AN ELLIPTIC CURVE OVER $\mathbb{Q}(u)$ WITH TORSION $\mathbb{Z}/4\mathbb{Z}$ AND RANK 6

Andrej Dujella and Juan Carlos Peral

ABSTRACT. In this paper, we present the construction of an elliptic curve over $\mathbb{Q}(u)$ with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 6. Previously only rank 5 examples for such curves were known.

Dedicated to Marko Tadić on the occasion of his 70th birthday

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$. By the Mordell-Weil theorem, the group $E(\mathbb{Q})$ of rationals points on E is a finitely generated Abelian group. Hence, it has the form $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ is called the torsion group of E, and the non-negative integer r is called the rank of E.

In 1978, Mazur [16] proved that there are precisely 15 possible torsion groups for elliptic curves over $\mathbb{Q}$:

$$\mathbb{Z}/k\mathbb{Z}, \qquad \text{for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, \qquad \text{for } k = 2, 4, 6, 8.$$

On the other hand, it is not known which values of rank r are possible for elliptic curves over $\mathbb{Q}$. It has been conjectured that there exist elliptic curves of arbitrarily high rank, even that for each of the torsion groups in Mazur's theorem, there exist curves with that torsion group and arbitrarily large rank. However, there are also recent heuristic arguments that suggest the boundedness of the rank of elliptic curves. According to this heuristic, only a finite number of curves would have rank higher than 21 (see [17]). The current record is an example of an elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found

by Elkies in 2006 (see [6] and also [14] where it is shown that, assuming the generalized Riemann hypothesis, Elkies's curve has rank equal to 28).

The first step in finding elliptic curves with large rank is usually constructing a parametric family of elliptic curves, i.e. an elliptic curve over the field of rational function $\mathbb{Q}(u)$, with the considered property (e.g. with a given torsion group). Thus, it is of interest to construct elliptic curves over $\mathbb{Q}(u)$ with a given torsion group and relatively large generic rank.

In this paper, we will present the construction of an elliptic curve over $\mathbb{Q}(u)$ with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 6, which is the current record for the rank over $\mathbb{Q}(u)$ for this torsion group. Let us mention that the largest known rank for an elliptic curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}$ is 13 (see [7]). Information on current rank records for all 15 possible torsion groups can be found in [1].

2. General equation of curves with torsion group $\mathbb{Z}/4\mathbb{Z}$

The general model of an elliptic curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ is given by

$$Y^2 + aXY + abY = X^3 + bX^2,$$

where $ab(a^2 - 16b) \neq 0$ (see, e.g. [6]). A torsion point of order 4 in this model is $(0,0)$.

We will use the construction of Elkies [6] for curves with torsion group $\mathbb{Z}/4\mathbb{Z}$. Elkies noticed that this torsion and rank 4 can be obtained for some elliptic $K3$ surfaces. In this case, the maximum rank is obtained with the following types of reducible fibers for such a surface: four of type I_4, two of type I_2 and four of type I_1, so giving a contribution to the Néron-Severi group of $4(4-1) + 2(2-1)) = 14$, hence the rank over this surface is at most $20 - 2 - 14 = 4$ (since the Néron-Severi rank of a $K3$ surface is at most 20, see, e.g. [18]). So in this sense, the Elkies example is optimal.

3. Elkies model for rank 4

By the result of Inose [10], we know that the Néron-Severi rank can be 20 only if the corresponding discriminant is one of the thirteen discriminants of imaginary quadratic orders of class number 1. Elkies [6] has shown that the discriminant -163 surface does have an elliptic model that attains rank 4 with torsion group $\mathbb{Z}/4\mathbb{Z}$ for the following values of parameters a and b:

$$a = (8t - 1)(32t + 7),$$
$$b = 8(t + 1)(15t - 8)(31t - 7).$$

With a simple change of variables, the surface can be written as

$$Y^2 = X^3 + (a^2 - 8b)X^2 + 16b^2X.$$

Inserting the values of a and b given above, one gets the following elliptic $K3$ surface E

$$E: \ Y^2 = X^3 + (65536t^4 - 17472t^3 - 10176t^2 + 18672t - 3535)X^2$$
$$+ 1024(t+1)^2(15t-8)^2(31t-7)^2 X.$$

It has torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 4. A torsion point of order 4 in this model is

$$(32(t+1)(15t-8)(31t-7), 2^5(1+t)(-1+8t)(-8+15t)(-7+31t)(7+32t))$$

and the X-coordinates of four independent points of infinite order are

$$X_1 = -361(t+1)(31t-7),$$
$$X_2 = -4(t+1)(15t-8)(16t-7)^2,$$
$$X_3 = -16(t+1)(8t+7)^2(15t-8),$$
$$X_4 = 4(15t-8)(16t+1)^2(31t-7).$$

In [7], it is quoted that for

$$a = 4(9+80t),$$
$$b = 1/2(-2+t)(-81+2t)(-1+2t)(-1+18t).$$

the resulting $K3$ surface also has rank 4.

