([GZ1])	$r \geq 8$
1977	Brumer, Kramer ([BK1])	$r \geq 9$
1979	Nakata ([NK1])	$r \geq 9$
1982	Mestre ([M1])	$r \geq 12$

Later on, in a series of papers, ([M2] and [M3]), Mestre constructed curves over $\mathbb{Q}(t)$ with $\mathbb{Q}(t)$-rank at least 11 and 12. By specializing, he gave examples of curves whose rank over $\mathbb{Q}$ is at least 15 ([M4]).

The same kind of ideas have been used by other authors to give examples of curves and families of curves with high rank, both over $\mathbb{Q}$ and $\mathbb{Q}(t)$, and of curves whose torsion group is assumed to be one of the groups allowed by Mazur's theorem.

For example, for curves with torsion group equal to $\mathbb{Z}/2$, Fermigier ([F1]) has shown a family of curves over $\mathbb{Q}(t)$, with a torsion point of order two and Mordell-Weil group of rank greater than 8, and an example of a curve with a torsion point of order two whose Mordell-Weil group over $\mathbb{Q}$ has rank 14.

Kihara in a series of articles, ([K1], [K2] and [K3]), has shown an infinite family of curves over $\mathbb{Q}$ with rank at least 14, and other results where the torsion group has a predetermined shape.

Nagao in [N2] considers a special family of elliptic curves having torsion group equal to $\mathbb{Z}/2$ and invariant $j = 1728$, namely, curves of the form

$$y^2 = x^3 + B\,x. \tag{1}$$

He constructs a polynomial $P(t) \in \mathbb{Q}(t)$ for which the elliptic curve $y^2 = x^3 + P(t)\,x$ has four independent points over $\mathbb{Q}(t)$. By specializing t to rational numbers he finds infinitely many elliptic curves over $\mathbb{Q}$ of the form (1) and whose rank is at least 4. Moreover he finds two curves of the same form whose rank over $\mathbb{Q}$ is at least 6.

The purpose of this note is to present seven elliptic curves over $\mathbb{Q}$ of the form (1) with rank at least 8. As in Nagao's article, our curves have torsion group equal to $\mathbb{Z}/2$ (and $j = 1728$), but our method is different and more elementary.

2 The method

In what follows we restrict our attention to elliptic curves of the form

$$y^2 = x^3 + A\,x^2 + B\,x \quad \text{with} \quad A^2 - 4\,B \neq 0, \tag{2}$$

and later on we will construct our examples with $A = 0$, showing in more detail the computations for one of the curves.

Before giving the examples we have found and explaining how we searched for the values of B producing these particular curves, we outline the procedure we have followed to get estimates for the rank. As general references for these and many other related topics, see [H1], [S1] and [S2].

We use the two isogenies method together with some considerations for a guided search for "good" values of B. In particular, we use several congruence relations related to the Birch and Swinnerton-Dyer conjecture, and we restrict B to a certain bi-parametric sequence where a minimum set of solutions for a crucial diophantine equation appearing in the process is guaranteed.

First we sketch these ideas and then we present the main results of our search.

Associated with the elliptic curve (2) is the curve

$$y^2 = x^3 - 2\,A\,x^2 + (A^2 - 4\,B)x. \tag{3}$$

We denote by Γ and $\bar{\Gamma}$ the group of rational points in the curve and the associated curve respectively.

From the formula for doubling a point, if $(x, y) = 2\,P$ with $P \in \Gamma$, then $x \in \mathbb{Q}^{*2}$, that is, x is the square of a rational number. The same is true for $\bar{\Gamma}$.

The mapping $\alpha\colon \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\alpha((x,y)) = \begin{cases} x \cdot \mathbb{Q}^{*2} & \text{if } x \neq 0, \\ B \cdot \mathbb{Q}^{*2} & \text{if } (x,y) = (0,0), \\ 1 \cdot \mathbb{Q}^{*2} & \text{if } (x,y) = \mathcal{O}, \end{cases}$$

where $\mathcal{O}$ is the point at infinity, is a group homomorphism, as well as the analog application $\bar{\alpha}$ defined on $\bar{\Gamma}$.

