

# TORSION GROUPS OF ELLIPTIC CURVES OVER THE $\mathbb{Z}_p$ -EXTENSIONS OF $\mathbb{Q}$

MICHAEL CHOU, HARRIS B. DANIELS, IVAN KRIJAN, AND FILIP NAJMAN

ABSTRACT. We determine, for an elliptic curve  $E/\mathbb{Q}$  and for all  $p$ , all the possible torsion groups  $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$ , where  $\mathbb{Q}_{\infty,p}$  is the  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ .

## 1. INTRODUCTION

For a prime number  $p$ , denote by  $\mathbb{Q}_{\infty,p}$  the unique  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ , and for a positive integer  $n$ , denote by  $\mathbb{Q}_{n,p}$  the  $n^{\text{th}}$  layer of  $\mathbb{Q}_{\infty,p}$ , i.e. the unique subfield of  $\mathbb{Q}_{\infty,p}$  such that  $\text{Gal}(\mathbb{Q}_{n,p}/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$ . Recall that the  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$  is the unique Galois extension  $\mathbb{Q}_{\infty,p}$  of  $\mathbb{Q}$  such that

$$\text{Gal}(\mathbb{Q}_{\infty,p}/\mathbb{Q}) \simeq \mathbb{Z}_p,$$

where  $\mathbb{Z}_p$  is additive group of  $p$ -adic integers and is constructed as follows. Let

$$G = \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n \text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Here we know that  $G = \Delta \times \Gamma$ , where  $\Gamma \simeq \mathbb{Z}_p$  and  $\Delta \simeq \mathbb{Z}/(p-1)\mathbb{Z}$  for  $p \geq 3$  and  $\Delta \simeq \mathbb{Z}/2\mathbb{Z}$  (generated by complex conjugation) for  $p = 2$ , so we define

$$\mathbb{Q}_{\infty,p} := \mathbb{Q}(\zeta_{p^\infty})^\Delta.$$

We also see that every layer is uniquely determined by

$$\mathbb{Q}_{n,p} = \mathbb{Q}(\zeta_{p^{n+1}})^\Delta,$$

so for  $p \geq 3$  it is the unique subfield of  $\mathbb{Q}(\zeta_{p^{n+1}})$  of degree  $p^n$  over  $\mathbb{Q}$ . More details and proofs of these facts about  $\mathbb{Z}_p$ -extensions and Iwasawa theory can be found in [24, Chapter 13].

Iwasawa theory for elliptic curves (see [9]) studies elliptic curves in  $\mathbb{Z}_p$ -extensions, in particular the growth of the rank and  $n$ -Selmer groups in the layers of the  $\mathbb{Z}_p$ -extensions.

In this paper we completely solve the problem of determining how the torsion of an elliptic curve defined over  $\mathbb{Q}$  grows in the  $\mathbb{Z}_p$ -extensions of  $\mathbb{Q}$ . These results, interesting in their own right, might also find applications in other problems in Iwasawa theory for elliptic curves and in general. For example, to show that elliptic curves over  $\mathbb{Q}_{\infty,p}$  are modular for all  $p$ , Thorne [23] needed to show that  $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$  for two particular elliptic curves.

Our results are the following.

---

*Date:* August 17, 2018.

*2010 Mathematics Subject Classification.* 11G05.

*Key words and phrases.* Elliptic curves, torsion.

The third and fourth author were supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

**Theorem 1.1.** *Let  $p \geq 5$  be a prime number, and  $E/\mathbb{Q}$  an elliptic curve. Then*

$$E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}.$$

**Theorem 1.2.** *Let  $E/\mathbb{Q}$  be an elliptic curve.  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  is exactly one of the following groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, & \quad 1 \leq N \leq 10, \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \quad 1 \leq N \leq 4, \end{aligned}$$

*and for each group  $G$  from the list above there exists an  $E/\mathbb{Q}$  such that  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$ .*

**Theorem 1.3.** *Let  $E/\mathbb{Q}$  be an elliptic curve.  $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$  is exactly one of the following groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, & \quad 1 \leq N \leq 10, \text{ or } N = 12, 21 \text{ or } 27, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \quad 1 \leq N \leq 4. \end{aligned}$$

*and for each group  $G$  from the list above there exists an  $E/\mathbb{Q}$  such that  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq G$ .*

*Remark.* By Mazur's theorem [18] we see that

$$\begin{aligned} \{E(\mathbb{Q}_{\infty,2})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\}, \\ \{E(\mathbb{Q}_{\infty,3})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} \cup \{\mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}. \end{aligned}$$

However, given a specific  $E/\mathbb{Q}$  it is not necessarily the case that  $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ . Indeed there are many elliptic curves for which torsion grows from  $\mathbb{Q}$  to  $\mathbb{Q}_{\infty,p}$ , and we investigate this question further in Section 6. Specifically, for each prime  $p$  we prove which groups  $G$  have infinitely many  $j$ -invariants of elliptic curves satisfying  $E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} \simeq G$ .

## 2. NOTATION AND AUXILIARY RESULTS

We will use the following notation throughout the paper:

- For a positive integer  $n$ ,  $\rho_{E,n}$  is the mod  $n$  Galois representation attached to elliptic curve  $E$ ; we will write just  $\rho_n$  when it is obvious what  $E$  is.
- For a number field  $K$ , we denote  $G_K := \text{Gal}(\overline{K}/K)$ .
- By  $G_{E,K}(n)$  (or just  $G_E(n)$ ) we will denote the image (after a choice of basis of  $E[n]$ ) of  $\rho_{E,n}(G_K)$  in  $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$  i.e.

$$G_{E,K}(n) = \{\rho_{E,n}(\sigma) : \sigma \in \text{Gal}(\overline{K}/K)\}.$$

- For a prime number  $\ell$ ,  $\overline{\rho}_{\ell,E}$  is the  $\ell$ -adic Galois representation and  $T_{\ell}(E)$  is  $\ell$ -adic Tate module attached to  $E$ .
- We say that an elliptic curve  $E$  has or admits an  $n$ -isogeny over  $K$  if there exists an isogeny  $f : E \rightarrow E'$  for some elliptic curve  $E'$  of degree  $n$  with cyclic kernel and such that  $E$ ,  $E'$  and  $f$  are all defined over  $K$ , or equivalently if  $G_K$  acts on  $\ker f$ .

To make this paper as self-contained as reasonably possible, we now list the most important known results that we will use.

**Proposition 2.1.** [22, Ch. III, Cor. 8.1.1] *Let  $E/L$  be an elliptic curve with  $L \subseteq \overline{\mathbb{Q}}$ . For each integer  $n \geq 1$ , if  $E[n] \subseteq E(L)$  then the  $n^{\text{th}}$  cyclotomic field  $\mathbb{Q}(\zeta_n)$  is a subfield of  $L$ .*

An immediate consequence of this proposition is

**Corollary 2.2.** *Let  $p$  and  $q$  be odd prime numbers. Then*

$$E(\mathbb{Q}_{\infty,p})[q] \simeq \{O\} \quad \text{or} \quad \mathbb{Z}/q\mathbb{Z}.$$

*Remark.* We have that  $E[q^n] \not\subseteq E(\mathbb{Q}_{\infty,p})$ , for each positive integer  $n$ .

*Proof.* Since  $-1$  and  $1$  are the only roots of unity contained in  $\mathbb{Q}_{\infty,p}$ , by Proposition 2.1  $E[q]$  cannot be contained in  $E(\mathbb{Q}_{\infty,p})$ . The result follows from Proposition 2.1.  $\square$

**Lemma 2.3.** [4, Lemma 4.6] *Let  $E$  be an elliptic curve over a number field  $K$ , let  $F$  be a Galois extension of  $\mathbb{Q}$ , let  $p$  be a prime, and let  $k$  be the largest integer for which  $E[p^k] \subseteq E(F)$ . If  $E(F)_{\text{tors}}$  contains a subgroup isomorphic to  $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$  with  $j \geq k$ , then  $E$  admits a  $K$ -rational  $p^{j-k}$ -isogeny.*

**Theorem 2.4.** [18, 13, 14, 15, 16] *Let  $E/\mathbb{Q}$  be an elliptic curve with a rational  $n$ -isogeny. Then*

$$n \leq 19 \quad \text{or} \quad n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

**Corollary 2.5.** *Let  $p$  be an odd prime number,  $E/\mathbb{Q}$  elliptic curve and  $P \in E(\mathbb{Q}_{\infty,p})_{\text{tors}}$  a point of order  $q^n$  for some prime  $q$  and positive integer  $n$ , then*

$$q^n \in \{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 25, 27, 32, 37, 43, 67, 163\}.$$

*Proof.* For  $q \geq 3$  we have  $E[q] \not\subseteq E(\mathbb{Q}_{\infty,p})$  by Corollary 2.2, so by Lemma 2.3 we conclude that  $E$  admits a rational  $q^n$ -isogeny.

For  $q = 2$  by Lemma 2.3, so  $E$  admits a rational  $2^{n-1}$ -isogeny.

