Elliptic curves with a point of order 13 defined over cyclic cubic fields

Bruin, P.J.; Derickx, M.; Stoll, M.

Functiones et Approximatio
65.2 (2021), 191–197
doi: 10.7169/facm/1945

ELLIPTIC CURVES WITH A POINT OF ORDER 13 DEFINED OVER CYCLIC CUBIC FIELDS

Peter Bruin, Maarten Derickx, Michael Stoll

Abstract: We show that there is essentially a unique elliptic curve E defined over a cubic Galois extension K of $\mathbb{Q}$ with a K-rational point of order 13 and such that E is not defined over $\mathbb{Q}$.

Keywords: elliptic curves, torsion points, cyclic cubic fields.

1. Introduction

Let K be a number field and let E be an elliptic curve over K. The question what the possible orders of torsion points in $E(K)$ are (or, more generally, which finite abelian groups occur as the group of K-rational torsion points of some E) has received much attention in the recent past. Mazur [18] famously solved this problem for $K = \mathbb{Q}$. Kenku and Momose [17] and Kamienny [15, 16] dealt with quadratic number fields. Merel [20] proved that for fields K of a given degree d, there are only finitely many possibilities for the order of a torsion point (and therefore also for the torsion subgroup). Jeon, with various coauthors [14, 9] determined which torsion structures occur infinitely often for cubic fields. Najman [21] found a sporadic example with a point of order 21 over a cubic field (with the curve defined over $\mathbb{Q}$); this is not on Jeon et al.'s list. The second author together with Etropolski, van Hoeij, Morrow and Zureick-Brown [4], building on the results of Parent [22, 23], proved that $\mathbb{Z}/21\mathbb{Z}$ is actually the only torsion structure that occurs finitely often over cubic fields. Jeon [8] also determined which torsion structures occur infinitely often over cyclic cubic fields. The second author and Najman [5] classified all torsion groups that occur over cyclic cubic fields. There are similar results by Jeon and coauthors for quartic fields [13, 10, 11, 12]. Results on which prime numbers can occur as the order of a torsion point over a field of degree $d \leqslant 7$ can be found in a forthcoming paper by Kamienny, Stein and the last two authors of this note [6].

2020 Mathematics Subject Classification: primary: 11G05, 14G05, 14G25, 14H52

In this note, we consider the cubic case. More precisely, we complete the classification of elliptic curves over cyclic cubic fields that have a point of order 13. Jeon in [8] already found an infinite family (with parameter space an open subset of the projective line) of such curves. They are obtained by pulling back rational points under a cyclic degree 3 Galois cover $X_1(13) \to \mathbb{P}^1$, which is derived from the action of the diamond operators on $X_1(13)$. This implies that the target $\mathbb{P}^1$ is a modular curve itself, and all the curves in the family are in fact already defined over $\mathbb{Q}$ (and acquire a point of order 13 over a cyclic cubic extension). We show that outside this family, there is essentially one other example, which is an elliptic curve that cannot be defined over $\mathbb{Q}$. This can be seen as a complement to [5], where similar results are obtained for points of order 16 and 20.

Acknowledgments. We thank the organizers of the conference on "Torsion groups and Galois representations of elliptic curves" in Zagreb in June 2018, where the work described in this note was done, and Daeyeol Jeon for providing the motivation for this work by pointing out in his talk at the conference that $X_1(13)$ arises as a Galois covering of $\mathbb{P}^1$ of degree 3 over $\mathbb{Q}$, raising the question whether there are additional "sporadic" elliptic curves over a cyclic number field with a point of order 13. We also thank the anonymous referee for the suggestion to provide a geometric explanation for the occurrence of hyperelliptic curves.

The computations were done using the Magma computer algebra system [1].

2. The result

Our goal is to classify all elliptic curves E defined over a cyclic cubic extension K of $\mathbb{Q}$ such that $E(K)$ contains points of order 13. The main result is as follows.

Theorem 2.1. *Let K be a cubic Galois extension of $\mathbb{Q}$ and let E be an elliptic curve defined over K with $E(K)[13] \neq 0$. Then either E can be defined over $\mathbb{Q}$, or else $K = \mathbb{Q}(\alpha)$ with*

$$\alpha^3 - \alpha^2 - 82\alpha + 64 = 0$$

and E is isomorphic to a Galois conjugate of the curve

$$E_0 \colon y^2 + (1-c)xy - by = x^3 - bx^2\,,$$

where

$$b = \frac{10\alpha^2 + 90\alpha - 1936}{19773} \qquad \text{and} \qquad c = \frac{6\alpha^2 + 50\alpha - 208}{1521}\,.$$