The following theorems of Tate (see [T1] or [ST1]) are the principal theoretical tool used to estimate the rank in the case, as is ours, of curves with a torsion point of order two.

Theorem 1. (Tate). *The rank, r, of the curve $y^2 = x^3 + A\,x^2 + B\,x$ satisfies the identity*

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4},$$

where $|\cdot|$ stands for the cardinality of the corresponding set.

Thus, estimating the rank is equivalent to calculating the cardinal of the images of α and $\bar{\alpha}$. The next theorem gives a description of these images in terms of the solutions of certain diophantine equations, called the homogeneous spaces associated with the curve.

For each divisor d of B consider the equation

$$U^4 \cdot d + V^4 \cdot \frac{B}{d} + U^2 \cdot V^2 \cdot A = N^2 \qquad (*)_d$$

in the unknowns (U,V,N), with $U \cdot V \neq 0$, and the primality conditions $\gcd(U,V) = 1$, $\gcd(U,N) = 1$, $\gcd(U,B/d) = 1$, $\gcd(V,N) = 1$ and $\gcd(V,d) = 1$. Observe that for each integral solution (U,V,N) of $(*)_d$, a rational point of the curve is given by the formula

$$(x,y) = \Big(\frac{d\,U^2}{V^2}, \frac{(B/d) \cdot U\,V}{V^3}\Big).$$

Theorem 2. (Tate). *The image of α is given by*

$$\alpha(\Gamma) = \{\mathbb{Q}^{*2}, B\,\mathbb{Q}^{*2}\} \cup \{\, d\,\mathbb{Q}^{*2} : d|B \text{ and } (*)_d \text{ has a solution.}\,\} \qquad (4)$$

The analog statement is valid for $\bar{\alpha}(\bar{\Gamma})$.

The idea behind the proof of these theorems is to use the Mordell-Weil theorem and the fact that the operation of doubling points is given by a rational function of degree four that can be factorized as the composition of two rational functions ϕ and ψ (called isogenies), $\phi\colon \Gamma \to \bar{\Gamma}$ and $\psi\colon \bar{\Gamma} \to \Gamma$, each of degree two, with $\phi(\psi(P)) = 2P$ and each being a homomorphism of groups. Next, it is proved that the kernels of ϕ and ψ are the images of the applications α and $\bar{\alpha}$ respectively, and finally an argument about the order of these groups gives the theorems.

In that way the problem of calculating the rank is reduced to deciding whether or not the equations $(*)_d$, one for each divisor of B, and the analog equations for the divisors of $b = A^2 - 4B$, have a solution.

The main difficulty with this approach is that no method is known for deciding if such an equation has a solution. Even worse, there are equations of this kind without solution, but with solution modulo m for all the integers m. Thus, in some cases, they can't be discarded by congruence arguments and more involved ideas are needed to decide about the existence of solutions. In other words, the local-global principle of Hasse, valid for other kind of diophantine equations such as the ones related to the conics, is not valid in the present context.

Another theoretical tool used as a guide in the process of our search for the values of B, is the conjecture of Birch and Swinnerton-Dyer, which links the rank of an elliptic curve with the order of the zero at $s = 1$ of the L-function attached to that curve, predicting that both numbers are the same. If the Birch and Swinnerton-Dyer conjecture is true, then to a curve with high rank corresponds an L-function with a zero of high order at 1.