The result now follows from Theorem 2.4.  $\square$

**Theorem 2.6.** [7, Theorem 5.7] *Let  $E/\mathbb{Q}$  be an elliptic curve,  $p$  a prime and  $P$  a point of order  $p$  in  $E$ . Then all of the cases in the table below occur for  $p \leq 13$  or  $p = 37$ , and they are the only ones possible.*

$p$	$[\mathbb{Q}(P) : \mathbb{Q}]$
2	1, 2, 3
3	1, 2, 3, 4, 6, 8
5	1, 2, 4, 5, 8, 10, 16, 20, 24
7	1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24, 36, 42, 48
11	5, 10, 20, 40, 55, 80, 100, 110, 120
13	3, 4, 6, 12, 24, 39, 48, 52, 72, 78, 96, 144, 156, 168
37	12, 36, 72, 444, 1296, 1332, 1368

For all other  $p$ , we have  $[\mathbb{Q}(P) : \mathbb{Q}]$  the following cases do occur:

- (1)  $p^2 - 1$ , for all  $p$ ,
- (2) 8, 16, 32, 136, 256, 272, 288, for  $p = 17$ ,
- (3)  $\frac{p-1}{2}$ ,  $p-1$ ,  $\frac{p(p-1)}{2}$ ,  $p(p-1)$ , if  $p \in \{19, 43, 67, 163\}$ ,

- (4)  $2(p-1), (p-1)^2$ , if  $p \equiv 1 \pmod{3}$  or  $\left(\frac{-D}{p}\right) = 1$ ,  
for some  $D \in \{1, 2, 7, 11, 19, 43, 67, 163\}$ ,
- (5)  $\frac{(p-1)^2}{3}, \frac{2(p-1)^2}{3}$ , if  $p \equiv 4, 7 \pmod{9}$ ,
- (6)  $\frac{p^2-1}{3}, \frac{2(p^2-1)}{3}$ , if  $p \equiv 2, 5 \pmod{9}$ ,

Apart from the cases above that have been proven to appear, the only other options that might be possible are:

$$\frac{p^2-1}{3}, \frac{2(p^2-1)}{3}, \quad \text{for } p \equiv 8 \pmod{9}.$$

**Theorem 2.7.** [7, Theorem 7.2.] *Let  $p$  be the smallest prime divisor of positive integer  $d$  and let  $K/\mathbb{Q}$  be a number field of degree  $d$ .*

- If  $p \geq 11$ , then  $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ .
- If  $p = 7$ , then  $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$ , for all primes  $q \neq 7$ .
- If  $p = 5$ , then  $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$ , for all primes  $q \neq 5, 7, 11$ .
- If  $p = 3$ , then  $E(K)[q^\infty] = E(\mathbb{Q})[q^\infty]$ , for all primes  $q \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$ .

We now prove a lemma that we will find useful.

**Lemma 2.8.** *Let  $p$  and  $q$  be prime numbers such that  $q-1 \nmid p$  and  $p \nmid q-1$ . Let  $K/\mathbb{Q}$  be a cyclic extension of degree  $p$ , and  $P \in E$  a point of degree  $q$ . If  $P \in E(K)$ , then  $P \in E(\mathbb{Q})$ .*

*Proof.* If we assume that  $\mathbb{Q}(\zeta_q) \subseteq K$ , it follows that  $q-1 = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] \mid [K : \mathbb{Q}] = p$ , and that is impossible by the assumption that  $q-1 \nmid p$ . Therefore, by Corollary 2.2 we conclude that  $E(K)[q] \simeq \mathbb{Z}/q\mathbb{Z}$ .

Let us assume that there is  $\sigma \in \text{Gal}(K/\mathbb{Q})$  such that  $P^\sigma \neq P$  (i.e. that  $P \notin E(\mathbb{Q})$ ). That means that there is some  $a \in \{2, 3, \dots, q-1\}$  such that  $P^\sigma = aP$ . Furthermore, we know that  $\sigma^p = 1$ , so

$$P = P^{\sigma^p} = a^p P,$$

which means that  $a^p \equiv 1 \pmod{q}$ , but there exist such an  $a \in \{2, 3, \dots, q-1\}$  if and only if  $p \mid q-1$  or  $q-1 \mid p$ , which is a contradiction.  $\square$

The following lemma will tell us how far up the tower we have to go to find a point of order  $n$ , if such a point exists.

**Lemma 2.9.** *Let  $E/\mathbb{Q}$  be an elliptic curve and  $P \in E$  a point of order  $n$  such that  $\mathbb{Q}(P)/\mathbb{Q}$  is Galois and let  $H := E(\mathbb{Q}(P))[n]$ . Then  $\text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$  is isomorphic to a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$ .*

*Proof.* We see that  $G_{\mathbb{Q}}$  acts on  $P$  through  $G := \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$  so that for any  $\sigma \in G_{\mathbb{Q}}$  we have  $P^\sigma = aP$ , for some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ , since  $|P^\sigma| = |P|$ . Since  $G$  acts faithfully on  $\langle P \rangle$ , this implies that  $G$  is isomorphic to a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$ .  $\square$

We immediately obtain the following corollary.

**Corollary 2.10.** *Let  $P \in E$  a point of order  $n$  such that  $\mathbb{Q}(P) \subseteq \mathbb{Q}_{\infty, p}$ . Then  $\mathbb{Q}(P) \subseteq \mathbb{Q}_{n, p}$ , where  $n = v_p(\phi(n))$ .*

**Proposition 2.11.** *Let  $E/F$  be an elliptic curve over a number field  $F$ ,  $n$  a positive integer,  $P \in E$  be a point of order  $p^{n+1}$  such that  $E(F(pP))$  has no points of order  $p^{n+1}$  and such that  $F(P)/F(pP)$  is Galois. Then  $[F(P) : F(pP)]$  divides  $p^2$ .*

*Proof.* Let  $Q := pP$ , and consider the equation

$$(1) \quad pX = Q.$$

So what we're looking for are all the possibilities for  $[K(P) : K(Q)]$  where  $P$  is some solution of (1). This degree is the same as the length of the orbit of  $P$  under the action of  $G := \text{Gal}(F(P)/F(pP))$  on the solutions of (1). The  $p^2$  solutions should decompose of (1) into orbits with the restriction that if  $P$  is defined over a certian field, then so are all multiples of  $P$  - so  $P$  and all the multiples of  $P$  should be in orbits of the same length. If  $P$  comes in an orbit of length  $n$ , and there are  $x$  orbits of length  $n$  such that all the elements inside are defined over  $F(P)$  (and since  $F(P)/F(pP)$  is Galois, if one element inside an orbit is defined over  $F(P)$ , then all of them are), then we have  $n \cdot x = p$  or  $p^2$  (as the number of solutions (1) is in bijection with  $E(F(P))[p]$ ). Hence  $n$  will have to be either  $p$  or  $p^2$ , proving the proposition.  $\square$

*Remark.* Proposition 2.11 is a version of [7, Proposition 4.6.] with stronger assumptions.

### 3. PROOF OF THEOREM 1.1

For primes  $p \geq 11$ , by Theorem 2.7 we know that  $E(\mathbb{Q}_{n,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ , for each positive integer  $n$ . It follows that  $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ . It remains to prove this fact for cases  $p = 7$  and  $p = 5$ .

**Theorem 3.1.**  $E(\mathbb{Q}_{\infty,7})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ .

*Proof.* From Theorem 2.7, we immediately conclude that  $E(\mathbb{Q}_{\infty,7})[q^\infty] = E(\mathbb{Q})[q^\infty]$  for all primes  $q \neq 7$ . It remains to prove that  $E(\mathbb{Q}_{\infty,7})[7^\infty] = E(\mathbb{Q})[7^\infty]$ .

By Corollary 2.5 we conclude that there is no 49-torsion in  $E(\mathbb{Q}_{\infty,7})$ , so it remains to prove that  $E(\mathbb{Q}_{\infty,7})[7] = E(\mathbb{Q})[7]$ .

Let  $P \in E(\mathbb{Q}_{\infty,7})$  be a point of order 7. By Theorem 2.6,  $P$  is defined over some field of degree at most  $7^2 - 1$ . Therefore,  $P \in E(\mathbb{Q}_{1,7})$ . From Lemma 2.8 it now follows that  $P \in E(\mathbb{Q})$  and we are done.  $\square$

**Lemma 3.2.**  $E(\mathbb{Q}_{\infty,5})[11^\infty] = \{O\}$ .

*Proof.* Again by Corollary 2.5 we conclude that there is no 121-torsion in  $E(\mathbb{Q}_{\infty,5})$ . It remains to prove that  $E(\mathbb{Q}_{\infty,5})[11] = \{O\}$ .

Let  $P \in E(\mathbb{Q}_{\infty,5})$  be a point of order 11. From Theorem 2.6 we conclude that  $P \in E(\mathbb{Q}_{1,5})$ . The modular curve  $X_1(11)$  is the elliptic curve

$$y^2 + y = x^3 - x^2.$$

We can easily compute (using Magma [1]) that  $X_1(11)$  has rank 0 and torsion  $\mathbb{Z}/5\mathbb{Z}$  over  $\mathbb{Q}_{1,5}$ , and all the torsion points are cusps, so there are no elliptic curves with 11-torsion over  $\mathbb{Q}_{1,5}$ .  $\square$

Before proving  $E(\mathbb{Q}_{\infty,5})[5^\infty] = E(\mathbb{Q})[5^\infty]$  we will need some technical results.

**Theorem 3.3.** [8, Theorem 2] *The index  $[\text{Aut}_{\mathbb{Z}_5}(T_5(E)) : \text{im}(\bar{\rho}_{5,E})]$  isn't divisible by 25.*

**Lemma 3.4.** *Let  $n$  be a positive integer and  $\zeta$  an  $n^{\text{th}}$  root of unity. Then for every  $\sigma \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$  we have*

$$\sigma(\zeta) = \zeta^{\det \rho_n(\sigma)}.$$

*Proof.* Let  $\{P, Q\}$  be a basis for  $E[n]$  and  $e_n(P, Q) = \zeta_n$ , where  $\zeta_n$  is a  $n^{\text{th}}$  primitive root of unity. For any  $n^{\text{th}}$  root of unity  $\zeta$ , there exists an  $m \in \mathbb{Z}$  such that  $\zeta = \zeta_n^m$ . So, it suffices to show that  $\sigma(\zeta_n) = \zeta_n^{\det \rho_n(\sigma)}$ .

