Elliptic Curves of High Rank with Nontrivial Torsion Group over $\mathbb{Q}$

Leopoldo Kulesz and Colin Stahlke

CONTENTS

We construct elliptic curves over $\mathbb{Q}$ of high Mordell–Weil rank, with a nontrivial torsion subgroup. We improve the rank records for the cases $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$.

INTRODUCTION

In order to find elliptic curves over $\mathbb{Q}$ with large rank, J.-F. Mestre [1991] constructed an infinite family of elliptic curves with rank at least 12. Then K. Nagao [1994] and S. Kihara [1997b] found infinite subfamilies of rank 13 and 14, respectively. By specialization, elliptic curves of rank at least 21 [Nagao and Kouya 1994], 22 [Fermigier 1997], and 23 [Martin and McMillen 1997] have also been found.

There have been quite a few efforts to construct families of curves with large rank having a nontrivial prescribed torsion group [Fermigier 1996; Nagao 1997; Kihara 1997c; 1997a; Kulesz 1998; 1999]. For example, S. Fermigier constructed a family of elliptic curves with rank at least 8 and a nontrivial point of order 2 and specialized it to a curve of rank 14.

Here we improve the rank records for curves with torsion group $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1. A BASIC CONSTRUCTION

While constructing curves with many rational points one often wants to find integers A and B such that $Ax + B$ is a square for many fixed rational numbers x. It turns out that one can fix four different values for x and still find A and B. We denote these four different rational numbers by x_1, x_2, x_3 and x_4.

Mestre uses the following method for finding such numbers A and B. Let $P \in \mathbb{Q}[x]$ be the polynomial $P(x) = \prod_{i=1}^{i=4}(x-x_i) = x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0$. We

can write it uniquely as $P = Q^2 - R$, with Q and R in $\mathbb{Q}[x]$ such that $Q(x) = x^2 + d_1 x + d_0$ and $R(x) = Ax + B$, for $d_1, d_0, A, B, \in \mathbb{Q}$. In fact we obtain this equality by setting $d_1 = c_3/2$, $d_0 = \frac{1}{2}(c_2 - d_1^2)$, $A = 2 d_1 d_0 - c_1$, and $B = d_0^2 - c_0$. Now $Ax + B$ is a square—namely $Ax + B = Q(x)^2$—for $x = x_1$, $x = x_2$, $x = x_3$ and $x = x_4$. Multiplying A and B by a suitable square makes them integers.

One can modify this method slightly. The polynomial P can be written in two ways as $P(x) = Q^2(x) - x^2 R(x)$, with Q and R in $\mathbb{Q}[x]$ such that $Q(x) = x^2 + d_1 x + d_0$ and $R(x) = Ax + B$, for $d_1, d_0, A, B \in \mathbb{Q}$. We obtain this by setting $d_0 = \pm\sqrt{c_0}$, $d_1 = c_1/(2d_0)$, $B = d_1^2 + 2d_0 - c_2$, and $A = 2d_1 - c_3$. This gives other solutions for A and B if $c_0 = x_1 x_2 x_3 x_4$ is a square.

Analoguously, P can be written in two ways as

$$P(X) = Q^2(X) - X R(X),$$

which still gives other solutions for A and B if the four numbers x_1, x_2, x_3 and x_4 are squares.

Finally, Thorsten Kleinjung has remarked that one can parametrize by $t \in \mathbb{Q}$ all possible values A and B (up to a square factor) such that $Ax + B$ is a square for $x = x_1$, $x = x_2$ and $x = x_3$ as follows:

$$A = 4(1-t)t\big(t(x_1 - x_2) + x_2 - x_3\big)$$
$$B = \big((t-1)^2(x_1 - x_2) + x_3 - x_1\big)^2 - Ax_1$$