The way we use the conjecture of Birch and Swinnerton-Dyer is the following heuristic argument. For each prime p, let N_p be the number of solutions of $y^2 = x^3 + Ax^2 + Bx$ over the finite field $\mathbb{F}_p$ and

$$M_p = \sum_{x=1}^{p} \left(\frac{x^3 + Ax^2 + Bx}{p} \right), \text{ where } \left(\frac{\cdot}{p} \right) \text{ is the Jacobi symbol.}$$

Then $N_p = p + 1 + M_p$, and the value of the L-function at 1 is given by $\prod_p \frac{p}{N_p}$. Thus, in principle, the bigger the M_p the higher the order of the zero of L at 1, and this should be reflected in a distribution of the M_p near to its maximum possible value for a substantial set of primes. In consequence we look for values of A and B which maximize M_p for

small primes.

Now we explain how all this is used, why we impose additional restrictions on B, and finally present the results of our computer search. The computations were carried out with the software *Mathematica* on a desktop computer.

From now on we will take curves of the form

$$y^2 = x^3 + B\,x, \qquad B \neq 0.$$

The associated curve is

$$y^2 = x^3 + b\,x, \qquad b = -4\,B.$$

Motivated by the ideas just explained, we look for values of B having several divisors d which satisfy the diophantine equations corresponding to the homogeneous spaces.

In order to automatically fulfill the primality conditions, we begin our search by taking $(U, V) = (1, 1)$, so that we look for values of B for which there are solutions of the form $(1, 1, N)$ for a large number of equations $(*)_d$. This is equivalent to

$$d + \frac{B}{d} = \text{a perfect square for } d \text{ a divisor af } B. \tag{5}$$

As mentioned in the previous discussion, we introduce another restriction for the values of B in order to guarantee at least two solutions for the equation (5). Consider

$$B = q\,d\,h,$$

where q is a free (integer) parameter and d, h are chosen so that both d and $q\,d$ satisfy (5). This yields the equations

$$\begin{aligned} q\,h + d &= m^2, \\ h + q\,d &= n^2, \end{aligned}$$

for some integers m and n. From this we arrive at

$$\begin{aligned} (q^2 - 1)d &= q\,n^2 - m^2, \\ (q^2 - 1)h &= q\,m^2 - n^2. \end{aligned}$$

Since we want d and h to be integers we are forced to impose another restriction on the possible values of m and n:

$$q^2 - 1 \text{ divides } q\,n^2 - m^2 \text{ and } q\,m^2 - n^2.$$

Then

$$B = q \cdot \frac{q\,n^2 - m^2}{q^2 - 1} \cdot \frac{q\,m^2 - n^2}{q^2 - 1}.$$

For example if $q = 2$, then $2\,m^2 - n^2$ must be divisible by 3, which implies that both m and n must be divisible by 3. Thus we get

$$d = 3(2\,n^2 - m^2),\ h = 3(2\,m^2 - n^2) \text{ and } B = 18(2\,n^2 - m^2)(2\,m^2 - n^2).$$

Furthermore, it is desirable that d and $2\,d$ give raise to independent points. This can be achieved by choosing n odd.

If we take $q = 4$, then $4\,n^2 - m^2$ and $4\,m^2 - n^2$ must be divisible by 15, giving rise to several possibilities.

There is something for and something against choosing q a perfect square, like $q = 4$. On the one hand, the factorizations $4\,n^2 - m^2 = (2\,n+m)(2\,n-m)$ and $4\,m^2 - n^2 = (2\,m+n)(2\,m-n)$ guarantee that B has a large number of factors and are an aid in lowering the computing time. On the other, d and $4\,d$ are equivalent modulo $\mathbb{Q}^{*2}$.

A new restriction comes from the desire of maximizing the Jacobi sums

$$M_p(B) = \sum_{x=1}^{p} \Big(\frac{x^3 + Bx}{p}\Big).$$

For $p \equiv 3 \bmod 4$ these sums are equal to zero for every value of B. For $p = 5$, the maximum value is achieved when

$$B \equiv 3 \bmod 5,$$

a condition that we impose in most of the runs of the program. In fact when we run an unrestricted search, only a small percentage of the B's found do not satisfy that condition. Other conditions of this kind were used during the running of the program.