Then there are some  $a, b, c, d \in (\mathbb{Z}/n\mathbb{Z})^\times$  such that

$$P^\sigma = aP + bQ \quad \text{and} \quad Q^\sigma = cP + dQ.$$

Using properties of Weil pairing [22, Ch. III, §8.] we calculate:

$$\begin{aligned} \sigma(\zeta_n) &= \sigma(e_n(P, Q)) = e_n(P^\sigma, Q^\sigma) = e_n(aP + bQ, cP + dQ) \\ &= e_n(P, P)^{ac} e_n(P, Q)^{ad} e_n(Q, P)^{bc} e_n(Q, Q)^{bd} \\ &= 1 \cdot \zeta_n^{ad} \cdot \zeta_n^{-bc} \cdot 1^{bd} = \zeta_n^{\det \rho_n(\sigma)}. \end{aligned} \quad \square$$

**Proposition 3.5.** *Let  $n$  be a positive integer and  $\zeta_n$  an  $n^{\text{th}}$  primitive root of unity. Let  $K$  be a number field, then*

$$\det \rho_{E,n}(G_K) \simeq \text{Gal}(\mathbb{Q}(\zeta_n)/K \cap \mathbb{Q}(\zeta_n)).$$

*Proof.* Let

$$f: G_K \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \quad \sigma \mapsto g \circ \det \circ \rho_{E,n}(\sigma),$$

where  $g$  is the canonical isomorphism mapping  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  by sending  $a$  to  $\sigma_a$ , where  $\sigma_a(\zeta_n) = \zeta_n^a$ .

As  $\det \rho_{E,n}(G_K) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ , it follows that  $f(G_K) \leq \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  and hence, by Galois theory,  $f(G_K) = \text{Gal}(\mathbb{Q}(\zeta_n)/K')$  for some subfield  $K'$  of  $\mathbb{Q}(\zeta_n)$ . From Proposition 3.4 it follows that  $f$  is the restriction map sending  $\sigma \in G_K$  to  $\sigma|_{\mathbb{Q}(\zeta_n)} = \sigma_{\det \rho_n(\sigma)}$ .

It follows that  $f(G_K)$  comprises exactly those  $\sigma_a$  that leave  $K \cap \mathbb{Q}(\zeta_n)$  fixed, proving  $K' = K \cap \mathbb{Q}(\zeta_n)$  and the proposition.  $\square$

**Lemma 3.6.**  $E(\mathbb{Q}_{\infty,5})[5^\infty] = E(\mathbb{Q})[5^\infty]$ .

*Proof.* There is no 125-torsion in  $E(\mathbb{Q}_{\infty,5})$  by Corollary 2.5. If  $P \in E(\mathbb{Q}_{\infty,5})$  is a point of order 5, then  $P$  is defined over  $\mathbb{Q}_{1,5}$  by Theorem 2.6, but then by Lemma 2.8 it follows that  $P \in E(\mathbb{Q})$ , so it remains to prove that  $E(\mathbb{Q}_{\infty,5})[25] = E(\mathbb{Q})[25]$ .

Let us assume that there is a point  $P \in E(\mathbb{Q}_{\infty,5})_{\text{tors}}$  of order 25; obviously  $P \notin E(\mathbb{Q})$ . By the previous argumentation, the order 5 point  $5P$  must be defined over  $\mathbb{Q}$ . Therefore,  $P \in E(\mathbb{Q}_{1,5})$ , the extension  $\mathbb{Q}_{1,5}/\mathbb{Q}$  is cyclic, so for every  $\sigma \in G_{\mathbb{Q}}$  there exist some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  such that  $P^\sigma = aP$ . Since  $5P \in E(\mathbb{Q})$ , we have  $(5P)^\sigma = 5P$ , so  $a \equiv 1 \pmod{5}$ . Hence,  $G_{\mathbb{Q}}(25)$  is of the form

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z} \right\}.$$

Furthermore,  $\det G_{\mathbb{Q}_{1,5},E}(25)$  is by Proposition 3.5, the unique subgroup of  $(\mathbb{Z}/25\mathbb{Z})^\times$  of order 4:  $\{7, -1, -7, 1\}$ . The group  $G_{\mathbb{Q}_{1,5}}$  fixes the point  $P$  so we conclude that  $G_{\mathbb{Q}_{1,5},E}(25)$  is of the form

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & b \end{pmatrix} : b \in \{7, -1, -7, 1\} \right\}.$$

Since  $G_{\mathbb{Q}_{1,5},E}(25)$  is a subgroup of  $G_{\mathbb{Q}}(25)$  of index 5, and  $P \notin E(\mathbb{Q})$ , so it follows that

$$G_{\mathbb{Q}}(25) = \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in 1 + 5\mathbb{Z}/25\mathbb{Z}, b \in \{7, -1, -7, 1\} \right\}.$$

Finally, we calculate that  $600 = [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_E(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{im}(\bar{\rho}_{5,E})]$ , a contradiction with Theorem 3.3.  $\square$

**Theorem 3.7.**  $E(\mathbb{Q}_{\infty,5})_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ .

*Proof.* From Theorem 2.7, we immediately conclude that  $E(\mathbb{Q}_{\infty,5})[q^\infty] = E(\mathbb{Q})[q^\infty]$  for all primes  $q \neq 5, 7, 11$ .

There is no 49-torsion in  $E(\mathbb{Q}_{\infty,5})$  by Corollary 2.5, so it remains to prove that  $E(\mathbb{Q}_{\infty,5})[7] = E(\mathbb{Q})[7]$ . Let  $P \in E(\mathbb{Q}_{\infty,5})$  be a point of degree 7 such that  $P \notin E(\mathbb{Q})$ . By Theorem 2.6 we conclude that  $\gcd(5, [\mathbb{Q}(P) : \mathbb{Q}]) = 1$ , which is a contradiction.

Cases  $q = 11$  and  $q = 5$  follow from Lemmas 3.2 and 3.6.  $\square$

#### 4. PROOF OF THEOREM 1.2

Using Theorem 2.6, Corollary 2.5 and the following facts:

- $p^2 - 1 = (p - 1)(p + 1)$  isn't a power of 2 for primes  $p > 3$ . This follows from the fact that  $\gcd(p - 1, p + 1) = 2$ ,
- $p - 1$  isn't a power of 2 for  $p \in \{19, 43, 67, 163\}$ ,
- $p - 1$  is power of two if and only if a prime  $p$  is of the form  $2^{2^k} + 1$ ,
- $3 \mid \frac{(p - 1)^2}{3}$  for  $p \equiv 4, 7 \pmod{9}$ ,
- $\frac{p^2 - 1}{3}$  isn't a power of 2 for  $p \equiv 2, 5 \pmod{9}$ . This follows from the fact that  $p$  is of the form  $3k - 1$  for some integer  $k \geq 6$ , and that means that  $\frac{p^2 - 1}{3} = (3k - 2) \cdot k$ , but  $\gcd(3k - 2, k) \leq 2$ ,
- $3 \mid \frac{p^2 - 1}{3}$  for  $p \equiv 8 \pmod{9}$ ,

we can conclude that  $E(\mathbb{Q}_{\infty,2})[q] = E(\mathbb{Q})[q]$  for all primes  $q \neq 2, 3, 5, 7, 13, 17$ .

**Lemma 4.1.**  $E(\mathbb{Q}_{\infty,2})$  does not contain a subgroup isomorphic to  $\mathbb{Z}/13\mathbb{Z}$ .

*Proof.* Suppose that there exists such a curve, then a point  $P \in E$  is defined over the quartic field  $\mathbb{Q}_{2,2} = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$  by Theorem 2.6. But then either  $E$  or a twist of  $E$  would have  $\mathbb{Z}/13\mathbb{Z}$  torsion over  $\mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$ , which is not possible by [12, Theorem 3].  $\square$

**Lemma 4.2.**  $E(\mathbb{Q}_{\infty,2})$  does not contain  $\mathbb{Z}/17\mathbb{Z}$ .

*Proof.* By Corollary 2.10 and Theorem 2.6, a point of order 17 can be defined over a number field of degree 8 or 16. Such a curve  $E/\mathbb{Q}$  has a 17-isogeny over  $\mathbb{Q}$ , so  $j(E) = -(17^2 \cdot 101^3)/2$  or  $j(E) = -(17 \cdot 373^3)/2^{17}$ . We factor the 17th division polynomials of an elliptic curve with each of these invariants (the choice of the exact quadratic twist we choose with each  $j$ -invariant will be irrelevant) over  $\mathbb{Q}_{3,2}$ , and obtain that in one case the smallest degree of an irreducible factor is 4, while in the other case the smallest degree of an irreducible factor is 8.  $\square$

So we have  $E(\mathbb{Q}_{\infty,2})[q^\infty] = E(\mathbb{Q})[q^\infty]$  for all primes  $q \neq 2, 3, 5, 7$ .

