

# ON THE RANK OF ELLIPTIC CURVES WITH A RATIONAL POINT OF ORDER 4

GARIKAI CAMPBELL

ABSTRACT. We find an infinite family of elliptic curves defined over  $\mathbb{Q}$  with rational torsion subgroup equal to  $\mathbb{Z}/4\mathbb{Z}$  and rank at least 3. This ties the rank-record set by Leopoldo Kulesz for an infinite family of elliptic curves defined over  $\mathbb{Q}$  with rational torsion subgroup  $\mathbb{Z}/4\mathbb{Z}$ . The family we describe here is derived from a family of curves found by Odile Lecacheux.

## 1. INTRODUCTION.

One of the fundamental open questions regarding the study of elliptic curves is whether or not there exists a bound on the ranks of the Mordell-Weil groups of elliptic curves defined over  $\mathbb{Q}$ . The folklore conjecture is that there is no such bound—that the ranks of the groups of rational points of elliptic curves can be as large as one would like. In fact, many suspect that an even stronger statement may be true. Suppose we let

$$\begin{aligned} B(\mathbb{T}) &= \sup\{\text{rank } E(\mathbb{Q}) \mid E \text{ is an elliptic curve with rational torsion } \mathbb{T}\} \text{ and} \\ C(\mathbb{T}) &= \limsup\{\text{rank } E(\mathbb{Q}) \mid E \text{ is an elliptic curve with rational torsion } \mathbb{T}\}. \end{aligned}$$

A long-standing conjecture is the following:

**Conjecture 1.1.**  $B(\mathbb{T})$  and  $C(\mathbb{T})$  are unbounded for all possible  $\mathbb{T}$ .

Recall that a theorem of Mazur tells us there are precisely 15 possible rational torsion subgroups  $\mathbb{T}$ :

$$\begin{aligned} \mathbb{T} &= \mathbb{Z}/n\mathbb{Z}, \text{ where } n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\} \text{ or} \\ \mathbb{T} &= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \text{ where } n \in \{2, 4, 6, 8\}. \end{aligned}$$

In this note, we give an explicit example of an elliptic curve defined over  $\mathbb{Q}(m)$  with a  $\mathbb{Q}(m)$ -rational point of order 4 and three linearly independent  $\mathbb{Q}(m)$ -rational points, thereby proving:

**Theorem 1.2.**  $C(\mathbb{Z}/4\mathbb{Z}) \geq 3$ .

We note that Leopoldo Kulesz [5], using a technique first developed by Jean-Francois Mestre [8], was first [4] to prove this theorem. The family of elliptic curves produced here is related to a family of elliptic curves found by Odile Lecacheux [7] and it is worth noting that the techniques used by Lecacheux are quite different from those discovered by Mestre.

---

2000 *Mathematics Subject Classification.* 14G05, 14H52, 11G05.

*Key words and phrases.* elliptic curves, rank, torsion.

The author was supported by the Woodrow Wilson Career Enhancement Fellowship.

## 2. A FAMILY OF ELLIPTIC CURVES OF RANK AT LEAST 2.

In [7], Lecacheux proves that  $C(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \geq 3$  by finding a particular elliptic curve defined over  $\mathbb{Q}(t)$ . This curve is derived (in a nontrivial) way from the curve:

$$\mathcal{L}_{u,t} : Y^2 - (ut + 1)(t - u)XY = X(X + u^2t^2)^2$$

defined over  $\mathbb{Q}(u, t)$ . Here, rather than consider  $\mathcal{L}_{u,t}$  as a single elliptic curve defined over  $\mathbb{Q}(u, t)$ , we will consider it as a family of elliptic curves defined over  $\mathbb{Q}(t)$  and parameterized by  $u \in \mathbb{Q}(t)$ .