3 Results

We present the results obtained in table 1. In many cases the number found in our search had as factors fourth powers. The number appearing in the table is then that number reduced modulo $\mathbb{Q}^{*4}$. An easy argument shows that this does not affect the value of the rank.

Table 1: Curves with $r \geq 8$.

B	Factorization of B
-14752493461692	$-1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 23 \cdot 71 \cdot 113 \cdot 281 \cdot 1129$
-22574232092412	$-1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 37 \cdot 43 \cdot 53$
-130692175866252	$-1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 53 \cdot 61 \cdot 151$
-173761825769532	$-1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 41 \cdot 47 \cdot 61 \cdot 127$
-254590018539857	$-1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 53 \cdot 419 \cdot 719 \cdot 937$
-30307917919972	$-1 \cdot 2^2 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 53 \cdot 251 \cdot 6449$
-128566324306497	$-1 \cdot 3 \cdot 7 \cdot 11 \cdot 23 \cdot 59 \cdot 107 \cdot 449 \cdot 8537$

Next we give some arithmetical details about the first curve. Moreover in this example we are able to prove that the estimate for the rank is actually an equality, i.e., we prove

Theorem 3. *The elliptic curve*

$$y^2 = x^3 - 14752493461692\, x \tag{6}$$

has rank equal to 8.

Proof. B factorizes as $B = -1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 23 \cdot 71 \cdot 113 \cdot 281 \cdot 1129$, so that it has exactly 512 square-free divisors (including the negatives) and $|\alpha(\Gamma)| \leq 512 = 2^9$.

In the case of $b = -4\,B$, there are also 512 square-free divisors, but since $b > 0$, the homogeneous spaces for $d|b$ and $d < 0$ have no positive real solution, and hence only 256 positive square-free divisors of b have to be considered. This gives the upper bound $|\bar{\alpha}(\bar{\Gamma})| \leq 256 = 2^8$. Thus we get

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4} \leq \frac{2^9 \cdot 2^8}{2^2} = 2^{15}, \quad \text{and hence} \quad r \leq 15.$$

By the search procedure explained above we found eight pairs (d, N), with d divisor of B, which are solution of the diophantine equation

$$d + \frac{B}{d} = N^2. \tag{7}$$

The set (d, N) of these pairs, appears in table 2. The factorization of the values of d is also included.

Table 2: Divisors of B solution of (7).

d	Factorization of d	N
3875109	$3 \cdot 7 \cdot 23 \cdot 71 \cdot 113$	261
5358234	$2 \cdot 3 \cdot 7 \cdot 113 \cdot 1129$	1614
6662229	$3 \cdot 7 \cdot 281 \cdot 1129$	2109
7750218	$2 \cdot 3 \cdot 7 \cdot 23 \cdot 71 \cdot 113$	2418
9636333	$3 \cdot 7 \cdot 23 \cdot 71 \cdot 281$	2847
19272666	$2 \cdot 3 \cdot 7 \cdot 23 \cdot 71 \cdot 281$	4302
33185826	$2 \cdot 3^2 \cdot 23 \cdot 71 \cdot 1129$	5722
645284466	$2 \cdot 3^2 \cdot 113 \cdot 281 \cdot 1129$	25402

Let D be the set of divisors d of B appearing in the first column of table 2 and S the subgroup of $\mathbb{Q}^{*2}$ generated by $D \cup \{1, B\}$. An independent set of generators for S is

$$G_S = \{ -1 \cdot 7,\ 2,\ 3 \cdot 7 \cdot 281,\ 23 \cdot 71,\ 113 \cdot 281,\ 1129 \}.$$

This implies that $2^6 = |S| \leq |\alpha(\Gamma)|$.