**Lemma 4.3.** *If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/7\mathbb{Z}$ , then  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$*

*Proof.* If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/7\mathbb{Z}$ , then  $E/\mathbb{Q}$  has by Corollary 2.10 the torsion point  $P$  of order 7 is defined over  $\mathbb{Q}_{1,2}$ . Hence either  $E(\mathbb{Q})$  or  $E^{(2)}(\mathbb{Q})$  has a point of order 7.

If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  contained a point of order 2, then both  $E(\mathbb{Q})$  and  $E^{(2)}(\mathbb{Q})$  would also have to contain a point of order 2, which would mean that one of these groups has a point of order 14, which is by Mazur's theorem impossible.

If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  contained a point of order 3, then by Corollary 2.10 it would have to be defined over  $\mathbb{Q}_{1,2}$ , which would mean that  $E(\mathbb{Q}_{1,2})$  has a point of order 21, which is impossible by [11, 17].

If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  contained a point of order 5, then  $E/\mathbb{Q}$  would be a 35-isogeny, contradicting Theorem 2.4.  $\square$

**Lemma 4.4.** *If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/5\mathbb{Z}$ , then  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}$  or  $\mathbb{Z}/10\mathbb{Z}$*

*Proof.* Suppose  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/5\mathbb{Z}$ . By Corollary 2.10, the point of order  $P$  on  $E$  has to be defined over  $\mathbb{Q}_{2,2}$ .

If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  had a point of order 15, then both a point of order 3 and of order 5 have to be defined over  $\mathbb{Q}_{2,2}$ , so the 15-torsion point must already be defined over  $\mathbb{Q}_{2,2}$ . But  $X_1(15)(\mathbb{Q}) = X_1(15)(\mathbb{Q}_{2,2})$ , so there are no elliptic curves with a point of order 15 over  $\mathbb{Q}_{2,2}$ .

Suppose now  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/10\mathbb{Z}$ . Then  $E(\mathbb{Q})$  has a point of order 2. Suppose

$$E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z},$$

then it would follow that  $E[2]$  is defined over  $\mathbb{Q}_{1,2}$  (as it has to be defined over some quadratic field if there is a point of order 2 over  $\mathbb{Q}$ ). Since  $E(\mathbb{Q}_{2,2})[5] \simeq \mathbb{Z}/5\mathbb{Z}$  and  $E(\mathbb{Q}_{2,2})[5] \simeq E(\mathbb{Q}_{1,2})[5] \oplus E^{(\delta)}(\mathbb{Q}_{1,2})[5]$ , for some quadratic twist (over  $\mathbb{Q}_{1,2}$ )  $E^{(\delta)}$  of  $E$ . So, since quadratic twisting does not change the 2-torsion, either  $E^{(\delta)}(\mathbb{Q}_{1,2}) \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$  or  $E(\mathbb{Q}_{1,2}) \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ . But we compute  $X_1(2,10)(\mathbb{Q}(\sqrt{2})) = X_1(2,10)\mathbb{Q}$ , so there are no elliptic curves over  $\mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$  with  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$  torsion.

Finally  $E(\mathbb{Q}_{\infty,2})[20]$  cannot be isomorphic to  $\mathbb{Z}/20\mathbb{Z}$  as then  $E$  would have a rational 20-isogeny, which is impossible by Theorem 2.4.  $\square$

**Lemma 4.5.** *If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/9\mathbb{Z}$ , then  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/9\mathbb{Z}$ .*

*Proof.* Suppose  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  contained a point of order 27. The point of order 9 would have to be defined over  $\mathbb{Q}_{1,2}$  by Corollary 2.10. There cannot be any 27-torsion over  $\mathbb{Q}_{1,2}$  [11, 17]. But then the point of order 9 cannot become divisible in a Galois extension of  $\mathbb{Q}_{1,2}$  of degree  $2^n$  by 2.11.



Suppose  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  contained a point of order 18. Then  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  would have to contain a 2-torsion point, and a point  $P$  of order 9 would have to be defined over  $\mathbb{Q}_{1,2}$  by Corollary 2.10. So  $E(\mathbb{Q}_{1,2})$  would contain a point of order 18. But there are no elliptic curves defined over  $\mathbb{Q}$  with a point of order 18 over a quadratic extension by [20, Theorem 2].  $\square$

**Lemma 4.6.** *If  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/12\mathbb{Z}$ , then  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/12\mathbb{Z}$ .*

*Proof.* By the previous Lemma,  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  cannot contain a point of order 9, so it remains to show that  $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$  does not have full 2-torsion and that it doesn't have a point of order 24. The fact that there are no points of order 24 follows from the fact that there are no points of order 24 over  $\mathbb{Q}^{ab}$  of which  $\mathbb{Q}_{\infty,2}$  is a subfield by [2, Theorem 1.2].

Suppose now that  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ , and let  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} = \langle P, Q \rangle$ , where  $P$  is of order 12 and  $Q$  is of order 2. We have  $2E(\mathbb{Q}_{\infty,2})_{\text{tors}} = \langle 2P \rangle \simeq \mathbb{Z}/6\mathbb{Z}$  is a  $G_{\mathbb{Q}}$ -invariant subgroup, and hence  $(6P)^{\sigma} = 6P$  for all  $\sigma \in G_{\mathbb{Q}}$ , i.e.  $6P$  is defined over  $\mathbb{Q}$ . By [7, Proposition 4.7],  $3P$  has to be defined over an extension of  $\mathbb{Q}$  which has Galois group  $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  or  $D_4$ . So we conclude that it has to be  $\mathbb{Z}/2\mathbb{Z}$  (since by assumption  $\mathbb{Q}(3P)$  is defined over  $\mathbb{Q}_{\infty,2}$ ). So the point  $3P$  of order 4 is defined over  $\mathbb{Q}_{1,2}$ .

The point  $4P$  is also defined over  $\mathbb{Q}_{1,2}$  by Corollary 2.10. Since  $6P$  is defined over  $\mathbb{Q}$ , then  $Q$  has to be defined over  $\mathbb{Q}_{1,2}$ .

So since  $4P, 3P$  and  $Q$  are all defined over  $\mathbb{Q}_{1,2}$ , we conclude that  $E(\mathbb{Q}_{1,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ , but this is impossible by [12, Theorem 10.].  $\square$

Finally, we have the following result that controls the 2-power torsion.

**Theorem 4.7.** [6, Theorem 1] *For an elliptic curve  $E/\mathbb{Q}$ ,  $E(\mathbb{Q}_{\infty,2})[2^{\infty}] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .*

These results combined prove Theorem 1.2.

## 5. PROOF OF THEOREM 1.3

Using theorem 2.6, Corollary 2.5 and the following facts:

- $p^2 - 1$  isn't a power of 3 for any odd prime  $p$  (it's divisible by 2),
- $p - 1$  isn't a power of 3 for any odd prime  $p$  (it's divisible by 2),

we can conclude that  $E(\mathbb{Q}_{\infty,3})[q] = E(\mathbb{Q})[q]$  for all primes  $q \neq 2, 3, 7, 13, 19$ .

**Lemma 5.1.**  $E(\mathbb{Q}_{\infty,3})[19] = \{O\}$ .

*Proof.* From Corollary 2.10 we deduce that a point of order 19 on  $E/\mathbb{Q}$  must be defined over  $\mathbb{Q}_{2,3}$ . Also  $E$  must have a rational 19-isogeny. There is only one family of quadratic twists (with  $j$ -invariant  $-2^{15} \cdot 3^3$ ), with complex multiplication by  $\mathbb{Z}[(1 + \sqrt{-19})/2]$ . We check that the 19<sup>th</sup> division polynomials of these elliptic curves with 19-isogeny don't have a root over the field  $\mathbb{Q}_{2,3}$ . It is enough to check this for one curve with  $j$ -invariant  $-2^{15} \cdot 3^3$ , as if the 19<sup>th</sup> division polynomial of this one curve with this  $j$ -invariant doesn't have a root over  $\mathbb{Q}_{2,3}$ , then neither does any quadratic twist of  $E$ . So  $E(\mathbb{Q}_{\infty,3})[19] = \{O\}$ .  $\square$

**Lemma 5.2.**  $E(\mathbb{Q}_{\infty,3})[13] = \{O\}$

*Proof.* From Corollary 2.10, a point of order 13 can be defined only over  $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$  (the maximal real subfield of  $\mathbb{Q}(\zeta_9)$ ). The modular curve  $X_1(13)$  is a curve of genus 2 with the

following model (as we can see in [12] for example):

$$y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

The rank of the Jacobian of this curve over  $\mathbb{Q}(\zeta_9)^+$  is 0, and the torsion is  $\mathbb{Z}/19\mathbb{Z}$ , and we easily check that  $X_1(13)(\mathbb{Q}_{1,3}) = X_1(13)(\mathbb{Q})$ , so there are no elliptic curves with 13-torsion over  $\mathbb{Q}_{1,3}$ . So  $E(\mathbb{Q}_{\infty,3})[13] = \{O\}$ .  $\square$

**Lemma 5.3.**  $E(\mathbb{Q}_{\infty,3})[5^\infty] = E(\mathbb{Q})[5^\infty]$ .

*Proof.* From Theorem 2.6, we see that if  $E(\mathbb{Q})[5] = \{O\}$ , then  $E(\mathbb{Q}_{\infty,3})[5] = \{O\}$ . If  $E(\mathbb{Q})[5] \neq \{O\}$ , then by Proposition 2.11, we see that  $E(\mathbb{Q})[5^\infty] = E(\mathbb{Q}_{\infty,3})[5^\infty]$ .  $\square$

**Lemma 5.4.** *If  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \supseteq \mathbb{Z}/7\mathbb{Z}$ , then  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$  or  $\mathbb{Z}/21\mathbb{Z}$*

*Proof.* By Proposition 2.11, the 7-power torsion can grow only if  $E(\mathbb{Q})[7] = \{O\}$ . We now determine, for an  $E/\mathbb{Q}$  such that  $E(\mathbb{Q})[7] = \{O\}$  and  $E(\mathbb{Q}_{\infty,3})[7] \neq \{O\}$ , what are the possible torsion groups of  $E(\mathbb{Q}_{\infty,3})$ . By Corollary 2.10 we conclude that a point of order 7 appears over  $\mathbb{Q}_{1,3}$ .

