TORSION POINTS ON ELLIPTIC CURVES OVER QUARTIC NUMBER FIELDS

SHELDON KAMIENNY, WILLIAM STEIN, AND MICHAEL STOLL

Abstract. We complete the proof that there are no elliptic curves over a number field K of degree ≤ 4 that have a K-rational point of prime order > 17.

1. Introduction

For an integer $d \geq 1$, we let $S(d)$ be the set of primes p such there exists an elliptic curve E over a number field K of degree $\leq d$ with a K-rational point of order p in $E(K)$. Mazur has famously proved that

$$S(1) = \{2, 3, 5, 7\}.$$

Kamienny and Mazur showed that

$$S(2) = \{2, 3, 5, 7, 11, 13\},$$

and Parent, building on earlier work by Kamienny, proved that

$$S(3) = \{2, 3, 5, 7, 11, 13\}.$$

Our main result is the following.

Theorem 1.

$$S(4) = \{2, 3, 5, 7, 11, 13, 17\}.$$

Proof. Kamienny and Stein [4] show that $S(4)$ does not contain any $p > 31$. Theorem 10 below shows that $19, 23 \notin S(4)$. Theorem 8 below shows that $31 \notin S(4)$. Finally, Theorem **??** below shows that $29 \notin S(4)$. □

Should be extended and proper references added.

Date: May 10, 2010.

2. The result

We first state a general results on points of degree $\leq d$ on a curve over $\mathbb{Q}$. All curves will be assumed to be smooth, projective and geometrically integral. We will use $C^{(d)}$ to denote the dth symmetric power of C.

Proposition 2. *Let $C/\mathbb{Q}$ be a curve with Jacobian J, let $d \geq 1$ be an integer, and let ℓ be a prime of good reduction for C. Let $P_0 \in C(\mathbb{Q})$ be chosen as base-point for an embedding $\iota : C \to J$. We make the following assumptions.*

1. *$J(\mathbb{Q})$ is finite.*
2. *$\ell > 2$ or $J(\mathbb{Q})[2]$ injects into $J(\mathbb{F}_\ell)$ (for example, $\#J(\mathbb{Q})$ is odd).*
3. *There is no rational function in $\mathbb{Q}(C)^\times$ of degree $\leq d$.*
4. *The reduction map $C(\mathbb{Q}) \to C(\mathbb{F}_\ell)$ is surjective.*
5. *If $P \in C(\bar{\mathbb{F}}_\ell) \setminus C(\mathbb{F}_\ell)$ is a point of degree $d' \leq d$, then $\mathrm{Tr}_{\mathbb{F}_{\ell^{d'}}/\mathbb{F}_\ell} \iota(P) \in J(\mathbb{F}_\ell)$ is not in the image of $J(\mathbb{Q})$.*

Then the only points of degree $\leq d$ on C are the rational points on C.

Proof. We will use ρ_X to denote the reduction map $X(\mathbb{Q}) \to X(\mathbb{F}_\ell)$, where X is a smooth projective variety over $\mathbb{Q}$ with good reduction at ℓ.

From assumptions 1 and 2 (and the fact that ℓ is a good prime) we can deduce that $\rho_J : J(\mathbb{Q}) \to J(\mathbb{F}_\ell)$ is injective. Assumption 3 implies that the map $C^{(d)}(\mathbb{Q}) \to J(\mathbb{Q})$ induced by ι is also injective. Considering the commutative diagram

$$\begin{array}{ccc} C^{(d)}(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow{\scriptstyle \rho_{C^{(d)}}} & & \downarrow{\scriptstyle \rho_J} \\ C^{(d)}(\mathbb{F}_\ell) & \xrightarrow{\iota} & J(\mathbb{F}_\ell), \end{array}$$

we conclude that $\rho_{C^{(d)}}$ is injective as well.