For each  $u \in \mathbb{Q}(t)$ ,  $\mathcal{L}_{u,t}$  contains the points  $A_u = (-u^2t^2, 0)$ ,  $2A_u = (0, 0)$  and  $B_u = (u^3t^3, u^3t^4(ut + 1))$ . It is easy to compute that  $A_u$  is a point of order 4 (and hence  $(0, 0)$  is a point of order 2) and that  $B_u$  is a point of infinite order. Moreover, we compute that  $\mathcal{L}_{u,t}$  has a  $\mathbb{Q}(t)$ -rational point of order 2 other than  $(0, 0)$  only if  $u$  is a  $\mathbb{Q}(t)$ -rational point on the curve:

$$\mathcal{K}_t : v^2 = u^4t^2 - u^32t(t^2 - 1) + u^2(t^4 + 12t^2 + 1) + u2t(t^2 - 1) + t^2.$$

We note that the discriminant of  $\mathcal{L}_{u,t}$  vanishes for  $u \in \mathbb{Q}(t)$  if and only if  $u \in \{0, t, -1/t\}$  and that these values of  $u$  produce points on  $\mathcal{K}_t$ . Therefore,  $\mathcal{L}_{u,t}$  has a  $\mathbb{Q}(t)$ -rational point of order 2 other than  $(0, 0)$  if only if  $u$  is a  $\mathbb{Q}(t)$ -rational point on  $\mathcal{K}_t$  not equal to  $(t, \pm 4t^2)$ ,  $(-1/t, \pm 4)$  or  $(0, \pm t)$ . Furthermore, regarding  $\mathcal{K}_t$  as the the intersection of two smooth quadrics in  $\mathbb{P}^3$  (as in II.2 of [9]), we have:

**Proposition 2.1.**  *$\mathcal{K}_t$  is an elliptic curve defined over  $\mathbb{Q}(t)$  and is isomorphic to*

$$\mathcal{E}_t : y^2 = x^3 + (t^4 + 18t^2 + 1)x^2 + 64t^4x.$$

*Proof.* Multiplying the equation for  $\mathcal{K}_t$  by  $t^2$  and making the substitution  $V = vt, U = u/t$ , we see that  $\mathcal{K}_t$  is isomorphic to

$$\mathcal{K}'_t : V^2 = U^4 - 2U^3(t^2 - 1) + U^2(t^4 + 12t^2 + 1) + 2Ut^2(t^2 - 1) + t^4.$$

The map  $(U, V) \mapsto (x, y)$ , where

$$\begin{aligned} x &= -2(V - U^2 + (t^2 - 1)U + t^2) \text{ and} \\ y &= -2(V(t^2 - 1) - 2UV + 2U^3 - 3U^2(t^2 - 1) + U(t^4 + 12t^2 + 1) + t^2(t^2 - 1)), \end{aligned}$$

defines an isomorphism, mapping points on  $\mathcal{K}'_t$  to points on  $\mathcal{E}_t$ .  $\square$

The points on  $\mathcal{K}_t$ , with  $u$ -coordinates  $0, -1/t$  and  $t$ , described above and the isomorphism given in the proof above lead us to find additional points on  $\mathcal{K}_t$ . In particular, we find the  $\mathbb{Q}(t)$ -rational points with  $u$ -coordinates  $1/t, -t$  and  $3t/(t^2 - 1)$ . Mapping these points to  $\mathcal{E}_t$ , we get the following two propositions:

**Proposition 2.2.** *The point  $S_t = (-8t^2, 8t^2(t^2 + 1))$  is a point of order 4 on  $\mathcal{E}_t$ .*

**Proposition 2.3.** *The two points  $P_t = (-8t^3, 8t^3(t^2 - 4t + 1))$  and  $Q_t = (8t^3, -8t^3(t^2 + 4t + 1))$  are linearly independent points on  $\mathcal{E}_t$ .*

Moreover, if we let  $E_t$  denote the curve  $\mathcal{E}_t$  specialized to a particular value of  $t \in \mathbb{Q}$  and let  $\mathbb{Q}^*$  denote the nonzero rationals, then we have:

**Proposition 2.4.** *For all  $t \in \mathbb{Q}^*$ ,  $E_t$  is an elliptic curve defined over  $\mathbb{Q}$  with rational torsion subgroup equal to  $\mathbb{Z}/4n\mathbb{Z}$ ,  $n \in \{1, 2, 3\}$ .*

*Proof.* The discriminant of  $\mathcal{E}_t$  is  $2^{16}t^8(t^2 + 1)^2(t^4 + 34t^2 + 1)$  and hence  $E_t$  is non-singular for  $t \in \mathbb{Q}$  if and only if  $t \neq 0$ . The discriminant of  $x^2 + (t^4 + 18t^2 + 1)x + 64t^4$  is  $(t^2 + 1)^2(t^4 + 34t^2 + 1)$ . Therefore,  $E_t$  has a rational point of order 2 other than  $(0, 0)$  if and only if  $t^4 + 34t^2 + 1$  is a square. However, the curve  $s^2 = t^4 + 34t^2 + 1$  is an elliptic curve of rank 0 (whose only rational points are the points at infinity and the points with  $t = 0$ ). Therefore, by Mazur's theorem, we have the result.  $\square$

*Remark 2.5.* Note that by examining the 3-division polynomial and the requirement that  $(-8t^2, 8t^2(t^2 + 1))$  be  $2P$  for some  $P \in E_t(\mathbb{Q})$ , we see that the cases  $\mathbb{Z}/8\mathbb{Z}$  and  $\mathbb{Z}/12\mathbb{Z}$  can happen at most finitely often (if at all). Furthermore, the specialization map is injective for almost all  $t \in \mathbb{Q}^*$ . These two statements immediately imply:

**Corollary 2.6.** *For all but finitely many  $t \in \mathbb{Q}^*$ , the curve  $E_t$  has rational torsion subgroup  $\mathbb{Z}/4\mathbb{Z}$  and rank at least 2.*

### 3. A SUB-FAMILY OF RANK AT LEAST 3.

We also find that if we set  $U = t^2 + 2$  in the equation defining  $\mathcal{K}'_t$ , then we get  $4(t^2 + 1)^2(4t^2 + 9)$ . We can parameterize the rational solutions to  $s^2 = 4t^2 + 9$  as follows:

$$t = \frac{6m}{m^2 - 4} \quad \text{and} \quad s = 3 \left( \frac{m^2 + 4}{m^2 - 4} \right),$$

with  $m \in \mathbb{Q}$ . Therefore, if we define  $\mathcal{K}'_{t(m)}$  to be the curve defined over  $\mathbb{Q}(m)$  gotten by specializing  $\mathcal{K}'_t$  to the value of  $t$  above, then in addition to the  $\mathbb{Q}(t)$ -rational points found earlier, we have the new  $\mathbb{Q}(m)$ -rational point  $(t^2 + 2, 2(t^2 + 1)s)$ . If we similarly define  $\mathcal{E}_{t(m)}$  to be the specialization of  $\mathcal{E}_t$  to this value of  $t$ , then the point  $(t^2 + 2, 2(t^2 + 1)s)$  maps to the point

$$R_{t(m)} = (-4(s + 1)t^2 - 4(s + 3), 4(s - 9)t^4 + 24(s - 4)t^2 + 4(5s - 12))$$

on  $\mathcal{E}_{t(m)}$ . To be consistent, we define  $P_{t(m)}$  and  $Q_{t(m)}$  to be the points  $P_t$  and  $Q_t$  (of proposition 2.3) specialized to  $t = 6m/(m^2 - 4)$  and observe that:

**Theorem 3.1.**  *$\mathcal{E}_{t(m)}$  is an elliptic curve defined over  $\mathbb{Q}(m)$  and the three  $\mathbb{Q}(m)$ -rational points  $P_{t(m)}$ ,  $Q_{t(m)}$  and  $R_{t(m)}$  are linearly independent.*