For the associated curve we found five solutions (d, N) of the equation

$$d + \frac{b}{d} = N^2 \quad \text{with } d \text{ divisor of } b. \tag{8}$$

The values of N and the factorization of these divisors are listed in table 3.

As before, let $\bar{D}$ be the set of divisors d of b appearing in the first column of table 3 and $\bar{S}$ the subgroup of $\mathbb{Q}^{*2}$ generated by $\bar{D} \cup \{1, b\}$. Then $\bar{S}$ has 2^4 elements and a system of generators is

$$G_{\bar{S}} = \{ 7 \cdot 71 \cdot 281,\ 23 \cdot 281,\ 113 \cdot 281,\ 1129 \},$$

Table 3: Divisors of b solution of (8).

d	Factorization of d	N
46948336	$2^4 \cdot 23 \cdot 113 \cdot 1129$	76207
63405769	$7 \cdot 71 \cdot 113 \cdot 1129$	38104
143396548	$2^2 \cdot 113 \cdot 281 \cdot 1129$	11992
1451874172	$2^2 \cdot 7 \cdot 23 \cdot 71 \cdot 113 \cdot 281$	8021
5807496688	$2^4 \cdot 7 \cdot 23 \cdot 71 \cdot 113 \cdot 281$	6943

implying

$$2^4 = |\bar{S}| \leq |\bar{\alpha}(\bar{\Gamma})|.$$

This, together with Theorem 1, give a lower estimate for the rank of the curve:

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4} \geq \frac{2^6 \cdot 2^4}{2^2} = 2^8 \Rightarrow r \geq 8.$$

In order to get that the rank is exactly 8, we have to prove that the order of the subgroups generated by the images of α and $\bar{\alpha}$ are exactly 2^6 and 2^4 respectively.

For the curve (6) we are able to prove, arguing with congruences of adequate moduli, that there are several homogeneous spaces without solution. In this way we get divisors of B (respectively b) which are not in $\alpha(\Gamma)$ (respectively not in $\bar{\alpha}(\bar{\Gamma})$).

For any divisor d of B such that $d \in \alpha(\Gamma)$, if d' is another divisor of B with $d' \notin \alpha(\Gamma)$, then $d \cdot d' \notin \alpha(\Gamma)$. Using this fact, we split the 512 divisors of B (counted mod $\mathbb{Q}^{*2}$) into two classes: the 64 already found, which are in $\alpha(\Gamma)$, and 448 which are not in that image. This implies that $|\alpha(\Gamma)|$ is exactly equal to 2^6.

For the associated curve we can discard all the negative divisors of b, because the corresponding homogeneous space do not have positive real solutions. We are left with 256 divisors of b (modulo $\mathbb{Q}^{*2}$), of which 16, those generated by $\bar{D} \cup \{1, b\}$, are in the image of $\bar{\alpha}$.

Observe that in proving that a divisor d of B is not in $\alpha(\Gamma)$, one has to take care of the homogeneous spaces for d and for all the divisors of B equivalent to d modulo $\mathbb{Q}^{*2}$. For example, when considering $d = 23$, as divisor of B, one has to study the homogeneous spaces corresponding

to 23, $23 \cdot 4$, $23 \cdot 9$ and $23 \cdot 36$. For $d = 23$, as divisor of b, we have to study the equations for 23, $23 \cdot 4$, $23 \cdot 9$, $23 \cdot 36$, $23 \cdot 16$ and $23 \cdot 144$.

Let us call D_B the set of square-free divisors of B. As mentioned above, D_B has 512 elements.

We observe that the equations for the homogeneous spaces for all the divisors of B such that $d \equiv 3 \bmod 4$, together with the primality conditions, have no solution modulo 4. This gives a set N_1 of 128 divisors of B outside $\alpha(\Gamma)$. When we multiply N_1 times the set S of 64 divisors found in $\alpha(\Gamma)$, we get a new set, N_2, of divisors not in that image. This set N_2 has 256 elements.