Assumption 5 tells us that the image of $\rho_{C^{(d)}}$ is contained in the image $C^{(d)}(\mathbb{F}_\ell)_{\mathrm{split}}$ of $C(\mathbb{F}_\ell)^d$ in $C^{(d)}(\mathbb{F}_\ell)$. We now consider the diagram

$$\begin{array}{ccc} C(\mathbb{Q})^d & \longrightarrow & C^{(d)}(\mathbb{Q}) \\ \downarrow{\scriptstyle \rho_{C^d}} & & \downarrow{\scriptstyle \rho_{C^{(d)}}} \\ C(\mathbb{F}_\ell)^d & \twoheadrightarrow & C^{(d)}(\mathbb{F}_\ell)_{\mathrm{split}}. \end{array}$$

The left hand vertical map is surjective by assumption 4, the right hand vertical map is injective by the argument above. We conclude that $C(\mathbb{Q})^d$ surjects onto $C^{(d)}(\mathbb{Q})$. This implies the claim, since a non-rational point of degree $\leq d$ on C would induce a point in $C^{(d)}(\mathbb{Q})$ that is not in the image of $C(\mathbb{Q})^d$. $\square$

We can apply this to torsion points on elliptic curves as follows. We use the cusp at infinity as a base-point on $X_1(p)$. Note that $X_1(p)$ has $p-1$ cusps, half of which are rational, the other half being conjugate and defined over the maximal real subfield of $\mathbb{Q}(\mu_p)$. William: Can you confirm this?

Theorem 3. *Let p and ℓ be primes with $\ell \neq p$, and let $d \geq 1$. Assume that*

1. *$J_1(p)(\mathbb{Q})$ is finite.*
2. *$\ell > 2$ or $\#J_1(p)(\mathbb{Q})$ is odd.*
3. *The order of ℓ in $\mathbb{F}_p^\times/\{\pm 1\}$ is $> d$.*
4. *$p > (\sqrt{\ell}+1)^2$.*
5. *If $E/\mathbb{F}_{\ell^e}$ is an elliptic curve that has an $\mathbb{F}_{\ell^e}$-rational point of order p and $e \leq d$, then the trace of its image in $J_1(p)$ is not in the image of $J_1(p)(\mathbb{Q})$.*

Then there are no elliptic curves E/K with $[K:\mathbb{Q}] \leq d$ that have a K-rational point of order p, or else there are infinitely many.

Proof. If $p \leq 7$, then there are even infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order p. So in the remainder of the proof, we can assume that $p \geq 11$.

We use Prop. 2. The first two assumptions in the theorem imply the first two assumptions of the proposition. We will deal with Assumption 3 in the proposition later.

Assumption 3 of the theorem implies that the only cusps of degree $\leq d$ on $X_1(p)/\mathbb{F}_\ell$ are the images of the rational cusps (the order of ℓ in $\mathbb{F}_p^\times/\{\pm 1\}$ gives the length of the Frobenius-orbits on the images of the non-rational cusps). Assumption 4 of the theorem shows that there all points in $X_1(p)(\mathbb{F}_\ell)$ are cusps. Together with the fact that $X_1(p)(\mathbb{Q})$ consists of cusps (since $p \geq 11$), this implies assumption 4 of the proposition. Assumption 5 of the theorem then implies assumption 5 of the proposition, since there are no other $\mathbb{F}_{\ell^e}$-rational points except for the $\mathbb{F}_\ell$-rational cusps.

Now we consider assumption 3 of the proposition. If it holds, we can apply the proposition, and we find that there are no non-rational points of degree $\leq d$ on $X_1(p)$. This implies that there are no elliptic curves over a number field K of degree $\leq d$ with a K-rational point of order p, since the rational points on $X_1(p)$ are all cusps (by our assumption that $p \geq 11$).