To obtain this result, we find all degree 3 morphisms $X_1(13) \to \mathbb{P}^1$ that are defined over $\mathbb{Q}$ and determine all their fibers above rational points that give rise to a cyclic cubic extension of $\mathbb{Q}$. There are exactly 13 such morphisms (up to automorphisms of $\mathbb{P}^1$). One of these is obtained by dividing by a subgroup of order 3 of the group generated by the diamond operators on $X_1(13)$. All its fibers are cyclic or split; this gives rise to the family of elliptic curves over $\mathbb{Q}$ with points

of order 13 defined over a cyclic cubic field found by Jeon [8]. Explicitly, this family can be obtained as

$$E_t\colon y^2 = x^3 - 27A(t)x + 54(t^2+1)B(t)$$

with

$$A(t) = \frac{t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1}{t^4 - t^3 + 5t^2 + t + 1}$$

and

$$B(t) = \frac{\begin{array}{r} t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 \\ - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1 \end{array}}{(t^4 - t^3 + 5t^2 + t + 1)^2}\,.$$

A point of order 13 on E_t is given by

$$P_t = \Big(\frac{36tw + 3(t^6 - 3t^5 + 4t^4 - 6t^3 - 8t^2 + 3t + 1)}{t^4 - t^3 + 5t^2 + t + 1}, \frac{108t((t+1)w - t)}{t^4 - t^3 + 5t^2 + t + 1}\Big)\,,$$

where

$$w^3 + (-t^3 + t^2 - 3t + 1)w^2 + (-t^3 + 2t^2 - 2t)w + t^2 = 0\,.$$

This last polynomial has discriminant $t^4(t^4 - t^3 + 5t^2 + t + 1)^2$ and therefore defines, for $t \in \mathbb{Q} \setminus \{0\}$, a cyclic cubic number field. (Our parameter t is related to t_{Jeon} of [8] by $t_{\text{Jeon}} = -\frac{7}{72} - \frac{1}{36t}$.)

The other 12 morphisms fall into two orbits under the group of diamond operators (which is cyclic of order 6). These morphisms are not Galois coverings of $\mathbb{P}^1$, so their fibers usually define S_3-extensions of $\mathbb{Q}$. The condition for a fiber to be cyclic is expressed by requiring the discriminant of a cubic polynomial over $\mathbb{Q}(t)$ (where t is a parameter on $\mathbb{P}^1$; adjoining a root of the cubic defines the covering) to be a square. This defines a hyperelliptic curve. For one of the two orbits, we obtain a curve of genus 2, for which we can prove by using Chabauty's method that it has exactly five rational points. Three of these points arise from split fibers containing cusps, but one pair of points corresponds to a rational point on $\mathbb{P}^1$ that has a cyclic fiber above it, leading to the curve E_0 in Theorem 2.1. The remaining orbit leads to a curve of genus 3, for which we can prove that it has exactly three rational points; they all correspond to ramified fibers containing cusps. The details are given in the next section.

A more geometric way of seeing that the question reduces to the determination of the set of rational points on some hyperelliptic curves is as follows. Points in $X_1(13)$ that are defined over cyclic cubic fields give rise to rational points on the quotient $X_1(13)^3/C_3$, where the cyclic group C_3 acts by permuting the factors. Viewing $C_3 = A_3$ as a subgroup of the symmetric group S_3, we obtain morphisms

$$X_1(13)^3/C_3 \xrightarrow{\varphi} X_1(13)^3/S_3 = X_1(13)^{(3)} \xrightarrow{\pi} \mathrm{Pic}^3_{X_1(13)}\,.$$

The symmetric cube in the middle parameterizes effective divisors of degree 3; π maps to the linear equivalence class. The fiber of π above any point is a $\mathbb{P}^1$ (by

Riemann-Roch); φ is a ramified double cover, so the fibers of the composition are ramified double covers of $\mathbb{P}^1$, i.e., hyperelliptic curves, unless the fiber of π meets the branch locus of φ everywhere with even multiplicity, in which case we obtain a union of two $\mathbb{P}^1$'s. This is what happens for Jeon's family; in all other cases of interest we do indeed obtain a hyperelliptic curve.

3. Proof of the theorem

In the following, we will write X for $X_1(13)$. We use the model of X given by

$$y^2 + (x^3 + x^2 + 1)y = x^2 + x\,;$$

see Sutherland's table [26]. In particular, X has genus 2 and is (therefore) hyperelliptic. The *canonical class* on X is the linear equivalence class of divisors arising by pulling back a point under the hyperelliptic covering map $X \to \mathbb{P}^1$; it is the same as the class containing the canonical divisors.