Therefore, if we let  $E_{t(m)}$  denote the curve  $\mathcal{E}_{t(m)}$  specialized to some particular value of  $m \in \mathbb{Q}$  as we did above, then we have:

**Corollary 3.2.** *For all  $m \in \mathbb{Q}^*$ ,  $m \neq \pm 2$ ,  $E_{t(m)}$  is an elliptic curve defined over  $\mathbb{Q}$  and for all but finitely many rational  $m$ ,  $E_{t(m)}$  has rational torsion subgroup exactly  $\mathbb{Z}/4\mathbb{Z}$  and  $E_{t(m)}(\mathbb{Q})$  has rank at least 3. Subsequently,  $C(\mathbb{Z}/4\mathbb{Z}) \geq 3$ .*

*Remark 3.3.* We note that  $E_{t(m)}$  is isomorphic (over  $\mathbb{Q}$ ) to  $E_{t(n)}$  if and only if  $n = \pm m$ ,  $n = \pm 4/m$  or  $(m, n)$  is a rational point on a curve of genus greater than 1 (and hence is one of only finitely many possibilities). Therefore, we may parameterize all the curves in this family by  $m \in \mathbb{Q}$ ,  $0 < m < 2$ . A brief search of curves with  $m$  in this range and denominator less than 100 found several examples of elliptic curves with rank 6 and one,  $m = 85/66$ , with rank 7. This falls short of the current record of 9 set by Kulesz and Stahlke [6], but we suspect that a more thorough search might at least tie this record.

This gives us only the second known example of an infinite family of elliptic curves defined over  $\mathbb{Q}$  with rational torsion subgroup equal to  $\mathbb{Z}/4\mathbb{Z}$  and rank at least 3.

#### ACKNOWLEDGEMENTS

Calculations were performed using a variety of packages: *GP/Pari* [1], *Mathematica* [10] and *mwrank* [3].

We would like to thank Odile Lecacheux for forwarding a preprint of her paper [7] and John Cremona for all his support with *mwrank*.

#### REFERENCES

1. C. Batut and K. Belabas and D. Benardi and H. Cohen and M. Olivier. *User's Guide to PARI-GP*. <ftp://megrez.math.u-bordeaux.fr/pub/pari>, 1998. (See also <http://pari.home.ml.org>.)
2. Garikai Campbell. *Finding Elliptic Curves and Families of Elliptic Curves over  $\mathbb{Q}$  of Large Rank*, Ph.D. Thesis, Rutgers University, 1999.
3. John Cremona. *mwrank*. <http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/>, 2002.
4. Andrej Dujella. *Infinite families of elliptic curves with high rank and prescribed torsion*. <http://www.math.hr/~duje/tors/generic.html>, 2002.
5. Leopoldo Kulesz. *Arithmetique des courbes algebriques de genre au moins deux*, These de doctorat, Universite Paris 7, 1998.
6. Leopoldo Kulesz and C. Stahlke. Elliptic curves of high rank with nontrivial torsion group over  $\mathbb{Q}$ . *Experiment. Math.* **10**: 475–480, 2001.
7. Odile Lecacheux. Rang de courbes elliptiques avec groupe de torsion non trivial. *J. Theor. Nombres Bordeaux*, to appear.
8. J.-F. Mestre. Courbes elliptiques de rang  $\geq 11$  sur  $\mathbb{Q}(t)$ . *C. R. Acad. Sci. Paris Ser. I.* **313**: 139–142, 1991.
9. Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
10. Wolfram Research, Inc. *Mathematica*. Version 4.2. Wolfram Research, Inc. Champaign, IL, 1999.

DEPARTMENT OF MATHEMATICS AND STATISTICS, SWARTHMORE COLLEGE, SWARTHMORE, PA 19081

*Current address:* Department of Mathematics and Statistics, Swarthmore College, Swarthmore, PA 19081

*E-mail address:* [kai@swarthmore.edu](mailto:kai@swarthmore.edu)