In order to make $Ax_4 + B$ a square, one has to choose t suitably, i.e. one needs to find the rational points (t, y) of the elliptic curve given by $y^2 = Ax_4 + B$. Therefore each method from above corresponds to a point on this elliptic curve. For example Mestre's method corresponds to a point with any of these t-coordinates:

$$t = \frac{x_1 - x_2 + x_3 - x_4}{2(x_1 - x_2)},$$

$$t = \frac{2(x_2 - x_3)}{-x_1 + x_2 - x_3 + x_4},$$

$$t = \frac{-x_1 - x_2 + x_3 + x_4}{x_1 - x_2 - x_3 + x_4},$$

$$t = \frac{x_1 x_2 - x_2^2 - x_1 x_3 + x_3^2 + x_2 x_4 - x_3 x_4}{(x_1 - x_2)(x_1 + x_2 - x_3 - x_4)}.$$

Pairwise differences of these eight points are torsion points.

2. HEURISTICS

We want to search the families of elliptic curves with fixed torsion group for curves with high Mordell–Weil rank. It is difficult to find rational points on a curve if the equation of the curve has large coefficients. Furthermore it is rather time consuming to check these points for independence in the Mordell–Weil group. Here we use the following heuristics: A curve with large rank should have a large number of points over finite fields. Similar heuristics have been used by many people for finding curves with large rank (see introduction).

Let $E/\mathbb{Q}$ be an elliptic curve and

$$L(E, s) := \prod_{p \text{ prime}} Q_p(p^{-s})^{-1}$$

its L-series. Let

$$\Lambda_p(s) := 1 - a_p p^{-s} + p p^{-2s}$$

where $a_p = 1 + p - N(p)$ if $N(p)$ is the number of points of $E(\mathbb{F}_p)$. For good prime numbers p we have $Q_p(p^{-s}) = \Lambda_p(s)$. Now set

$$L_n(E, s) := \prod_{\substack{\text{first } n \\ \text{primes } p}} \Lambda_p(s)^{-1}$$

and

$$M_n := -\log L_n(E, 1) = \sum_{\substack{\text{first } n \\ \text{primes } p}} \Lambda_p(1) = \sum_{\substack{\text{first } n \\ \text{primes } p}} \frac{N(p)}{p}.$$

For $\operatorname{Re} s > 1$ and large n the number $L_n(E, s)$ is an approximation for $L(E, s)$ up to a factor (since we dont bother to find out the correct factors for the bad primes). Since the rank of E is conjecturally equal to the order of vanishing of $L(E, s)$ at $s = 1$, a high rank heuristically should imply that $L_n(E, 1)$ is small, which means that M_n is large. Since M_n can be calculated very fast by a computer, we will search the families of elliptic curves for curves with large M_{50} or large M_{500} and then search for independent points on these fewer curves.

3. RESULTS

In order to simplify the presentation of our results, we define

$$C(G, \mathbb{K}) = \max_E \operatorname{rank} E(\mathbb{K}),$$

with E running over all elliptic curves over $\mathbb{K}$ with a torsion subgroup over $\mathbb{K}$ isomorphic to G. If we call an equation an "elliptic curve", we are talking about the elliptic curve onto which the points of the curve map in a canonical way. For example, we call $y^2 = x^2 + 3/x^2$ an elliptic curve with a rational point with $x = 1$ and mean by that the elliptic curve described by $y^2 = 4x^3 - 3x$ with a rational point with $x = \frac{3}{2}$. The map here is not obvious, but it comes from a standard construction [Mordell 1969]. It is one-to-one except at one point.

The constructions are all based on [Kulesz 1998], sometimes modified in order to get many equations with small coefficients. All such constructions are basically variants of constructions of [Mestre 1991].

We find elliptic curves with large rank by specialization of parameterized families of elliptic curves with large rank and a certain fixed torsion group. In order to find the rank of our elliptic curves, we identify independent rational points on the curves. Sometimes we manage to identify this lower bound for the rank as being the exact rank by using a computer program by Michael Stoll [2001] which calculates an upper bound for the rank using Selmer group computations.

Proposition 1. $C(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) \geq 14$.

This result was proved by Fermigier [1996]. We re-prove it here by another construction.