Previous to the Elkies construction in 2007, in 2004, Kihara [12, 13] and Lecacheux [15] found curves with rank 4 and 5 over $\mathbb{Q}(u)$. The coefficients in the Kihara and Lecacheux constructions are much larger than those in Elkies examples, and so they are less suited for finding particular good examples of high-rank curves. In fact, the family with rank 4 in the Elkies paper is $y^2 = x^3 + A(t)x^2 + B(t)x$, where $A(t)$ is a polynomial of degree 4 and $B(t)$ is a polynomial of degree 6, and the examples with rank 5 have polynomial coefficients of degree 8 and 16, while the corresponding coefficients in the Kihara family have degrees 52 and 102, respectively. In 2016, Khoshnam and Moody [11] gave an example of rank 5 over $\mathbb{Q}(u)$ with a simpler version of the Kihara method. In fact, the coefficients A and B in this curve are polynomials of degrees 19 and 38, respectively.

The object of this note is to construct an example of an elliptic curve over $\mathbb{Q}(u)$ with torsion $\mathbb{Z}/4\mathbb{Z}$ and rank 6. It will be obtained as a specialization of the Elkies surface.

4. A CURVE OVER $\mathbb{Q}(u)$ WITH TORSION $\mathbb{Z}/4\mathbb{Z}$ AND RANK 6

Elkies [6] mentions, without explicitly writing such examples, that there are several quadratic sections giving curves over $\mathbb{Q}(u)$ with rank 5 for this torsion and several combinations of pairs of quadratic sections leading to infinite families of curves with rank 6 parametrized by the points of elliptic curves of positive rank.

In [5], we made explicit the ideas of Elkies, and presented there 25 elliptic curves over $\mathbb{Q}(u)$ with rank 5 and several infinite families of curves with rank 6 parametrized by elliptic curves with positive rank.

Now we have many more examples of quadratic sections over $\mathbb{Q}(u)$ leading to rank 5 curves. In one of these curves, we found a further quadratic section leading to the curve over $\mathbb{Q}(u)$ having rank 6.

In fact, observe that imposing

$$\frac{-64(1+t)^2(-4+7t)(4+17t)}{(1+4t)^2}$$

as the X-coordinate of a new point in the Elkies surface E is equivalent to the condition $-(-4+7t)(4+17t) = \square$, which can be solved with

$$t \mapsto \frac{4(-1+u^2)}{(17+7u^2)}.$$

The resulting curve has rank 5. (For a general strategy for imposing new points which might lead to conditions equivalent to genus 0 or 1 curves, see, e.g. [4].)

On the other hand, imposing

$$\frac{576(-4+7t)(-8+15t)^2(-1324+5551t)}{49(-39+28t)^2}$$

as the X-coordinate of a new point in the Elkies surface E is equivalent to the condition $(-4+7t)(-1324+5551t) = \square$, which can be solved with

$$t \mapsto \frac{4(-331+u^2)}{7(-793+u^2)}.$$

The corresponding specialization also has rank 5.

But now we observe that in both conditions

$$-(-4+7t)(4+17t) = \square$$
$$(-4+7t)(-1324+5551t) = \square,$$

the same factor $(-4+7t)$ appears. This implies that both conditions can be satisfied simultaneously since when we apply the solution of the first condition to the second, we have to solve $-(-1863+539u^2) = z^2$ in order to satisfy both conditions. But this genus 0 curve has rational points, i.e. $(u, z) = (13/7, 2)$, so we can find the parametric solution

$$u \mapsto \frac{-7007 - 28r + 13r^2}{7(539 + r^2)}.$$

So we can satisfy both conditions with

$$t \mapsto \frac{4\left(3r^2 - 14r - 5390\right)\left(10r^2 - 14r - 1617\right)}{7\left(72r^4 - 182r^3 - 13279r^2 + 98098r + 20917512\right)}.$$

By inserting this into E, we get the curve over $\mathbb{Q}(r)$ given by

$$y^2 = x^3 + a_6(r)x^2 + b_6(r)x,$$

where

$a_6(r) = 3(6637977907200r^{16} - 327957190299648r^{15} - 132939477324670464r^{14} +$