We first note that  $E(\mathbb{Q}_{\infty,3})[7^\infty] \simeq \mathbb{Z}/7\mathbb{Z}$ , as there cannot be any 49-torsion by Proposition 2.5. Also  $E(\mathbb{Q}_{\infty,3})$  obviously cannot contain a subgroup isomorphic to  $\mathbb{Z}/35\mathbb{Z}$  due to Theorem 2.4.

Suppose  $E(\mathbb{Q}_{\infty,3})$  contains  $\mathbb{Z}/14\mathbb{Z}$ . Then  $E(\mathbb{Q})$  has a point of order 2, and so  $E(\mathbb{Q}_{1,3})$  contains a subgroup isomorphic to  $\mathbb{Z}/14\mathbb{Z}$ . But we compute that  $X_1(14)(\mathbb{Q}_{1,3}) = X_1(14)(\mathbb{Q})$ , which shows that this is impossible.

Suppose  $E(\mathbb{Q}_{\infty,3})$  contains  $\mathbb{Z}/21\mathbb{Z}$ . First note that then  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/21\mathbb{Z}$ , as a larger torsion group would contradict Theorem 2.4. By Corollary 2.10, we see that the 21-torsion point has to be defined over  $\mathbb{Q}_{1,3}$ . By [20, Theorem 1], there is a unique such curve  $E = 162b1$  satisfying this property.  $\square$

**Lemma 5.5.** *If  $E(\mathbb{Q})[2^\infty] \neq E(\mathbb{Q}_{\infty,3})[2^\infty]$ , then  $E(\mathbb{Q}_{\infty,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .*

*Proof.* By [19, Lemma 1],  $E(\mathbb{Q})[2] \neq \{O\}$ , then  $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q}_{\infty,3})[2^\infty]$  and the 2-power torsion can grow only if  $E(\mathbb{Q})[2] \neq \{O\}$  and all the growth that occurs, occurs over the field obtained by adjoining a 2-torsion point. By [20, Proposition 9], if  $E(\mathbb{Q}_{1,3})[2] \neq \{O\}$  then  $E(\mathbb{Q}_{1,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  and so  $E(\mathbb{Q}_{\infty,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .  $\square$

**Lemma 5.6.** *There are no points of order 18 in  $E(\mathbb{Q}_{\infty,3})$ .*

*Proof.* Suppose that  $E/\mathbb{Q}$  has a point of order 18 over  $\mathbb{Q}_{\infty,3}$ . By Corollary 2.10, we see that the points of order 18 are defined over  $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$ . We will prove that  $X_1(18)(\mathbb{Q}(\zeta_9)^+)$  consists of only cusps. We compute that the rank of  $J_1(18)(\mathbb{Q}(\zeta_9)^+)$  is 0. By considering reduction modulo small primes of good reduction, we get that the torsion of  $J_1(18)(\mathbb{Q}(\zeta_9)^+)$  is a subgroup of  $\mathbb{Z}/21\mathbb{Z}^2$ . We find 12 points in  $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ , all of which are cusps, and the differences of pairs of these cusps generate a group isomorphic to  $\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$ . To prove that  $J_1(18)(\mathbb{Q}(\zeta_9)^+) \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$ , we use the following nice argument. One finds that

$$J_1(18)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/21\mathbb{Z},$$

$$J_1(18)(\mathbb{Q}(\zeta_3))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z},$$

and by considering reduction modulo small primes, that

$$J_1(18)(\mathbb{Q}(\zeta_3)) \leq \mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Since  $\mathbb{Q}(\zeta_9) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_9)^+$  and  $\mathbb{Q}(\zeta_3) \cap \mathbb{Q}(\zeta_9)^+ = \mathbb{Q}$ , we see that the field of definition of the non-rational elements of  $J_1(18)(\mathbb{Q}(\zeta_9))[3]$  is  $\mathbb{Q}(\zeta_3)$ . Hence  $J_1(18)(\mathbb{Q}(\zeta_9)^+)[3] \simeq \mathbb{Z}/3\mathbb{Z}$  and after checking that none of the points in  $J_1(18)(\mathbb{Q}(\zeta_9)^+)$  come from points in  $X_1(18)(\mathbb{Q}(\zeta_9)^+)$  apart from the 12 known ones, we are done.  $\square$

*Proof of Theorem 1.3.* It remains to consider when the 3-power torsion grows.

By Lemma 2.8, if  $E(\mathbb{Q}_{\infty,3})[3] \neq 0$ , then  $E(\mathbb{Q})[3] \neq 0$ .

Suppose  $E(\mathbb{Q}_{\infty,3})$  has a point  $P$  of order 27; then  $E$  has a rational 27-isogeny over  $\mathbb{Q}$ , so  $j(E) = -2^{15} \cdot 3 \cdot 53$ . By Corollary 2.10,  $P \in E(\mathbb{Q}_{2,3})$ . Let  $E = 27a2$ , we have  $j(E) = -2^{15} \cdot 3 \cdot 53$ . We factor  $\psi := \psi_{27}/\psi_9$ , where  $\psi_n$  denotes the  $n$ -division polynomial  $E$  - the polynomial which is the product of all the  $x$ -coordinates of the points of order 27 of  $E$  and obtain that this polynomial has roots over  $\mathbb{Q}_{2,3}$ . This implies that there exists a single quadratic twist (over  $\mathbb{Q}_{2,3}$ )  $E^\delta$  of  $E$ , for some  $\delta \in L^*/(L^*)^2$  such that  $E^\delta(\mathbb{Q}_{2,3})$  has a point of order 27. It remains to check whether  $E^\delta$  is defined over  $\mathbb{Q}$ , or equivalently, whether  $\delta \cdot u^2 = d$  for some  $u \in L^*$  and some  $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ . We compute a  $\delta$  and obtain the  $N_{\mathbb{Q}_{2,3}/\mathbb{Q}}(\delta) = 3^{49}$ , so the only twists that we can consider are  $d = 3$  and  $-3$ . We obtain that  $E^{-3}$ , which is  $27a4$  has a point of order 27 over  $\mathbb{Q}_{2,3}$ . Note that from our argumentation it follows that  $27a4$  is the only elliptic curve with a point of order 27 over  $\mathbb{Q}_{\infty,3}$ . For  $E = 27a4$ , we have that  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/27\mathbb{Z}$ , as any larger torsion would violate Theorem 2.4.

If  $E(\mathbb{Q})[3^\infty] \simeq \mathbb{Z}/9\mathbb{Z}$ , then we claim that  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/9\mathbb{Z}$ . Indeed there cannot be any  $q$ -torsion for any  $q \neq 2, 3$  as this would force the existence of a  $9q$ -isogeny over  $\mathbb{Q}$ . It is impossible that  $E(\mathbb{Q}_{\infty,3})$  gains any 2-torsion, as this would imply that there is  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$  torsion over  $\mathbb{Q}_{1,3}$ , which is impossible by [20, Theorem 1].

Finally from what we have already proved, when  $E(\mathbb{Q}_{\infty,3})[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z}$  then  $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$  has to be either  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/12\mathbb{Z}$ ,  $\mathbb{Z}/21\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ .

This, together with the previous lemmas, completes the proof of the Theorem.  $\square$

## 6. EXAMPLES OF TORSION GROWTH

In this last section, we address the following question. Fix a prime  $p$ . Given a group  $G$  that can appear as  $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$  for some  $E/\mathbb{Q}$ , do there exist infinitely many  $j$ -invariants such that there exists an  $E/\mathbb{Q}$  with such a  $j$ -invariant with  $E(\mathbb{Q}_{\infty,p}) \simeq G$  but  $E(\mathbb{Q})_{\text{tors}} \not\simeq G$ ? By Theorem 1.1 we need only consider the cases where  $p = 2, 3$ .

**Theorem 6.1.** *Let  $G$  be one of the following groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, \quad & 3 \leq N \leq 10, \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad & 1 \leq N \leq 4, \end{aligned}$$

*There exist infinitely many elliptic curves  $E/\mathbb{Q}$  with distinct  $j$ -invariants such that  $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$  and  $E(\mathbb{Q})_{\text{tors}} \not\simeq G$ .*

*Proof.* We break this down into cases depending on whether  $E(\mathbb{Q})[2]$  needs to be trivial or not.