The map $X = X_1(13) \to X_0(13)$, obtained by sending a point of order 13 to the group it generates, is Galois over $\mathbb{Q}$. Its automorphism group consists of the diamond operators and is canonically isomorphic to $(\mathbb{Z}/13\mathbb{Z})^\times/\{\pm 1\}$, which is a cyclic group of order 6; we denote this group by G.

It is known that $X(\mathbb{Q})$ consists of the six rational cusps and that the group of rational points on its Jacobian J is cyclic of order 19; see [19]. The rational points on X form one orbit under G; they are the two points at infinity and the points $(-1,-1)$, $(-1,0)$, $(0,-1)$ and $(0,0)$ on our model of X.

Since the genus of X is 2, every rational point on J except the origin has a unique representation as an effective divisor D of degree 2 minus the canonical class, with the points in the support of D either rational or defined over a quadratic extension of $\mathbb{Q}$ and conjugate, where D is not in the canonical class. Since the six rational points lead to exactly 18 effective divisors of degree 2 outside the canonical class, they account for all the rational points in J, which implies that there are no quadratic points with irrational x-coordinate. See [2, 7].

Now consider a point $P \in X$ with $[\mathbb{Q}(P) : \mathbb{Q}] = 3$. The sum of P and its two Galois conjugates is a rational effective divisor D of degree 3, so it gives a rational point on the symmetric cube S of X. Under the canonical map $\pi\colon S \to \mathrm{Pic}^3(X)$, it maps to a rational point on $\mathrm{Pic}^3(X)$. The fibers of π are $\mathbb{P}^1$'s; this follows from the Riemann-Roch theorem.

Since $\mathrm{Pic}^3(X)$ is isomorphic to J (note that X has rational points), it has exactly 19 rational points. Therefore D lies in the fiber of π above one of these points. Six of the rational points on $\mathrm{Pic}^3(X)$ arise as a rational point on X plus the canonical class. This implies that all divisors in the corresponding fiber contain this rational point and can therefore never contain a cubic point.

For the remaining 13 rational points on $\mathrm{Pic}^3(X)$, the corresponding line bundle $\mathcal{L}$ is basepoint-free. In this case, the fiber of π above the point can be identified with the target of the morphism $X \to \mathbb{P}^1$ defined by the two-dimensional space of global sections of the line bundle $\mathcal{L}$. This implies that each cubic point on X lies in the fiber of one of these morphisms $X \to \mathbb{P}^1$ above a rational point of $\mathbb{P}^1$.

These 13 rational points on $\mathrm{Pic}^3(X)$ consist of one point that is fixed by G and two orbits of size 6 under G. It clearly suffices to determine the cyclic cubic points in the fibers of the degree 3 morphisms $X \to \mathbb{P}^1$ associated to one representative of each orbit.

Let G' be the subgroup of order 3 of G. The quotient X/G' is a curve of genus 0, so the map $X \to X/G'$ must show up in our list. Since this quotient is unique, the map must correspond to the point in $\mathrm{Pic}^3(X)(\mathbb{Q})$ that is fixed by G. Since $X \to X/G'$ is a Galois covering, all its fibers over rational points are either ramified, split, or cyclic. The modular curve X/G' is a double cover of $X_0(13)$; viewing G' as the group of diamond operators $\{\langle 1\rangle, \langle 3\rangle, \langle 9\rangle\}$, we see that X/G' is a fine moduli space outside the branch locus of $X \to X/G'$ (the image in X/G' of the zero locus of $x^2 + x + 1$ in our model of X.) Since the cubic points arising in fibers of $X \to X/G'$ map to rational points on X/G' outside this branch locus, the elliptic curves they represent are defined over $\mathbb{Q}$. This accounts for the first alternative in Theorem 2.1. (We have made this one-parameter family explicit in the previous section.)

One representative of one of the other two orbits of degree 3 morphisms to $\mathbb{P}^1$ is given by the y-coordinate map of our model of X. The discriminant with respect to x of the equation defining X is

$$d_1(y) = (y+1)(-27y^5 - 31y^4 - 6y^3 + 6y^2 + 5y + 1)\,;$$

the condition that this is a square then defines a hyperelliptic curve D_1 of genus 2. A quick search finds five rational points on D_1: one point with $y = -1$ and two each with $y = 0$ and $y = -\frac{4}{13}$. So there are three fibers of the y-coordinate map with Galois group contained in A_3. The first two contain rational points on X, but the fiber above $-\frac{4}{13}$ really consists of three conjugate points defined over the cyclic extension K; they and the other points in their G-orbits give rise to the curve E_0 and its Galois conjugates mentioned in 2.1. (It can be easily checked that the point $(0, 0)$ on E_0 indeed has order 13. The discriminant of K is $(13 \cdot 19)^2$.)