If assumption 3 of the proposition does not hold, then $X_1(p)^{(d)} \to J_1(p)$ is not an embedding. Let Y be a fiber of positive dimension. If Y contains a rational point, then $Y \cong \mathbb{P}^n$ for some $n \geq 1$, and so Y contains infinitely many rational points. Since the image of $X_1(p)(\mathbb{Q})^d$ in $X_1(p)^{(d)}(\mathbb{Q})$ is finite ($X_1(p)(\mathbb{Q})$ is finite), the infinitely many rational points on Y involve infinitely many non-cuspidal points. Hence there are infinitely many elliptic curves with the required property. If, on

the other hand, none of the positive-dimensional fibers contains a rational point, then the proof of Prop. 2 applies, and there are no elliptic curves with the required properties. □

Corollary 4. *Let p be a prime and $d \geq 1$ such that*

(1) *$J_1(p)(\mathbb{Q})$ is finite.*
(2) *$\#J_1(p)(\mathbb{Q})[2]$ injects into $J_1(p)(\mathbb{F}_2)$ and $p > (2^{d/2}+1)^2$, or $p > (3^{d/2}+1)^2$.*

The either there are infinitely many elliptic curves E/K with $[K:\mathbb{Q}] \leq d$ such that $E(K)$ contains a point of order p, or else there are none.

Proof. We take $\ell = 2$ or $\ell = 3$ in Thm 3. The first two assumptions in the theorem are satisfied, and so is assumption 4. Assumption 3 follows from $\ell^d < p+1$, which is a consequence of assumption 2 in the corollary. Finally, assumption 5 again follows from the second assumption in the corollary, since by the Hasse bound, any elliptic curve $E/\mathbb{F}_{\ell^e}$ with $e \leq d$ satisfies $\#E(\mathbb{F}_{\ell^e}) < p$. Therefore the theorem applies. □

We quote Prop. 6.2.1. of [2] (in an equivalent formulation), adding some more information from Section 6.2 in loc.cit.

Proposition 5. *The primes p such that $J_1(p)$ has rank zero are the primes $p \leq 31$ and 41, 47, 59, and 71.*

For all of these except possibly $p = 29$, the Mordell-Weil group is generated by differences of rational cusps, and for all except $p = 17, 29, 31$ and 41, the order of $J_1(p)(\mathbb{Q})$ is odd.

We also quote the main result from [3].

Theorem 6. *Exactly the following torsion structures occur infinitely often for elliptic curves over number fields K of degree ≤ 4.*

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\quad \text{for } m \leq 18, \text{ or } m \in \{20, 21, 22, 24\}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2v\mathbb{Z} &\quad \text{for } v \leq 9, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3v\mathbb{Z} &\quad \text{for } v \leq 3, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4v\mathbb{Z} &\quad \text{for } v \leq 2, \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\quad \text{and} \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}. & \end{aligned}$$

In particular, there are infinitely many such elliptic curves with a K-rational point of prime order p if and only if $p \leq 17$.

Corollary 7. *Let $p = 29$ or $p = 31$. If $J_1(p)(\mathbb{Q})[2] \to J_1(p)(\mathbb{F}_2)$ is injective, then there are no elliptic curves E/K with $[K:\mathbb{Q}] \leq d$ such that $E(K)$ contains a point of order p.*

Proof. By Prop. 5, $J_1(29)(\mathbb{Q})$ and $J_1(31)(\mathbb{Q})$ are both finite. Since $(2^{4/2}+1)^2 < 29$, Cor. 4 applies. By Thm. 6, there are at most finitely many elliptic curves over a number field K of degree ≤ 4 that have a K-rational point of order > 17. Corollary 4 therefore shows that there are in fact no such curves with a K-rational point of order p. □

We can use this to deal with $p = 31$.