In table 4 we include a set L of divisors of B in the first column, together with the equivalent set of divisors and the moduli used to prove that the corresponding homogeneous space is empty in the second and third.

Table 4:

$d \in L$	Equivalent divisors	Modulus
3	$3 \cdot 4$	7
7	$7 \cdot 4$, $7 \cdot 9$, $7 \cdot 36$	7
21	$21 \cdot 4$	23
23	$23 \cdot 4$, $23 \cdot 9$, $21 \cdot 36$	4
42		23
69	$69 \cdot 4$	7
161	$161 \cdot 4$, $161 \cdot 9$, $161 \cdot 36$	23
483	$483 \cdot 4$	23

For example, for $d = 3$ we have to consider two diophantine equations, one for each of the equivalent forms of $3 \bmod \mathbb{Q}^{*2}$ inside the set of divisors of B (3 and $3 \cdot 4$). The equations are:

$$3 \cdot U^4 + \frac{B}{3} \cdot V^4 = N^2 \quad \text{and} \quad 3 \cdot 4 \cdot U^4 + \frac{B}{3 \cdot 4} \cdot V^4 = N^2.$$

If we take these equations modulo 7, because of the primality conditions, it is enough to use the following values:

$$U = \{1, 2, 3, 4, 5, 6\} \quad \text{and} \quad V = \{1, 2, 3, 4, 5, 6, 7\}.$$

In all the 42 cases we get a residue in one of the classes 3, 5 or 6 modulo 7, which are exactly the non-quadratic residues. So neither equation is solvable and hence $3 \notin \alpha(\Gamma)$.

When we multiply the elements in the set of divisors not in the image of α defined by $N_2 = N_1 \cup L$ times S, a new set of divisors outside the image of α is obtained. This set has 448 elements, which together with the 64 elements in S gives the total set D_B. This implies that $|\alpha(\Gamma)| = 2^6$.

The argument for b and $\bar{\alpha}(\bar{\Gamma})$ is similar. We observe that in this case the set of positive divisors has 256 elements, the set $\bar{S}$ has 2^4 elements and for any $d \equiv 2 \bmod 3$, the homogeneous space has no solution modulo 3. So we have a set, $\bar{N}_1$, of 64 elements outside $\bar{\alpha}(\bar{\Gamma})$. The set $\bar{N}_1$ multiplied by $\bar{S}$ produces a new set, $\bar{N}_2$, of 128 elements not in $\bar{\alpha}(\bar{\Gamma})$. In table 5 we list a set $\bar{L}$ of divisors of b for which the corresponding homogeneous space is empty, together with the moduli used to prove the non solvability

Table 5:

$d \in \bar{L}$	Equivalent divisors	Modulus
3	$3 \cdot 4$, $3 \cdot 16$	7
6	$6 \cdot 4$	7
7	$7 \cdot 4$, $7 \cdot 9$, $7 \cdot 16$, $7 \cdot 36$, $7 \cdot 144$	23
21	$21 \cdot 4$, $21 \cdot 16$	23
42	$42 \cdot 4$	23
46	$46 \cdot 4$, $46 \cdot 9$, $46 \cdot 36$	23
69	$69 \cdot 4$, $69 \cdot 16$	23
138	$138 \cdot 4$, $138 \cdot 16$	23
142	$142 \cdot 4$, $142 \cdot 9$, $142 \cdot 36$	4
213	$213 \cdot 4$, $213 \cdot 16$	7
426	$426 \cdot 4$	7

Next we observe that $\bar{N}_2 \cup \bar{L}$ times $\bar{S}$ is a set of 240 elements, which proves that the image of $\bar{\alpha}$ has exactly 2^4 elements. This concludes the proof that the rank of Γ is exactly equal to 8. ■

Finally, in table 6 we list the values of B, reduced modulo $\mathbb{Q}^{*4}$, found in our search, for which the curve (1) has rank at least seven.