Using the Magma implementation of 2-descent on hyperelliptic Jacobians as described in [24], we find that the Mordell-Weil rank of the Jacobian of D_1 is at most 1. From the rational points we have found on D_1, we can easily construct a rational point of infinite order on the Jacobian. A combination of Chabauty's method with the Mordell-Weil sieve as explained in [3] and implemented in Magma then quickly proves that the five points we found are indeed all the rational points on D_1.

A representative of the remaining orbit is $X \to \mathbb{P}^1$ given by $\frac{y+1}{x}$. Writing t for the parameter on $\mathbb{P}^1$, we have $y = xt - 1$. Plugging this into the equation of X and taking the discriminant with respect to x gives

$$d_2(t) = t(t+1)^3(-4t^5 + 5t^4 - t^3 - 25t^2 - 23t - 4)\,.$$

Setting $d_2(t)/(t+1)^2$ equal to a square gives a hyperelliptic curve D_2 of genus 3. It has three obvious rational Weierstrass points at infinity and with $t = -1$ or 0. We do not find any other rational point. Using 2-descent again, we can show that

the Mordell-Weil rank of the Jacobian is 0. A minimal model of D_2 is

$$v^2 + (u^3 + u^2)v = u^7 - 8u^5 - 13u^4 - 7u^3 - 2u^2 - u\,;$$

from this we see that D_2 has good reduction at 2. The reduction has exactly three $\mathbb{F}_2$-points, which are the images of the three rational points we had found. Since their residue disks are fixed by the hyperelliptic involution, we know that each of the three residue disks contains an odd number of rational points. Since the Mordell-Weil group is finite, all 2-adic integrals $\int_P^Q \omega$ between rational points $P, Q \in D_2(\mathbb{Q})$ for regular differentials ω must vanish. In particular, we can, for each residue class, choose a differential whose reduction mod 2 does not vanish in the corresponding $\mathbb{F}_2$-point on the reduction. By [25, Section 6], the corresponding integral vanishes for at most two points in the residue class. Since it has to vanish at each rational point and the number of rational points in the residue class is odd, there is only the known rational point in each of the three residue classes, which shows that $\#D_2(\mathbb{Q}) = 3$. These three points are all images of cusps, so we do not obtain any further cyclic cubic points on X. This concludes the proof.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN (2014), no. 11, 2885–2923.

[3] N. Bruin, M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306.

[4] M. Derickx, A. Etropolski, M. van Hoeij, J.S. Morrow, D. Zureick-Brown, *Sporadic Cubic Torsion*, arXiv:2007.13929, to appear in Algebra & Number Theory.

[5] M. Derickx, F. Najman, *Torsion of elliptic curves over cyclic cubic fields*, Math. Comp. **88** (2019), no. 319, 2443–2459.

[6] M. Derickx, S. Kamienny, W. Stein, M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, arXiv:1707.00364.

[7] M. Derickx, B. Mazur, S. Kamienny, *Rational families of 17-torsion points of elliptic curves over number fields*, Number theory related to modular curves — Momose memorial volume, Contemp. Math. **701**, Amer. Math. Soc., Providence, RI, 2018, 81–104.

[8] D. Jeon, *Families of elliptic curves over cyclic cubic number fields with prescribed torsion*, Math. Comp. **85** (2016), no. 299, 1485–1502.

[9] D. Jeon, C.H. Kim, Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 273, 579–591.

[10] D. Jeon, C.H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 276, 2395–2410.

[11] D. Jeon, C.H. Kim, Y. Lee, *Infinite families of elliptic curves over dihedral quartic number fields*, J. Number Theory **133** (2013), no. 1, 115–122.
[12] D. Jeon, C.H. Kim, Y. Lee, *Families of elliptic curves with prescribed torsion subgroups over dihedral quartic fields*, J. Number Theory **147** (2015), 342–363.
[13] D. Jeon, C.H. Kim, E.Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), no. 1, 1–12.
[14] D. Jeon, C.H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301.
[15] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162.
[16] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.
[17] M.A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
[18] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978).
[19] B. Mazur, J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49.
[20] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.
[21] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett. **23** (2016), no. 1, 245–272.
[22] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749.
[23] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux **15** (2003), no. 3, 831–838.
[24] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277.
[25] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214.
[26] A. Sutherland, *Optimized equations for* $X_1(N)$, http://math.mit.edu/~drew/X1_optcurves.html.

Addresses: Peter Bruin: Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands;
Maarten Derickx: Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands;
Michael Stoll: Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail: P.J.Bruin@math.leidenuniv.nl, maarten@mderickx.nl, Michael.Stoll@uni-bayreuth.de

Received: 26 January 2021; **revised:** 8 March 2021