On the number of elliptic curves with prescribed isogeny or torsion group over number fields of prime degree

Filip Najman

Abstract

Let p be a prime and K a number field of degree p. We determine the finiteness of the number of elliptic curves, up to $\overline{K}$-isomorphism, having a prescribed property, where this property is either that the curve contains a fixed torsion group as a subgroup, or that it has a cyclic isogeny of prescribed degree.

1   Introduction

Our goal is to study the number of elliptic curves over number fields of prime degree $K/\mathbb{Q}$, up to $\overline{K}$-isomorphism, having a prescribed property. This property will be one of the following:

1) The curve's group of K-rational points contains a subgroup isomorphic to a fixed torsion group T.

2) The curve admits a cyclic n-isogeny defined over K, for some prescribed integer n.

Our methods will actually solve the first problem for number fields of degree d, where d is not divisible by any of 2, 3 or 5.

It is clear that, when counting the number of elliptic curves over K with a cyclic n-isogeny, one has to count up to $\overline{K}$-isomorphism, since if E/K has a cyclic n-isogeny, then so does every quadratic twist of E (in other words, the modular curve $Y_0(n)$ classifying cyclic n-isogenies is a coarse moduli space).

On the other hand, it is not clear whether it is better to count elliptic curves with prescribed torsion up to K-isomorphism or $\overline{K}$-isomorphism. Since we will mostly be concerned with the finiteness of the number of curves with given torsion, and since (see for example [12, Lemma 5.5]) the number of elliptic curves over K whose group of K-rational points contains a subgroup isomorphic to T is finite up to $\overline{K}$-isomorphism if and only if it is finite up to K-isomorphism, we see that the choice of the isomorphism does not really matter.

Thus, for simplicity's sake, we will always count elliptic curves up to $\overline{K}$-isomorphism, and we will do so, usually without mention, throughout the paper.

The number of curves will naturally depend on the prescribed property. Let $m|n$. Folowing [9], we define

$$\Gamma_1(m,n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) | a-1 \equiv c \equiv 0 \mod n, \ b \equiv d-1 \equiv 0 \mod m \right\},$$

and let $X_1(m,n)$ be $\Gamma_1(m,n)\backslash\mathcal{H}^*$. The curve $X_1(m,n)$ is defined over $\mathbb{Q}(\zeta_m)$. Let $Y_1(m,n) = X_1(m,n)\backslash\{cusps\}$. The moduli interpretation of $Y_1(m,n)$ is that its K-rational points classify isomorphism classes of the triples (E, P_m, P_n), where E is an elliptic curve (over K) and P_m and P_n are torsion points (over K) which generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Note that $X_1(1,n) = X_1(n)$ and $Y_1(n) = Y_1(1,n)$. Similarly $X_0(n) = \Gamma_0(n)\backslash\mathcal{H}^*$ and $Y_0(n) = X_0(n) \backslash\{cusps\}$. The moduli interpretation of $Y_0(n)$ is that its K-rational points classify isomorphism classes of pairs (E, C), where E/K is an elliptic curve and C is a cyclic $(\mathrm{Gal}(\overline{K}/K)$-invariant) subgroup of E.

Let Y be the modular curve ($Y_1(m,n)$ or $Y_0(n)$) corresponding to the property we are studying, and X its compactification. It is clear that the number of elliptic curves with the desired property over K is positive and finite if and only if $0 < |Y(K)| < +\infty$. Hence, we will from now on, express our problem in determining when $0 < |Y(K)| < +\infty$, or equivalently $|\{K$-rational cusps of $X\}| < |X(K)| < +\infty$.

The key value that will determine whether $0 < |Y(K)| < +\infty$ is its genus. If Y is a genus 0 curve, then $Y(K)$ has either none or infinitely many points, thus implying that there are none or infinitely many curves with the given property.

In particular, for $X = X_1(m,n)$ of genus 0 and $m > 2$, that is for $(m,n) = (3,3), (3,6), (4,4),$ or $(5,5)$, $|Y(K)| = \infty$ if K contains ζ_m, an m-th primitive root of unity, and zero otherwise. One direction follows from the Weil pairing, and the other from the fact that the curve $X_1(m,n)$ has a $\mathbb{Q}(\zeta_m)$-rational point (and hence infinitely many) for all of the listed pairs.

On the other hand, if X is of genus ≥ 2, then by Faltings' theorem [6], $X(K)$ has only finitely many points. Thus, we see that we are left only with the genus 1 case.

In Section 2 we study $|Y_1(m,n)(K)|$; combining the obtained results with the results of [8] and [13], we solve this problem for number fields of prime degree completely.

In Section 3 we study the number of points on $Y_0(n)$, for a prescribed n, over prime degree fields K.