$1334557851651990784r^{13} + 73205200037549219248r^{12} -$

$171812511935907428476 8r^{11} - 193538301177692188691736r^{10} +$

$190518955562616527788687 2r^9 + 966248556489928542202478 19r^8 -$

$1026897170482503084781024008r^7 - 56226940796444312350911834456r^6 +$

$269042619584910197333660344992r^5 + 617869834139793935422678253636 8r^4 -$

$607129353511324518060938011420 16r^3 - 325976699371446457995776649598310 4r^2 +$

$4334495070152077221968455683796992 r + 4728745316169389643146171120056320 0),$

$b_6(r) = 7225344(r - 224)^2(r + 154)^2(2r - 7)^2(32r + 77)^2 \left(18r^2 + 14r + 16709\right)^2$

$\left(24r^2 - 1001r + 14014\right)^2 \left(26r^2 + 1001r + 12936\right)^2 \left(31r^2 - 14r + 9702\right)^2$

$\left(72r^4 - 182r^3 - 13279r^2 + 98098r + 20917512\right)^2.$

The x-coordinates of six independent points of infinite order are

$x_1 = -53067(r - 224)(r + 154)(2r - 7)(32r + 77)(24r^2 - 1001r + 14014) \times$

$(26r^2 + 1001r + 12936)(72r^4 - 182r^3 - 13279r^2 + 98098r + 20917512)^2,$

$x_2 = -48(r - 224)(r + 154)(2r - 7)(32r + 77)(18r^2 + 14r + 16709) \times$

$(31r^2 - 14r + 9702)(2424r^4 - 12922r^3 - 3840473r^2 + 6964958r + 704222904)^2,$

$x_3 = 144(16709 + 14r + 18r^2)(14014 - 1001r + 24r^2)(12936 + 1001r + 26r^2) \times$

$(9702 - 14r + 31r^2)(155719256 - 490490r + 1032283r^2 + 910r^3 + 536r^4)^2,$

$x_4 = 576(16709 + 14r + 18r^2)(14014 - 1001r + 24r^2)(12936 + 1001r + 26r^2) \times$

$(9702 - 14r + 31r^2)(434619416 + 2648646r - 841477r^2 - 4914r^3 + 1496r^4)^2,$

$x_5 = (12936 + 1001r + 26r^2)^2(20917512 + 98098r - 13279r^2 - 182r^3 + 72r^4)^2 \times$

$\dfrac{88510464(539 + r^2)^2(-7007 - 28r + 13r^2)^2(14014 - 1001r + 24r^2)^2}{(285872664 + 2256254r - 1029833r^2 - 4186r^3 + 984r^4)^2},$

$x_6 = (9702 - 14r + 31r^2)^2(20917512 + 98098r - 13279r^2 - 182r^3 + 72r^4)^2 \times$

$\dfrac{260112384(539 + r^2)^2(-539 + 1001r + r^2)^2(16709 + 14r + 18r^2)^2}{(676332888 + 2256254r + 418999r^2 - 4186r^3 + 2328r^4)^2}.$

Since the specification map is a homomorphism, to show that these six points are independent, it suffices to find a rational number r for which the points are specialized to six independent $\mathbb{Q}$-rational points. It is easy to check that we may take, e.g. $r = 1$.

Moreover, for $r = 13$, the conditions of the Gusić-Tadić algorithm for finding injective specializations (see [9, Theorem 1.3] and [8]) are satisfied, so the rank over $\mathbb{Q}(r)$ is exactly 6.

This specialization also indicates that the points $P_1, P_2, P_3, P_4, P_5, P_6$, where $x(P_i) = X_i$ for $i = 1, 2, \ldots, 6$, do not generate the full Mordell-Weil

group over $\mathbb{Q}(r)$ modulo torsion, but a subgroup of order 4 (since the quotient of the corresponding regulators is 16). Indeed, it holds that $P_3 + P_4 + P_5 = 2R_5$ and $P_3 + P_4 + P_6 = 2R_6$, where

$$x(R_5) = 1344(72r^4 - 182r^3 - 13279r^2 + 98098r + 20917512)(2r - 7)^2(32r + 77)^2 \times$$
$$(18r^2 + 14r + 16709)^2(11r^2 + 14r + 12936)^2,$$
$$x(R_6) = 1344(18r^2 + 14r + 16709)(26r^2 + 1001r + 12936)(31r^2 - 14r + 9702) \times$$
$$(24r^2 - 1001r + 14014)(72r^4 - 182r^3 - 13279r^2 + 98098r + 20917512) \times$$
$$\frac{(r + 154)^2(32r + 77)^2(6r^2 - 91r + 3332)^2}{(30r^2 - 1001r + 17248)^2},$$

and now the points $P_1, P_2, P_3, P_4, R_5, R_6$ generate the full Mordell-Weil group over $\mathbb{Q}(r)$ modulo torsion.