Table 6: Curves with $r \geq 7$.

B	Factorization of B
-2172367197	$-1 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 59 \cdot 61 \cdot 67$
-15380890602	$-1 \cdot 2 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 71$
-51891702972	$-1 \cdot 2^2 \cdot 3 \cdot 17 \cdot 29 \cdot 41 \cdot 349 \cdot 613$
-158697338877	$-1 \cdot 3^2 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 71 \cdot 73 \cdot 113$
-202052651805	$-1 \cdot 3^2 \cdot 5 \cdot 19 \cdot 53 \cdot 101 \cdot 131 \cdot 337$
-220952437692	$-1 \cdot 2^2 \cdot 3 \cdot 7 \cdot 19 \cdot 137 \cdot 233 \cdot 4337$
-244629607677	$-1 \cdot 3 \cdot 7^2 \cdot 13 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 151$
-247121673777	$-1 \cdot 3^2 \cdot 11 \cdot 19 \cdot 23 \cdot 41 \cdot 127 \cdot 1097$
-343928823777	$-1 \cdot 3^2 \cdot 7 \cdot 11 \cdot 17 \cdot 29 \cdot 41 \cdot 43 \cdot 571$
-345987474525	$-1 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23 \cdot 31 \cdot 37 \cdot 757$
-507158904252	$-1 \cdot 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41 \cdot 83 \cdot 653$
-606799510317	$-1 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 59 \cdot 139 \cdot 191$
-667630174332	$-1 \cdot 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 43 \cdot 71 \cdot 223$
-1238514463725	$-1 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 19 \cdot 31 \cdot 79 \cdot 419$
-1667390880687	$-1 \cdot 3 \cdot 7 \cdot 17 \cdot 19 \cdot 43 \cdot 109 \cdot 179 \cdot 293$
-3338186079921	$-1 \cdot 3 \cdot 7^2 \cdot 11 \cdot 41 \cdot 47 \cdot 71 \cdot 79 \cdot 191$
-4871074840632	$-1 \cdot 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61 \cdot 103 \cdot 347$
-6317726835420	$-1 \cdot 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 89 \cdot 163 \cdot 2417$
-9423877722525	$-1 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 101 \cdot 107 \cdot 461 \cdot 1201$
-11784209924921	$-1 \cdot 7 \cdot 17^2 \cdot 37 \cdot 47 \cdot 61 \cdot 89 \cdot 617$
-14280772851345	$-1 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13^2 \cdot 19 \cdot 53 \cdot 97 \cdot 107$
-15888014186316	$-1 \cdot 2^2 \cdot 3 \cdot 19 \cdot 23 \cdot 47 \cdot 53 \cdot 61 \cdot 127 \cdot 157$
-30307917919972	$-1 \cdot 2^2 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 53 \cdot 251 \cdot 6449$
-43409660388237	$-1 \cdot 3^2 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 79 \cdot 317 \cdot 1889$
-45904825606332	$-1 \cdot 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 43 \cdot 73 \cdot 1277$
-56630455507332	$-1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 73 \cdot 103 \cdot 167 \cdot 191 \cdot 937$
-67837692616317	$-1 \cdot 3^2 \cdot 13 \cdot 19 \cdot 29 \cdot 43 \cdot 127 \cdot 233 \cdot 827$
-159848787638232	$-1 \cdot 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 37 \cdot 47 \cdot 89 \cdot 241 \cdot 773$
-212035673488892	$-1 \cdot 2^2 \cdot 11 \cdot 23 \cdot 41 \cdot 59 \cdot 79 \cdot 89 \cdot 97 \cdot 127$
-287749273343532	$-1 \cdot 2^2 \cdot 3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19 \cdot 47 \cdot 79 \cdot 179 \cdot 271$
-2396200602455352	$-1 \cdot 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 61 \cdot 101 \cdot 103 \cdot 127 \cdot 173$

References

[BK1] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J., **44** (1977), 715–743.