Theorem 8. *There is no elliptic curve E/K with $[K : \mathbb{Q}] \leq 4$ such that $E(K)$ contains a point of order 31.*

Proof. From [2], we know that the 2-part of $J_1(31)(\mathbb{Q})$ has order 4. We construct $X_1(31)$ and the intermediate curve $X_3(31)$ explicitly over $\mathbb{F}_2$ (they are cut out by quadratic relations between the corresponding cusp forms). We find the $\mathbb{F}_2$-rational cusps on $X_1(31)$ and their image on $X_3(31)$. We then check that their differences generate a subgroup of $J_3(31)(\mathbb{F}_2)$ of order a multiple of 4. This shows that the composition

$$J_1(31)(\mathbb{Q})[2] \longrightarrow J_1(31)(\mathbb{F}_2) \longrightarrow J_3(31)(\mathbb{F}_2)$$

is injective, whence the first map is also injective. The claim then follows from Cor. 7. The computations were done using MAGMA [1]. □

We have not been able to show that $J_1(29)(\mathbb{Q})[2]$ injects into $J_1(29)(\mathbb{F}_2)$. However, we can show the following.

Proposition 9. *If differences of the rational cusps on $X_1(29)$ generate $J_1(29)(\mathbb{Q})$, then $29 \notin S(4)$.*

Proof. Again using MAGMA, we construct $X_1(29)$ and its quotient $X_7(29)$ over $\mathbb{F}_3$. We check that the images of the points of degrees 3 and 4 on $X_1(29)/\mathbb{F}_3$ (for degree ≤ 2, there are only the cusps) on $X_7(29)$ do not map into the subgroup generated by the images of the cusps in $J_7(29)(\mathbb{F}_3)$. This establishes assumption 5 of Thm. 3, if the condition in the statement of the proposition is satisfied. The other assumptions also hold, so Thm. 3 together with Thm. 6 implies the claim. □

Theorem 10. *There is no elliptic curve E/K with $[K : \mathbb{Q}] \leq 4$ such that $E(K)$ contains a point of order 19 or 23.*

Proof. By Prop. 5, $J_1(19)(\mathbb{Q})$ and $J_1(23)(\mathbb{Q})$ are both finite and of odd order. Taking $p = 19$ or 23, $d = 4$, $\ell = 2$ in Thm. 3, we see that the first four assumptions are satisfied. We need to check the last assumption. In fact, an exhaustive enumeration shows that there are no elliptic curves over $\mathbb{F}_{2^4}$ with a point of order 19 or 23, so the last assumption is trivially satisfied. (For smaller e, it follows from the Hasse bound, since $(2^{3/2} + 1)^2 < 19$.) Invoking Thm. 6 again, we see that Thm. 3 shows that 19 and 23 are both not contained in $S(4)$. □

Remark 11. If $E/\mathbb{F}_{2^e}$ is an elliptic curve with $e \leq 4$ and a point of order $p = 19$ or 23, then the Hasse bound forces $e = 4$ and $\#E(\mathbb{F}_{2^4}) = p$. So the number of points must be odd. This implies that E is supersingular, so E is a twist of an elliptic curve defined over $\mathbb{F}_{2^2}$. All those curves (they are the curves with $j = 0$) have $\#E(\mathbb{F}_{2^4}) \equiv 1 \bmod 4$. Does this follow from some theoretical result? If so, we can eliminate the computational part from the proof (other than that going into Prop. 5 and Thm. 6, of course.)

References

[1] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265.
(Also see the Magma home page at `http://www.maths.usyd.edu.au:8000/u/magma/` .)

[2] B. Conrad, B. Edixhoven, and W.A. Stein, $J_1(p)$ *has connected fibers*, Documenta Math. **8** (2003), 331–408.

[3] D. Jeon, C.H. Kim and E. Park. *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. **74** (2006), 1–12. doi:10.1112/S0024610706022940

[4] S. Kamienny and W.A. Stein, *Torsion points on elliptic curves over quartic number fields*, Draft manuscript (2010).

University of Southern California, 3620 South Vermont Ave., KAP 108, Los Angeles, California 90089-2532, USA

E-mail address: `kamienny@usc.edu`

University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195-4350, USA.

E-mail address: `wstein@gmail.com`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: `Michael.Stoll@uni-bayreuth.de`