5. CONCLUDING REMARKS

Let us mention that the heuristic of Park, Poonen, Voight and Wood (see [17, Section 8.3]) predicts that there are only finitely many elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank greater than 7, which indicates that our result might be close to the best possible.

However, the recent paper by Dujella, Kazalicki and Peral [3] might indicate that the heuristic in [17] needs some adjustments, at least in the case of curves with certain torsion groups. Namely, they examined families with rank 3 for torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and the experiments suggest that in these families, root numbers 1 and -1 (which conjecturally means even and odd ranks) are equidistributed, which would imply that there are infinitely many curves with rank ≥ 4 for these torsion groups, while the heuristic in [17] predicts that there are only finitely many elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank greater than 3.

REFERENCES

[1] A. Dujella, *High rank elliptic curves with prescribed torsion*,
    `http://web.math.hr/~duje/tors/tors.html`.
[2] A. Dujella, *Infinite families of elliptic curves with high rank and prescribed torsion*,
    `http://web.math.hr/~duje/tors/generic.html`.
[3] A. Dujella, M. Kazalicki and J. C. Peral, *Elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115** (2021), Article 169, (24pp).
[4] A. Dujella and J. C. Peral, *Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$*, in: Trends in Number Theory, Contemp. Math. **649** (2015), 47–62.

[5] A. Dujella and J. C. Peral, *Construction of high rank elliptic curves,* J. Geom. Analysis **31** (2021), 6698–6724.

[6] N. Elkies, *Three lectures on elliptic surfaces and curves of high rank,* `arXiv:0709.2908` (2007)

[7] N. Elkies and Z. Klagsbrun, *New rank records for elliptic curves having rational torsion,* Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley, 2020, pp. 233–250.

[8] I. Gusić and P. Tadić, *A remark on the injectivity of the specialization homomorphism,* Glas. Mat. Ser. III **47** (2012), 265–275.

[9] I. Gusić and P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves,* J. Number Theory **148** (2015), 137–152.

[10] H. Inose, *Defining equations of singular K3 surfaces and a notion of isogeny,* in: Proceedings of the International Symposium on Algebraic Geometry, Kinokuniya Book Store, Tokyo, 1978, pp. 495–502.

[11] F. Khoshnam and D. Moody, *High rank elliptic curves with torsion $\mathbb{Z}/4\mathbb{Z}$) induced by Kihara's elliptic curves,* Integers **16** (2016), Paper No. A70, 12 pp.

[12] S. Kihara, *On the rank of elliptic curves with a rational point of order 4,* Proc. Japan Acad. Ser A Math. Sci. **80** (2004), 26–27.

[13] S. Kihara, *On the rank of elliptic curves with a rational point of order 4, II,* Proc. Japan Acad. Ser A Math. Sci. **80** (2004), 158–159

[14] Z. Klagsbrun, T. Sherman and J. Weigandt, *The Elkies curve has rank 28 subject only to GRH,* Math. Comp. **88** (2019), 837–846

[15] O. Lecacheux, *Rang de courbes elliptiques dont le groupe de torsion est non trivial,* Ann. Sci. Math. Quebec **28** (2004), 145–151

[16] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[17] J. Park, B. Poonen, J. Voight and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves,* J. Eur. Math. Soc. (JEMS) **21** (2019), 2859–2903.

[18] M. Schutt and T. Shioda, Mordell-Weil Lattices, Springer, Singapore, 2019.

Eliptička krivulja nad $\mathbb{Q}(u)$ s torzijom $\mathbb{Z}/4\mathbb{Z}$ i rangom 6

Andrej Dujella i Juan Carlos Peral

SAŽETAK. U ovom radu prikazujemo konstrukciju eliptičke krivulje nad $\mathbb{Q}(u)$ s torzijskom grupom $\mathbb{Z}/4\mathbb{Z}$ i rangom 6. Prethodno su bili poznati samo primjeri ranga 5 za takve krivulje.

Department of Mathematics
Faculty of Science
University of Zagreb
Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail: `duje@math.hr`

Departamento de Matemáticas
Universidad del País Vasco
Aptdo. 644, 48080 Bilbao, Spain
E-mail: `juancarlos.peral@ehu.es`