Choose a natural number n which is the product of exactly three primes which are congruent to 1 mod 4. We get the four pairs of numbers (a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4), which satisfy $a_i^2 + b_i^2 = n$. Then we get the four numbers $x_i := -a_i^2 b_i^2$ and an elliptic curve associated to these numbers x_i as in section 1. Each point on this elliptic curve corresponds to a pair of numbers (A, B) such that $Ax_i + B$ is a square for $i = 1, 2, 3, 4$. Now we consider the elliptic curve $y^2 = A(x^4 - nx^2) + B$. We have 8 point pairs on this curve described by the 8 x-coordinates $x = a_i$ and $x = b_i$. Generically the curve has torsion group $\mathbb{Z}/2\mathbb{Z}$ and rank 8.

For $n = 6210037 = 73 \cdot 97 \cdot 877$ we get the pairs $(359, 2466)$, $(649, 2406)$, $(1351, 2094)$, and $(1386, 2071)$. Therefore

$$x_1 = -783745466436, \quad x_2 = -2438263512036,$$
$$x_3 = -8003207052036, \quad x_4 = -8239230604836.$$

As in Section 1 we have to search for points on the elliptic curve

$$\begin{aligned} y^2 =\ & 2737429963216043679360000t^4 \\ &- 4934093880074165404416000t^3 \\ &+ 2407498340897212736256000 00t^2 \\ &- 2152983542347619977881600 00t \\ &+ 52120625585954066127360000. \end{aligned}$$

There is a point with $t = \frac{5034}{2291}$ which corresponds to

$$A = -28547814,$$
$$B = -21926930204749905279.$$

Now we consider the elliptic curve

$$y^2 = A(x^4 - 6210037x^2) + B,$$

or

$$y^2 = -28547814x^4 + 177282981209118x^2$$
$$- 21926930204749905279.$$

It has torsion group $\mathbb{Z}/2\mathbb{Z}$ and rank at least 14. Generators are given by the x-coordinates 359, -359, 649, 1351, 1386, 1694, 2071, 2094, 2406, 2466, $\frac{12331}{5}$, $\frac{24355}{19}$, $\frac{43190}{67}$, $\frac{55578}{43}$ and $\frac{62021}{97}$.

Proposition 2. $C(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) \geq 10$.

Let $F(x) = (x^2 + b)/x$ with a parameter b. We want to construct an elliptic curve $y^2 = AF(x)^2 + B$, where A is a square. It is easy to check that such curves have a cubic model of the form

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

with $\alpha, \beta, \gamma \in \mathbb{K}$, which is the general model for elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Set

$$\begin{aligned} A =\ & \tfrac{1}{4}(-x_1 + x_2 - x_3 + x_4)(-x_1 - x_2 + x_3 + x_4) \\ &\times (x_1 + x_2 + x_3 + x_4)(x_1 - x_2 - x_3 + x_4), \\ B =\ & (x_4 x_3 - x_1 x_2)(x_4 x_2 - x_3 x_1)(x_3 x_2 - x_4 x_1). \end{aligned}$$

Then $y^2 = Ax^2 + B$ has rational solutions for $x = x_1$, x_2, x_3, x_4. Now choose rational numbers z_1, z_2, z_3, z_4. If we replace in A the x_i by $F(z_i)$, then $y^2 = A$ is an elliptic curve in y and the parameter b. Let b be a fixed rational solution of this equation. Then

$$y^2 = AF(x)^2 + B,$$

or equivalently $y^2 = A(x^2 + b)^2 + Bx^2$, gives an elliptic curve of generic rank 4. For $z_1 = \frac{2}{7}$, $z_2 = \frac{10}{11}$,

$z_3 = \frac{7}{12}$ and $z_4 = \frac{5}{14}$, we get the equation of the elliptic curve $y^2 = A$:

$$y^2 = \frac{1}{42688800^2}(16305169766307846^4$$
$$+ 43298624875968006^3 - 15962486558436006^2$$
$$- 2342999181600006 + 83485429515625).$$

It has a rational point with $b = -\frac{4295}{264}$. Then the equation $y^2 = AF(x)^2 + B$ is equivalent to

$$y^2 = 1070976614400\,x^4 + 9071790616574169\,x^2$$
$$+283464364960000,$$

which corresponds to an elliptic curve over $\mathbb{Q}$ of rank exactly 10. Ten independent points are given by the x-coordinates $\frac{2}{7}, \frac{21}{8}, \frac{10}{11}, \frac{5}{14}, \frac{4}{21}, \frac{842}{39}, \frac{860}{81}, \frac{147}{89}, \frac{710}{123}, \frac{325}{168}$.