Suppose that  $G = \mathbb{Z}/N\mathbb{Z}$  for some odd integer  $N$ . Then there exist infinitely many elliptic curves  $E/\mathbb{Q}$  with different/distinct  $j$ -invariants such that  $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/N\mathbb{Z}$  and  $E$  has no additional isogenies. This is true because for each  $N$  in the statement the rational elliptic curves with  $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/N\mathbb{Z}$  come in a non-isotrivial 1-parameter family that generically doesn't have any additional isogenies. So by Hilbert irreducibility, outside of a "thin" set every curve in the family also has no additional isogenies. For more details about Hilbert irreducibility and thin sets, see [21, Chapter 9]. Thus, for each of these  $E$  the quadratic twist of by 2, denoted  $E^2$ , will have no rational points, as for odd  $N$ , we have that  $E(\mathbb{Q}(\sqrt{2}))[N] \simeq E(\mathbb{Q})[N] \oplus E^2(\mathbb{Q})[N]$  and since  $\mathbb{Q}(\sqrt{2})$  does not contain any  $m^{\text{th}}$ -roots of unity for any  $2 < m \mid N$  the existence of the Weil-pairing gives that  $E^2(\mathbb{Q})[N] = \{\mathcal{O}\}$ . Further, since  $E$  and  $E^2$  become isomorphic over  $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}_{\infty,2}$ , it follows that  $E^2(\mathbb{Q}_{\infty,2}) \simeq \mathbb{Z}/N\mathbb{Z}$ . Notice that the torsion can't grow any further since  $E$  and hence  $E^2$  don't have any additional isogenies.

Next, suppose that  $G = \mathbb{Z}/2n\mathbb{Z}$  with  $n \geq 2$ . Then again, there are infinitely many elliptic curves  $E/\mathbb{Q}$  such that  $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2n\mathbb{Z}$  and no additional isogenies. This time the twist  $E^2(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$  and  $E^2(\mathbb{Q}_{2,\infty}) \simeq \mathbb{Z}/2n\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ . Again, the torsion can't grow any further since  $E$  and hence  $E^2$  don't have any additional isogenies. If  $n \geq 4$ , we can't have that  $E^2(\mathbb{Q}_{2,\infty}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$  by Theorem 1.2, while when  $n = 2, 3, 4$  both cases are possible depending on the square class of the discriminant of  $E$ . Checking the generic elliptic curves with a rational torsion subgroup isomorphic to  $\mathbb{Z}/2n\mathbb{Z}$  for  $n = 2, 3, 4$  we see that there are infinitely many curves whose discriminant are congruent to 2 mod squares and infinitely many curves whose discriminants are  $-1$  mod squares. In the first case we have that  $E^2(\mathbb{Q}_{2,\infty}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$  while in the second  $E^2(\mathbb{Q}_{2,\infty}) \simeq \mathbb{Z}/2n\mathbb{Z}$ . So all that remains to check is the case when  $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .

To finish the last case we give a non-isotrivial family  $E_t$  with  $E_t(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$  and  $\mathbb{Q}(E_t[2]) = \mathbb{Q}(\sqrt{2})$ . This family is

$$E_t : y^2 = x^3 - \frac{2}{t^2 - 1/2}x^2 - \frac{2}{t^2 - 1/2}x$$

and generically these curves have no other isogenies and so for infinitely many of them  $E_t(\mathbb{Q}_{2,\infty})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . □

We list in Table 1 examples of elliptic curves with minimal discriminant achieving growth to each possible torsion structure over  $\mathbb{Q}_{\infty,2}$ .

*Remark.* Clearly it is impossible for an elliptic curve to have its torsion "grow" and become trivial so in Theorem 6.1  $G$  cannot be the trivial group and since an elliptic curve can only go from having trivial 2-torsion to having a point of order 2 in an extension degree divisible by 3, it cannot be that torsion grows to  $\mathbb{Z}/2\mathbb{Z}$  over  $\mathbb{Q}_{\infty,2}$ .

Now we consider the cases of torsion growth over  $\mathbb{Q}_{\infty,3}$ . By the results in Section 5 we need to consider the cases of torsion growth listed on Table 2 (we offer an example of minimal conductor for each type of growth in question). We prove that besides  $\mathbb{Z}/3\mathbb{Z}$  to  $\mathbb{Z}/21\mathbb{Z}$  and  $\mathbb{Z}/3\mathbb{Z}$  to  $\mathbb{Z}/27\mathbb{Z}$  (which are easily explained by  $X_0(21)$  and  $X_0(27)$  having finitely many rational points), all of these cases occur for infinitely many  $j$ -invariants.

First we have a theorem that gives the conductor of a cyclic cubic number field in terms of its defining polynomial.

**Theorem 6.2** ([10]). *Let  $K$  be a number field with  $[K : \mathbb{Q}] = 3$  and  $\text{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ . Then  $K = \mathbb{Q}(\theta)$  for a  $\theta$  satisfying  $\theta^3 + A\theta + B = 0$  with  $A, B \in \mathbb{Z}$  and, for any  $R \in \mathbb{Z}$ , if  $R^2 \mid A$  and  $R^3 \mid B$ , then  $|R| = 1$ . Further, the conductor  $\mathfrak{f}(K)$  is given by*

$$\mathfrak{f}(K) = 3^\alpha \prod_{\substack{p(\text{prime}) \equiv 1 \pmod{3} \\ p \mid (A, B)}} p$$

where, letting  $C$  be the square root of the discriminant of  $K$ ,

$$\alpha = \begin{cases} 0 & \text{if } 3 \nmid A \text{ or } 3 \parallel A, \ 3 \nmid B, \ 3^3 \mid C \\ 2 & \text{if } 3^2 \parallel A, \ 3^2 \parallel B \text{ or } 3 \parallel A, \ 3 \nmid B, \ 3^2 \parallel C. \end{cases}$$

The following lemma gives a way to construct an elliptic curve with torsion growth  $\{\mathcal{O}\}$  to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  and also an elliptic curve with torsion growth  $\mathbb{Z}/3\mathbb{Z}$  to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$  over  $\mathbb{Q}_{\infty,3}$ .

**Lemma 6.3.** *Let*

$$j_3(h) = \frac{(h+27)(h+3)^3}{h}.$$

*Suppose that we have  $u, v \in \mathbb{Z}$  with  $(u, v) = 1$  and  $u^2 + 27v^2 = 4 \cdot 3^k \cdot p^3$  for some  $k = 2, 3$  and any  $p \equiv 1 \pmod{3}$ . Then there is an elliptic curve  $E/\mathbb{Q}$  with  $j$ -invariant  $j_3(\frac{u^2}{v^2})$  such that*

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\} \quad \text{and} \quad E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

*Moreover there is a quadratic twist  $E'$  of  $E$  such that*

$$E'(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \quad \text{and} \quad E'(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

*Proof.* Let  $E/\mathbb{Q}$  be an elliptic curve with  $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$  and  $E(\mathbb{Q}_{\infty,3}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ . Then  $E$  has a 3-isogeny and square discriminant, so  $E$  corresponds to a rational point on  $X_0(3)$ , and so

$$j(E) = \frac{(h+27)(h+3)^3}{h},$$

for some  $h \in \mathbb{Q}$ . A model for an elliptic curve with such a  $j$ -invariant is given by

$$E_h : y^2 = f(x) = x^3 + \frac{-27(h+3)^3(h+27)}{(h^2+18h-27)^2}x + \frac{54(h+3)^3(h+27)}{(h^2+18h-27)^2},$$

and by computing the discriminant of this model we can see that  $E_h$  has square discriminant if and only if  $h \in (\mathbb{Q}^*)^2$ . If we choose an  $h$  such that the discriminant of  $E_h$  is a square, then  $\text{Gal}(\mathbb{Q}(E_h[2])/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$  and  $\mathbb{Q}(E_h[2]) = \mathbb{Q}(f)$ .

Now we examine  $\mathbb{Q}(f)$  to determine when  $\mathbb{Q}(f) = \mathbb{Q}_{1,3}$ . This will occur precisely when the conductor of  $\mathbb{Q}(f)$  is divisible only by 3. Through a change of variables we see that  $\mathbb{Q}(f) = \mathbb{Q}(x^3 + A(h)x + B(h))$  where

$$A(h) = -27(h+3)(h+27) \text{ and } B(h) = 54(h+27)(h^2+18h-27).$$

We homogenize the equations by letting  $h = \frac{u^2}{v^2}$  written in lowest terms, so that all parameters are integers to obtain

$$A(u, v) = -27(u^2 + 3v^2)(u^2 + 27v^2) \text{ and } B(u, v) = 54(u^2 + 27v^2)(u^4 + 18u^2v^2 - 27v^4).$$

By Theorem 6.2 the conductor will be a power of 3 when the gcd of  $A(u, v)$  and  $B(u, v)$  is divisible only by a primes  $p \equiv 2 \pmod{3}$ , 3, and by cubes since, by a change of variables, we can remove cubes from the gcd of  $A(u, v)$  and  $B(u, v)$ .

We can see that  $(A(u, v), B(u, v)) = 2^a \cdot 3^b \cdot (u^2 + 27v^2)$  for some  $a, b \in \mathbb{Z}^{\geq 0}$ , since if a prime divides both  $u^2 + 3v^2$  and  $u^4 + 18u^2v^2 - 27v^4$  then it must be 2 or 3. Thus, if we choose  $u$  and  $v$  as in the statement of the lemma, we see that  $\mathbb{Q}(E_h[2])$  will have conductor a power of 3, and thus  $\mathbb{Q}(E_h[2]) = \mathbb{Q}_{1,3}$ .

Finally, by construction,  $E_h$  is defined over  $\mathbb{Q}$  and has a rational 3-isogeny. Thus, there is a twist of  $E_h$  that has a 3-torsion point over  $\mathbb{Q}$ . Note that taking a quadratic twist does not change the field of definition of the 2-torsion points, so this twist indeed has the growth we are looking for over  $\mathbb{Q}_{1,3}$ . □

Now, we have a lemma to ensure there are infinitely many non-isomorphic  $E/\mathbb{Q}$  with the above torsion growth.

