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 $d \ge 1$, we let S(d) be the set of primes p such there exists an elliptic curve E over a number field K of degree $\le d$ 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 9 below shows that $29 \notin S(4)$.

Should be extended and proper references added.

Date: May 11, 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 *d*th symmetric power of *C*.

Proposition 2. Let C/\mathbb{Q} be a curve with Jacobian J, let $d \ge 1$ 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 $P \in C(\overline{\mathbb{F}}_{\ell}) \setminus C(\mathbb{F}_{\ell})$ is a point of degree $d' \leq d$, then $\operatorname{Tr}_{\mathbb{F}_{\ell}d'}/\mathbb{F}_{\ell} \iota(P) \in J(\mathbb{F}_{\ell})$ 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

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 $C^{(d)}(\mathbb{F}_{\ell})_{\text{split}}$ of $C(\mathbb{F}_{\ell})^d$ in $C^{(d)}(\mathbb{F}_{\ell})$. We now consider the diagram

$$\begin{array}{c|c} C(\mathbb{Q})^d & \longrightarrow C^{(d)}(\mathbb{Q}) \\ \rho_{C^d} & & & & & \\ \rho_{C^{(d)}} & & & & \\ C(\mathbb{F}_{\ell})^d & \longrightarrow C^{(d)}(\mathbb{F}_{\ell})_{\text{split}}. \end{array}$$

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 $C(\mathbb{Q})^d$. \Box 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 $\tilde{\ell}$ in $\mathbb{F}_p^{\times}/\{\pm 1\}$ is > d.
- (4) $p > (\sqrt{\ell} + 1)^2$.
- (5) If E/\mathbb{F}_{ℓ^e} is an elliptic curve that has an \mathbb{F}_{ℓ^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}_{ℓ^e} -rational points except for the \mathbb{F}_{ℓ} -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 $n \ge 1$, 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. $\hfill \Box$

Corollary 4. Let p be a prime and $d \ge 1$ 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 $\ell^d , which is a consequence of assumption 2 in the corollary. Finally, assumption 5 again follows from the second assumption in the corollary, since by the Hasse bound, any elliptic curve <math>E/\mathbb{F}_{\ell^e}$ 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 .

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

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 $p \notin S(4)$.

4

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.

$$31 \notin S(4).$$

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]. \Box

We have not been able to show that $J_1(29)(\mathbb{Q})[2]$ injects into $J_1(29)(\mathbb{F}_2)$. However, with a bit more computational work, we can still obtain the desired result.

Theorem 9.

 $29 \notin S(4).$

Proof. We apply Thm. 3 with $\ell = 11$. Let $X = X_1(29)$, and let Y be its genus 8 quotient by the action of the diamond operator $\langle 12 \rangle$ (note that $12^2 \equiv -1 \mod 29$, so we have a double cover). Since $(\sqrt{11} + 1)^2 < 29$, the only \mathbb{F}_{11} -points on X are the images of the rational cusps (11 generates \mathbb{F}_{29}^{\times} , so the other cusps don't split). We find all points on X/\mathbb{F}_{11} of degree 2, 3 and 4. We map them down to Y. Taking the image of the infinite cusp as base-point, we embed Y ito its Jacobian J. It is known [2] that the subgroup generated by the differences of rational cusps on X/\mathbb{Q} has index at most 8 in the Mordell-Weil group of $J_1(29)$. We find that

$$J(\mathbb{F}_{11}) \cong (\mathbb{Z}/2\mathbb{Z})^5 \times \mathbb{Z}/2 \cdot 7 \cdot 17 \cdot 43 \cdot 1933 \mathbb{Z}$$

so that the image of Mordell-Weil is included in the subgroup G obtained as the cuspidal subgroup plus the 2-torsion subgroup. This subgroup G has index $17 \cdot 1933 = 32861$ in $J(\mathbb{F}_{11})$, so there is a good chance that our points will miss it. Indeed, taking the image of each prime divisor on $X_1(29)/\mathbb{F}_{11}$ of degree $2 \leq d \leq 4$ and subtracting d times the base-point, we can check that the class of the resulting divisor in $J(\mathbb{F}_{11})$ is not contained in G. This implies that the corresponding points on $X_1(29)/\mathbb{F}_{11}$ have the property that the trace of the image in $J_1(29)$ is not in the image of the Mordell-Weil group. Therefore, assumption 5 in Thm. 3 is satisfied. The first asumption holds by Prop. 5, and the remaining ones are clearly satisfied. Using Thm. 6, we obtain the result.

The computations were done with MAGMA again.

Theorem 10. S(4) does not contain 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 $\#E(\mathbb{F}_{2^4}) \equiv 1 \mod 4$. 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

- 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, J₁(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