Proposition 3. $C(\mathbb{Z}/3\mathbb{Z}, \mathbb{Q}) \geq 8$.

We know from [Knapp 1992] that an elliptic curve defined over a field $\mathbb{K}$ has a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$, if and only if it has a cubic model of the form $y^2 + a_1 xy + a_3 y = x^3$.

Consider the rational fraction $F(x) = x^3/(x+1)^2$. We would like to construct an elliptic curve $y^2 = AF(x)^2 + B$, where B is a square, say $B = \tilde{B}^2$. This curve has a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$:

$$y^2 + \frac{2\tilde{B}}{A}xy + \frac{2\tilde{B}}{A^2}y = x^3 \to y^2 = Ax^3 + \tilde{B}^2(x+1)^2,$$
$$(x, y) \qquad \mapsto (Ax, A^2y + A\tilde{B}x + \tilde{B}).$$

Set $G(x) = -\frac{1}{4}(x^2+3)^3/(x^2-1)^2$, and let z_1, z_2, z_3 be rational numbers. Set $x_i = G(z_i)$ for $i = 1, 2, 3$ and $x_4 = 0$. Using Mestre's method as in Section 1, we find A and B such that $Ax_i + B$ is a square. Since $x_4 = 0$, B is a square. The special form of the other x_i guarantees that the elliptic curve $y^2 = AF(x)^2 + B$ has many rational points, since the numerator of $\prod_{i=1}^4 (F(x) - x_i)$ splits into linear factors over $\mathbb{Q}$. Now set $z_1 = \frac{4}{5}$, $z_2 = \frac{1}{17}$, $z_3 = \frac{13}{17}$ and $t = \frac{5962}{7605}$. This value of t corresponds to Mestre's method (see Section 1). The equation $y^2 = AF(x)^2 + B$ is equivalent to

$$y^2 = -713805507245376000\,x^3 + 1377737557^2\,(x+1)^2,$$

which is an elliptic curve with rank at least 8. Eight independent points are given by the x-coordinates $-91, -\frac{259}{4}, -\frac{217}{64}, -\frac{217}{81}, -\frac{91}{81}, -\frac{259}{225}, \frac{4123}{1275}$ and $-\frac{4123}{1989}$.

Proposition 4. $C(\mathbb{Z}/4\mathbb{Z}, \mathbb{Q}) \geq 9$.

We know from [Knapp 1992] that an elliptic curve defined over a field $\mathbb{K}$ has a torsion subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if and only if it has a cubic model of the form $y^2 + xy - by = x^3 - bx^2$.

Consider the rational fraction $F(x) = x^2/(x-1)$. We would like to construct an elliptic curve $y^2 = AF(x)^2 + B$, where B is a square, say $B = \tilde{B}^2$. This curve has a torsion subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$:

$$y^2 = Ax^2(x-1) + \tilde{B}^2(x-1)^2$$
$$\to y^2 + xy - \frac{A}{4\tilde{B}^2}y = x^3 - \frac{A}{4\tilde{B}^2}x^2,$$
$$(x, y) \qquad \mapsto \left(\frac{A}{4\tilde{B}^2}x, \frac{A}{4\tilde{B}^2}\left(\frac{y}{2\tilde{B}} + \frac{1-x}{2}\right)\right).$$