**Lemma 6.4.** *For any prime  $p \equiv 1 \pmod{3}$  and  $k = 2, 3$  there exists  $u, v \in \mathbb{Z}$  with  $(u, v) = 1$  such that  $u^2 + 27v^2 = 4 \cdot 3^k \cdot p^3$ .*

*Proof.* Let  $K = \mathbb{Q}(\sqrt{-3})$ . Then

$$u^2 + 27v^2 = \text{Nm}_{K/\mathbb{Q}}(u + 3v\sqrt{-3})$$

and so we wish to prove that there are elements of the form  $u + 3v\sqrt{-3}$  with  $(u, v) = 1$  of norm  $4 \cdot 3^k \cdot p^3$  for any  $p \equiv 1 \pmod{3}$  and for  $k = 2, 3$ . Since norms are multiplicative, and we see that

$$4 \cdot 3^2 = \text{Nm}_{K/\mathbb{Q}}(3 + 3\sqrt{-3})$$

and

$$4 \cdot 3^3 = \text{Nm}_{K/\mathbb{Q}}(9 + 3\sqrt{-3})$$

it remains to show that there is an element of norm  $p^3$  in  $K$ .

Let  $\alpha$  be a root of  $x^2 + x + 1$ , so that the ring of integers of  $K$  is equal to  $\mathbb{Z}[\alpha]$ . Since  $p \equiv 1 \pmod{3}$ , this prime splits in  $K$  and so

$$p = \mathfrak{p}\bar{\mathfrak{p}} = (x + y\alpha)(x + y\alpha^2)$$

for some  $x, y \in \mathbb{Z}$ . We have  $\text{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) = p$  and so we claim  $\mathfrak{p}^3$  is the element we want to take. We can find relatively prime  $a, b \in \mathbb{Z}$  such that

$$\mathfrak{p}^3 = a + 3b\alpha.$$

Indeed, simply writing  $\mathfrak{p}^3 = (x + y\alpha)^3$  for some  $x, y \in \mathbb{Z}$  and expanding shows that the coefficient of  $\alpha$  is divisible by 3. Further, if  $d = (a, b) > 1$ , then

$$\mathfrak{p}^3 = (d) \left( \frac{a}{d} + 3\frac{b}{d}\alpha \right).$$

However, taking norms on both sides shows that  $d = p$ , so then  $\bar{\mathfrak{p}} \mid \mathfrak{p}^3$ , which is impossible.

Thus, we have found elements in  $K$  of norm  $4 \cdot 3^2$ ,  $4 \cdot 3^3$ , and  $p^3$  for any prime  $p \equiv 1 \pmod{3}$ . The lemma follows from expanding the product of  $3 + 3\sqrt{-3}$  and  $9 + 3\sqrt{-3}$  with  $\mathfrak{p}^3$  to show that the product is indeed of the form  $u + 3v\sqrt{-3}$  with  $(u, v) = 1$ . □

An immediate corollary of this lemma is:

**Corollary 6.5.** *There are infinitely many  $j \in \mathbb{Q}$  such that there exists an elliptic curve  $E/\mathbb{Q}$  with  $j(E) = j$  that satisfy  $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$  and  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .*

*There are infinitely many  $j \in \mathbb{Q}$  such that there exists an elliptic curve  $E/\mathbb{Q}$  with  $j(E) = j$  that satisfy  $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$  and  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ .*

Now we illustrate a parallel idea for torsion growth from  $\{\mathcal{O}\}$  to  $\mathbb{Z}/7\mathbb{Z}$  and from  $\mathbb{Z}/3\mathbb{Z}$  to  $\mathbb{Z}/9\mathbb{Z}$  over  $\mathbb{Q}_{\infty,3}$  respectively.

**Lemma 6.6.** *Let*

$$j_7(h) = \frac{(h^2 + 13h + 49)(h^2 + 5h + 1)^3}{h}$$

*Suppose that we have  $u, v \in \mathbb{Z}$  with  $(u, v) = 1$  and  $u^2 + 13uv + 49v^2 = 3^k \cdot p^3$  for some  $k = 2, 3$  and any  $p \equiv 1 \pmod{3}$ . Then there is an elliptic curve  $E/\mathbb{Q}$  with  $j$ -invariant  $j_7(\frac{u}{v})$  such that  $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$  and  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$ .*

*Proof.* Let  $E/\mathbb{Q}$  be an elliptic curve with  $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$ . Then  $E/\mathbb{Q}$  has a 7-isogeny over  $\mathbb{Q}$ , so it corresponds to a rational point on  $X_0(7)$ , and so

$$j(E) = \frac{(h^2 + 13h + 49)(h^2 + 5h + 1)^3}{h}$$

for some  $h \in \mathbb{Q}$ . A model for an elliptic curve with such a  $j$ -invariant is given by

$$E_h : y^2 = x^3 - \frac{27(h^2 + 5h + 1)^3(h^2 + 13h + 49)}{(h^4 + 14h^3 + 63h^2 + 70h - 7)^2}x + \frac{54(h^2 + 5h + 1)^3(h^2 + 13h + 49)}{(h^4 + 14h^3 + 63h^2 + 70h - 7)^2}.$$

We can compute the 7<sup>th</sup> division polynomial of  $E_h$ , and obtain that it has one irreducible factor of degree 3, which we denote by  $f_7$ , and one factor of degree 21. We wish to determine for which values of  $h$  does this degree 3 factor define the extension  $\mathbb{Q}_{1,3}$ .

By a change of coordinates we see that  $\mathbb{Q}(f_3(h)) = \mathbb{Q}(x^3 + A(h)x + B(h))$  where

$$A(h) = -3(h^2 + 13h + 49) \text{ and } B(h) = -(2h + 13)(h^2 + 13h + 49).$$

We homogenize the equations by letting  $h = \frac{u}{v}$  with  $(u, v) = 1$  so that all parameters are integers to obtain

$$A(u, v) = -3(u^2 + 13uv + 49v^2) \text{ and } B(u, v) = -(2u + 13v)(u^2 + 13uv + 49v^2).$$

By Theorem 6.2 the conductor will be a power of 3 when the gcd of  $A(u, v)$  and  $B(u, v)$  is divisible only by a primes  $p \equiv 2 \pmod{3}$ , 3, and by cubes since, by a change of variables, we can remove cubes from the gcd of  $A(u, v)$  and  $B(u, v)$ .

We can see that  $(A(u, v), B(u, v)) = 2^a \cdot 3^b \cdot (u^2 + 13uv + 49v^2)$  for some  $a, b \in \mathbb{Z}^{\geq 0}$ . Thus, if we choose  $u$  and  $v$  as in the statement of the lemma, we see that  $\mathbb{Q}(f_7)$  will have conductor a power of 3, and thus  $\mathbb{Q}(f_7) = \mathbb{Q}_{1,3}$ . Now taking an appropriate quadratic twist, we can make  $\mathbb{Q}(f_7) = \mathbb{Q}(P)$  for a point  $P \in E[7]$  of order 7.

□

**Lemma 6.7.** *Let  $h = \frac{u}{v}$  for  $u, v \in \mathbb{Z}$  with  $(u, v) = 1$  satisfying*

$$u^2 + 3uv + 9v^2 = 3^3 \cdot p^3$$

for some prime  $p \equiv 1 \pmod{3}$  and let  $E_h/\mathbb{Q}$  be the elliptic curve given by

$$E_h : y^2 = x^3 - 27h^5(h^3 - 24)^5x + 54h^6(h^3 - 24)^6(h^6 - 36h^3 + 216).$$

Then  $E_h(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$  and  $E_h(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/9\mathbb{Z}$ .

*Proof.* For such torsion growth to occur, an elliptic curve must have a 3-torsion point over  $\mathbb{Q}$  as well as a 9-isogeny over  $\mathbb{Q}$  whose kernel contains this point of order 3. A model for elliptic curves over  $\mathbb{Q}$  with this level structure is given in [3] Table 6, and they are elliptic curves precisely of the form

$$E_h : y^2 = x^3 - 27h^5(h^3 - 24)^5x + 54h^6(h^3 - 24)^6(h^6 - 36h^3 + 216).$$

for some  $h \in \mathbb{Q}$ . We can compute the  $9^{\text{th}}$  division polynomial of  $E_h$  and divide it by the  $3^{\text{rd}}$  division polynomial and obtain one factor of degree 3, which we denote by  $f_9$ . We wish to determine for which values of  $h$  does this degree 3 factor define the extension  $\mathbb{Q}_{1,3}$ .

By a change of coordinates we see that  $\mathbb{Q}(f_9(h)) = \mathbb{Q}(x^3 + A(h)x + B(h))$  where

$$A(h) = -432(h^2 + 3h + 9) \quad \text{and} \quad B(h) = -1728(2h + 3)(h^2 + 3h + 9).$$

We homogenize the equations by letting  $h = \frac{u}{v}$  with  $(u, v) = 1$  so that all parameters are integers to obtain

$$A(u, v) = -432(u^2 + 3uv + 9v^2) \quad \text{and} \quad B(u, v) = -1728(2u + 3v)(u^2 + 3uv + 9v^2).$$

By Theorem 6.2 the conductor will be a power of 3 when the gcd of  $A(u, v)$  and  $B(u, v)$  is divisible only by a primes  $p \equiv 2 \pmod{3}$ , 3, and by cubes since, by a change of variables, we can remove cubes from the gcd of  $A(u, v)$  and  $B(u, v)$ .