[F1] S. Fermigier, *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.

[F2] ———, *Une courbe elliptique definie sur $\mathbb{Q}$ de rang $\geq$ 22*, Acta Arith., **82** (1997), 359–363.

[GZ1] F. J. Grunewald and R. Zimmert, *Uber einige rationale elliptische Kurven mit freiem Rang $\geq$ 8* J. Reine Angew. Math., **296** (1977), 100–107.

[H1] D. Husemöller, "Elliptic curves", Springer-Verlag, Berlin, 1987.

[K1] S. Kihara, *On a infinite family of elliptic curves with rank $\geq$ 14 over $\mathbb{Q}$*, Proc. Japan Acad. Ser. A Math., **73** (1997), 32.

[K2] ———, *On the rank of elliptic curves with three rational points of order two*, Proc. Japan Acad. Ser. A Math., **73** (1997), 77–78.

[K3] ———, *On the rank of elliptic curves with three rational points of order two II*, Proc. Japan Acad. Ser. A Math., **73** (1997), 151.

[MZ1] B. Mazur, *Modular curves and the Eisestein ideal*, IHES Publi. Math, **47** (1977), 33–186.

[MZ2] ———, *Rational isogenies of prime degree*, Invent. Math., **44** (1978), 129–162.

[M1] J. F. Mestre, *Construction d'une courbe elliptique de rang $\geq$ 12*, C. R. Acad. Sci. Paris Ser. I Math., **295** (1982), 643–644.

[M2] ———, *Courbes elliptiques de rang $\geq$ 11 sur $\mathbb{Q}(t)$*, C. R. Acad. Sci. Paris Ser. I Math., **313** (1991), 139–142.

[M3] ———, *Courbes elliptiques de rang $\geq$ 12 sur $\mathbb{Q}(t)$*, C. R. Acad. Sci. Paris Ser. I Math., **313** (1991), 171–174.

[M4] ———, *Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang $\geq$ 15*, C. R. Acad. Sci. Paris Ser. I Math., **314** (1992), 453–455.

[N1] K. Nagao, *An example of elliptic curve over $\mathbb{Q}$ with rank $\geq$ 21*, Proc. Japan Acad. Ser. A, **70** (1994), 104–105.

[N2] ———, *On the rank of the elliptic curves $y^2 = x^3 - k\,x$* , Kobe J. Math., **11** (1994), 205–210.

[NK1] K. Nakata, *On some elliptic curves defined over* $\mathbb{Q}$ *of free rank* ≥ 9, Manuscripta Math., **29** (1979), 183–194.

[PP1] D. Penney and C. Pomerance, *Three elliptic curves with rank at least seven*, Math. Comp., **29** (1975), 965–968.

[S1] J. H. Silverman, "The arithmetic of elliptic curves", Springer-Verlag, Berlin, 1986.

[S2] ———, "Advanced topics in the arithmetic of elliptic curves", Springer-Verlag, Berlin, 1994.

[ST1] J. H. Silverman and J. Tate, "Rational points on elliptic curves", UTM, Springer-Verlag, Berlin, 1992.

[T1] J. Tate, "Rational points on elliptic curves", Phillips Lectures, Haverford College, 1961.

[W1] H. Wiman, *Uber rationale Punkte auf Kurven dritter Ordnung von geschlecchte eins*, Acta Math., **80** (1948), 223–257.

Departamento de Matemáticas
Universidad del Pais Vasco
Aptdo. 644
48080 Bilbao
Spain
E-mail address: J. Aguirre, mtpagesj@lg.ehu.es
E-mail address: F. Castañeda, mtpcabrf@lg.ehu.es
E-mail address: J.C. Peral, mtppealj@lg.ehu.es

Recibido: 22 de Marzo de 1999
Revisado: 19 de Julio de 1999