Let z_1, z_2, z_3 be rational numbers. Set $x_i := F(z_i)$ for $i = 1, 2, 3$ and $x_4 = 0$. As in Section 1 we find A and B such that $Ax_i + B$ is a square. Since $x_4 = 0$, B is a square. Now set $z_1 = \frac{6}{7}$, $z_2 = \frac{25}{7}$, $z_3 = \frac{11}{19}$ and $t = \frac{47}{713}$. This value of t corresponds to Mestre's method (Section 1). The equation $y^2 = AF(x)^2 + B$ is equivalent to

$$y^2 = 267942346717248\,x^2(x-1) + 75133085^2(x-1)^2,$$

which is an elliptic curve with rank at least 9. Nine independent points are given by the x-coordinates $-6, \frac{25}{7}, -\frac{11}{8}, \frac{13631}{84}, -\frac{1255}{161}, \frac{42835}{427}, -\frac{12011}{575}, \frac{8137}{713}$ and $-\frac{1965}{1457}$.

Proposition 5. $C(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}) \geq 5$.

The general elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/5\mathbb{Z}$ has equation

$$y^2 + (1-c)xy - by = x^3 - cx^2,$$

with $c \in \mathbb{Q}$. A change of coordinates leads to

$$E_c: y^2 = x^3 + \frac{1}{4}(1-6c+c^2)x^2 + \frac{1}{2}(-1+c)cx + \frac{1}{4}c^2.$$

Generically this has rank 2 if we set

$$c = \frac{-(3t^2+6t+4)(t^2+6t+12)}{(t-2)^2(t+2)^2}.$$

For $t = \frac{10}{23}$ we get

$$y^2 = x^3 + \frac{6344230390033}{258096513024}x^2 + \frac{3920922576337}{129048256512}x + \frac{3449165839249}{258096513024},$$

an elliptic curve over $\mathbb{Q}$ of rank exactly 5. Five independent points are given by the x-coordinates $-1, -\frac{325}{196}, -\frac{1387}{256}, -\frac{949}{504}$ and $-\frac{6935}{3456}$.

Proposition 6. $C(\mathbb{Z}/6\mathbb{Z}, \mathbb{Q}) \geq 3$.

The general elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/6\mathbb{Z}$ has equation

$$y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2,$$

with $c \in \mathbb{Q}$. A change of coordinates leads to E_c with equation

$$y^2 = x^3 + \tfrac{1}{4}(1-6c-3c^2)x^2 + \tfrac{1}{2}(-1+c)c(1+c)x + \tfrac{1}{4}c^2(1+c)^2.$$

Generically it has rank 2 if we set

$$c = \frac{4(t-1)(-2t+1+2t^2)}{(5-8t+4t^4)}.$$

For $t = \frac{5}{6}$ we get

$$y^2 = x^3 + \tfrac{13777}{28900}x^2 - \tfrac{1334658}{614125}x + \tfrac{30669444}{52200625},$$

which is an elliptic curve over $\mathbb{Q}$ of rank at least 3. Three independent points are given by the x-coordinates $-\frac{26}{17}$, $\frac{156}{85}$ and $\frac{78}{289}$.

Proposition 7. $C(\mathbb{Z}/7\mathbb{Z}, \mathbb{Q}) \geq 3$.

The general elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/7\mathbb{Z}$ has equation

$$E_d : \ y^2 + (1-c)xy - by = x^3 - bx^2,$$

with $b = d^3 - d^2$, $c = d^2 - d$, and $d \in \mathbb{Q}$. A change of coordinates leads to E_d with equation

$$y^2 = x^3 + \tfrac{1}{4}(1-4b-2c+c^2)x^2 + \tfrac{1}{2}b(-1+c)x + \tfrac{1}{4}b^2.$$

Generically it has rank 1 if we set

$$d = \frac{2(3-t)}{3+t^2}.$$

For $t = -\frac{1}{5}$ we get

$$y^2 = x^3 - \tfrac{2324159}{521284}x^2 + \tfrac{8047200}{2476099}x + \tfrac{282240000}{47045881},$$

an elliptic curve over $\mathbb{Q}$ of rank exactly 3. Three independent points are given by the x-coordinates $\frac{30}{19}$, $\frac{240}{19}$ and $\frac{1344}{19}$.

Proposition 8. $C(\mathbb{Z}/8\mathbb{Z}, \mathbb{Q}) \geq 3$.