We can see that  $(A(u, v), B(u, v)) = 2^a \cdot 3^b \cdot (u^2 + 3uv + 9v^2)$  for some  $a, b \in \mathbb{Z}^{\geq 0}$ . Thus, if we choose  $u$  and  $v$  as in the statement of the lemma, we see that  $\mathbb{Q}(f_9)$  will have conductor a power of 3, and thus  $\mathbb{Q}(f_9) = \mathbb{Q}_{1,3}$ . Now, if  $P$  is a generator of the kernel of the isogeny, then  $G_{\mathbb{Q}}$  acts on  $\langle P \rangle$  by multiplication by 1, 4, or 7, since  $3P \in E(\mathbb{Q})$ . Hence,  $P$  is fixed by an index 3 subgroup of  $G_{\mathbb{Q}}$ , and thus defined over a cubic field, in particular, the cubic field where it's  $x$ -coordinate is defined, i.e.  $\mathbb{Q}(f_9) = \mathbb{Q}_{1,3}$ .  $\square$

We remark that the criteria given in Lemma 6.6 and Lemma 6.7 are asking when  $3^3p^3$  is primitively represented by some binary quadratic form. In both Lemmas, the binary quadratic forms have discriminant  $-27$ . We now prove that both the above criteria are satisfied for infinitely many primes  $p$  by proving a statement about integers represented by binary quadratic forms of discriminant  $-27$ .

**Lemma 6.8.** *Let  $f(x, y)$  be any binary quadratic form of discriminant  $-27$ . Then there exist primitive solutions to  $f(x, y) = 3^3 \cdot p^3$  for all  $p \equiv 1 \pmod{3}$ .*

*Proof.* Since  $f(x, y)$  has discriminant  $-27$ , there is an  $\text{SL}_2(\mathbb{Z})$  transformation of variables so that

$$f(x, y) \sim u^2 + uv + 7v^2$$

i.e.  $\begin{bmatrix} u \\ v \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix}$  for some  $M \in \text{SL}_2(\mathbb{Z})$ . Moreover,  $\text{SL}_2(\mathbb{Z})$  transformations preserve the gcd of the coordinates, so we need only find primitive solutions to

$$u^2 + uv + 7v^2 = 3^3 \cdot p^3$$



for all primes  $p \equiv 1 \pmod{3}$ . We let  $K = \mathbb{Q}(\sqrt{-3})$  with ring of integers by  $\mathbb{Z}[\alpha]$  where  $\alpha = \frac{-1+\sqrt{-3}}{2}$  is a primitive  $3^{rd}$  root of unity. Notice that

$$u^2 + uv + 7v^2 = \text{Nm}_{K/\mathbb{Q}}(u + 3v\alpha)$$

so we want to find elements in  $K$  of the form  $u + 3v\alpha$  with  $(u, v) = 1$  and norm  $3^3 \cdot p^3$ .

Let  $p$  be a prime such that  $p \equiv 1 \pmod{3}$ . Then  $p$  is split in  $K$ , so

$$p = \mathfrak{p}\bar{\mathfrak{p}} = (x + y\alpha)(x + y\alpha^2)$$

for some  $x, y \in \mathbb{Z}$ . Recalling the argument given in the proof of Lemma 6.4,

$$\mathfrak{p}^3 = a + 3b\alpha$$

for some relatively prime integers  $a, b \in \mathbb{Z}$ . Further, we have that 3 is ramified in  $K$ ,

$$(3) = \mathfrak{p}_3^2 = (1 + 2\alpha)^2$$

and finally that  $\mathfrak{p}_3^3 = (3 + 2(3\alpha))$ . Thus, an element of norm  $3^3 p^3$  is

$$\mathfrak{p}_3^3 \mathfrak{p}^3$$

and the lemma follows from expanding the product of the two elements to show that the product is indeed of the form  $u + 3v\alpha$  with  $(u, v) = 1$ .  $\square$

Thus, an immediate corollary is

**Corollary 6.9.** *There are infinitely many  $j \in \mathbb{Q}$  such that there exists an elliptic curve  $E/\mathbb{Q}$  with  $j(E) = j$  that satisfy  $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$  and  $E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$ .*

*There are infinitely many  $j \in \mathbb{Q}$  such that there exists an elliptic curve  $E/\mathbb{Q}$  with  $j(E) = j$  that satisfy  $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z}$  and  $E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/9\mathbb{Z}$ .*

Cremona Reference	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,2})_{\text{tors}}$
704d1	$\{\mathcal{O}\}$	$\mathbb{Z}/3\mathbb{Z}$
24a6	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$
704a1	$\{\mathcal{O}\}$	$\mathbb{Z}/5\mathbb{Z}$
320c1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$
832f	$\{\mathcal{O}\}$	$\mathbb{Z}/7\mathbb{Z}$
24a3	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$
1728j3	$\{\mathcal{O}\}$	$\mathbb{Z}/9\mathbb{Z}$
768b1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$
30a5	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$
14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
24a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
32a4	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

TABLE 1. Elliptic curves of minimal conductor with torsion growth over  $\mathbb{Q}_{\infty,2}$ .

Cremona Reference	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,3})_{\text{tors}}$
162b2	$\{\mathcal{O}\}$	$\mathbb{Z}/7\mathbb{Z}$
324a2	$\{\mathcal{O}\}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
27a3	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$
162b1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/21\mathbb{Z}$
27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$
324a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

TABLE 2. Elliptic curves of minimal conductor with torsion growth over  $\mathbb{Q}_{\infty,3}$ .

## REFERENCES

- [1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265. 3
- [2] M. Chou, *Torsion of rational elliptic curves over the maximal abelian extension of  $\mathbb{Q}$* , preprint <https://arxiv.org/abs/1711.00412> 4
- [3] H. Daniels, M. Derickx, J. Hatley *Groups of generalized  $G$ -type and applications to torsion subgroups of rational elliptic curves over infinite extensions of  $\mathbb{Q}$* ; arXiv:1803.09614 [math.NT]. 6
- [4] H. B. Daniels, A. Lozano-Robledo, F. Najman, A. V. Sutherland, *Torsion points on rational elliptic curves over the compositum of all cubic fields*, Math. Comp. **87** (2018), 425–458. 2.3
- [5] M. Derickx, F. Najman, *Torsion of elliptic curves over cyclic cubic fields*, preprint. [https://web.math.pmf.unizg.hr/~fnajman/cyclic\\_cubic.pdf](https://web.math.pmf.unizg.hr/~fnajman/cyclic_cubic.pdf)
- [6] Y. Fujita, *The 2-primary torsion on elliptic curves in the  $\mathbb{Z}_p$ -extensions of  $\mathbb{Q}$* , manuscripta math. **118** (2005), 339–360. 4.7
- [7] E. Gonzalez-Jimenez, F. Najman, *Growth of torsion groups of elliptic curves upon base change*, preprint. 2.6, 2.7, 2, 4
- [8] R. Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), 1167–1196 3.3
- [9] R. Greenberg, *Iwasawa theory for elliptic curves*, In: Viola C. (eds) Arithmetic Theory of Elliptic Curves. Lecture Notes in Mathematics, vol 1716. Springer, Berlin, Heidelberg, 1999. 1
- [10] J. Huard, B. Spearman, K. Williams, *A short proof of the formula for the conductor of an abelian cubic field*, Norske Vid. Selsk. 2 (1994), 3–8. 6.2
- [11] S. Kamienny, *Torsion points on elliptic curves and  $q$ -coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. 4, 4
- [12] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. **152** (2012), 291–305. 4, 4, 5
- [13] M. A. Kenku, *The modular curve  $X_0(39)$  and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. 2.4
- [14] M. A. Kenku, *The modular curves  $X_0(65)$  and  $X_0(91)$  and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. 2.4
- [15] M. A. Kenku, *The modular curve  $X_0(169)$  and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244. 2.4
- [16] M. A. Kenku, *The modular curve  $X_0(125)$ ,  $X_1(25)$  and  $X_1(49)$* , J. London Math. Soc. (2) **23** (1981), 415–427. 2.4
- [17] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 4, 4
- [18] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), pp. 129–162. 1, 2.4
- [19] F. Najman, *Torsion of elliptic curves over cubic fields*, J. Number Theory **132** (2012), 26–36. 5
- [20] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on  $X_1(n)$* , Math. Res. Letters **23** (2016) 245–272. 4, 5, 5, 5
- [21] J. P. Serre *Lectures on the Mordell-Weil theorem*. Third edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997. x+218 pp. 6
- [22] J. H. Silverman, *Arithmetic of elliptic curves*, Second Edition, Springer-Verlag, New York, 2009. 2.1, 3
- [23] J. A. Thorne, *Elliptic curves over  $\mathbb{Q}_\infty$  are modular*, J. Eur. Math. Soc. (JEMS), to appear. 1
- [24] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997. 1

DEPT. OF MATHEMATICS, TUFTS UNIVERSITY, MEDFORD, MA, 02155, USA

*E-mail address:* `michael.chou@tufts.edu`

*URL:* `https://sites.tufts.edu/michaelchou/`

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMHERST COLLEGE, AMHERST, MA 01002, USA

*E-mail address:* `hdaniels@amherst.edu`

*URL:* `https://hdaniels.people.amherst.edu/`

UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

*E-mail address:* `ikrijan@math.hr`

*URL:* `http://web.math.pmf.unizg.hr/~ikrijan/`

UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

*E-mail address:* `fnajman@math.hr`

*URL:* `http://web.math.pmf.unizg.hr/~fnajman/`