The general elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/8\mathbb{Z}$ has equation

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

with $b = (2d-1)(d-1)$ and $c = (2d-1)(d-1)/d$, for $d \in \mathbb{Q}$. A change of coordinates leads to E_d with equation

$$y^2 = x^3 + \tfrac{1}{4}(1-4b-2c+c^2)x^2 + \tfrac{1}{2}b(c-1)x + \tfrac{1}{4}b^2.$$

Generically it has rank 1 if we set

$$d = \frac{2 - 2t + t^2}{2 + t^2}.$$

For $t = \frac{49}{66}$ we get

$$y^2 = x^3 + \tfrac{28536641}{395612100}x^2 - \tfrac{8016052}{232802505}x + \tfrac{1024144}{547981281},$$

an elliptic curve over $\mathbb{Q}$ of rank exactly 3. Three independent points are given by the x-coordinates $-\frac{8}{51}$, $\frac{143}{1620}$ and $-\frac{440}{1989}$.

REFERENCES

[Fermigier 1996] S. Fermigier, "Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possédant des points d'ordre 2", *C. R. Acad. Sci. Paris Sér. I Math.* **322**:10 (1996), 949–952.

[Fermigier 1997] S. Fermigier, "Une courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 22", *Acta Arith.* **82**:4 (1997), 359–363.

[Kihara 1997a] S. Kihara, "Construction of high-rank elliptic curves with a non-trivial rational point of order 2", *Proc. Japan Acad. Ser. A Math. Sci.* **73**:9 (1997), 165.

[Kihara 1997b] S. Kihara, "On an infinite family of elliptic curves with rank ≥ 14 over $\mathbb{Q}$", *Proc. Japan Acad. Ser. A Math. Sci.* **73**:2 (1997), 32.

[Kihara 1997c] S. Kihara, "On the rank of elliptic curves with three rational points of order 2, II", *Proc. Japan Acad. Ser. A Math. Sci.* **73**:8 (1997), 151.

[Knapp 1992] A. Knapp, *Elliptic curves*, Math. Notes **40**, Princeton University Press, Princeton, NJ, 1992.

[Kulesz 1998] L. Kulesz, *Arithmétique des courbes algébriques de genre au moins deux*, Ph.D. thesis, Université de Paris VII, 1998.

[Kulesz 1999] L. Kulesz, "Courbes elliptiques de rang ≥ 5 sur $\mathbb{Q}(t)$ avec un groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$", *C. R. Acad. Sci. Paris Sér. I Math.* **329**:6 (1999), 503–506.

[Martin and McMillen 1997] R. Martin and W. McMillen, informal report, 1997. See http://www.math.niu.edu/~rusin/known-math/98/hirank.

[Mestre 1991] J.-F. Mestre, "Courbes elliptiques de rang ≥ 12 sur $\mathbb{Q}(t)$", *C. R. Acad. Sci. Paris Sér. I Math.* **313**:4 (1991), 171–174.

[Mordell 1969] L. J. Mordell, *Diophantine equations*, Pure and Applied Math. **30**, Academic Press, London, 1969. Reprinted by Chelsea, New York, 1970.

[Nagao 1994] K. Nagao, "An example of elliptic curve over $\mathbb{Q}(T)$ with rank ≥ 13", *Proc. Japan Acad. Ser. A Math. Sci.* **70**:5 (1994), 152–153.

[Nagao 1997] K. Nagao, "Construction of high-rank elliptic curves with a nontrivial torsion point", *Math. Comp.* **66**:217 (1997), 411–415.

[Nagao and Kouya 1994] K. Nagao and T. Kouya, "An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 21", *Proc. Japan Acad. Ser. A Math. Sci.* **70**:4 (1994), 104–105.

[Stoll 2001] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98**:3 (2001), 245–277.

Leopoldo Kulesz, UFR de mathématiques, Université Paris 7, 2 place Jussieu, F-75251 Paris, France (kulesz@math.jussieu.fr)

Colin Stahlke, Mathematisches Institut der Universität Bonn, Beringstraße 1, D-53115 Bonn, Germany (colin@math.uni-bonn.de)