2 Number of elliptic curves with prescribed torsion

As stated in the introduction, we need to study the modular curves $X_1(m,n)$ of genus 1. One can see in [7, Theorem 2.6, Proposition 2.7] that $X_1(m,n)$ is of

genus 1 only for $(m, n) = (1, 11),\ (1, 14),\ (1, 15),\ (2, 10),\ (2, 12),\ (3, 9),\ (4, 8)$ or $(6, 6)$. Note that if K is a field of odd degree, $m > 2$ and $m | n$, then $|Y_1(m, n)(K)| = 0$, as otherwise $\mathbb{Q}(\zeta_m)$ would have to be a subfield of K (because of the Weil pairing [18, Corollary 3.11]), which is impossible. Thus we can ignore the cases $(3, 9),\ (4, 8)$ and $(6, 6)$, implying that we are left with the cases

$$(m, n) \in \{(1, 11),\ (1, 14),\ (1, 15),\ (2, 10),\ (2, 12)\}. \tag{1}$$

The number of points on $Y_1(m, n)$ was determined by Kamienny and the author [8] over all quadratic fields and by the author [13] over all cubic fields. In both cases there were exceptional cases where, there are a few fields K over which $0 < |Y_1(m, n)(K)| < +\infty$. Note also that in [14] it is proven that there are infinitely many such quartic fields. In this paper, we prove that there are no such number fields of degree d, where d is not divisible by any of $2, 3$ or 5. For $d = 5$, we find that $|Y_1(11)(\mathbb{Q}(\zeta_{11})^+| = 15$ (where $\mathbb{Q}(\zeta_{11})^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_{11})$) and $|Y_1(m, n)(K)| = 0$ or ∞ for all other triples (K, m, n), where K is a quintic field and (m, n) are listed in (1).

We state our results in the theorem.

Theorem 1. *a) Let d be a positive integer coprime to 6 and K a number field of degree d. Then*

$$|Y_1(m, n)(K)| = \begin{cases} 0 \ or \ \infty & if\ (m, n) \in \{(1, 14), (1, 15), (2, 10), (2, 12)\} \\ 0 & if\ (m, n) \in \{(3, 9), (4, 8), (6, 6)\} \end{cases} \tag{2}$$

b) Let K a number field of degree d. Then

$$|Y_1(11)(K)| = \begin{cases} 0 \ or \ \infty & if\ 3, 4, 5 \nmid d \ or \ if\ d = 5 \ and\ K \neq \mathbb{Q}(\zeta_{11})^+ \\ 15 & if\ K = \mathbb{Q}(\zeta_{11})^+ \end{cases} \tag{3}$$

Remark 1.

An elliptic curve over $\mathbb{Q}$ has one of the following 15 torsion groups (see [10] for the proof):

$$\mathbb{Z}/n\mathbb{Z},\ \text{where}\ n = 1 \dots 10, 12$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}\ \text{where}\ n = 1 \dots 4, \tag{4}$$

For any number field K, there are infinitely many elliptic curves containing any of the groups from (4). All of the groups (4) are parameterized by modular curves of genus 0. On the other hand, the groups from (2) and (3) are parameterized by curves of genus 1.

We can summarize our results in terms of elliptic curves with prescribed torsion groups. The following corollary follows trivially from Theorem 1 and Remark 1.

Corollary 2. *Let d be a positive integer not divisible by any of 2, 3 or 5, and let be K a number field of degree d. If T is one of the following groups*

$$\mathbb{Z}/n\mathbb{Z},\ \text{where}\ n = 1, \dots, 12, 14, 15,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ where } n = 1, \dots, 6, \tag{5}$$

then there are either none or infinitely many elliptic curves over K containing T as a subgroup. If T is any other finite group, then there are only finitely many (maybe 0) elliptic curves containing T as a subgroup.

Let $Y_1(m,n)$ be of genus 1. For $0 < |Y_1(m,n)(K)| < +\infty$ to be true, the following two conditions have to hold.

(C1) $rank(X_1(m,n)(K)) = 0$.

(C2) At least one of the torsion points of $X_1(m,n)(K)$ is not a cusp (note that this implies $|X_1(m,n)(K)|_{tors} > |X_1(m,n)(\mathbb{Q})|_{tors}$).

To prove Theorem 1, we will use division polynomials and Galois representations.

We denote by ψ_n the n-th division polynomial, which has the property that, for a point $P \neq \mathcal{O}$ on an elliptic curve in Weierstrass form, $\psi_n(x(P)) = 0$ if and only if $nP = 0$. For a definition and more information on division polynomials see [18]. Note that the field of definition of P will be either the number field F obtained by adjoining a root of ψ_n or a quadratic extension of F.

Let $E[n]$ denote the n-torsion subgroup of $E/\mathbb{Q}$ over $\overline{\mathbb{Q}}$ and let $\mathbb{Q}(E[n])$ be the n-th division field of E. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ and gives rise to an embedding $\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ called a *Galois representation associated to $E[n]$*. Serre's Open Image Theorem [15] tells us that for an elliptic curve without complex multiplication (all of the $X_1(m,n)$-s that we study do not have complex multiplication) this embedding is surjective for all but finitely many primes. The primes for which this embedding is possibly not surjective can be computed in SAGE [16] with the non_surjective() function, which uses the bounds for the non-surjective primes from [1].

To prove Theorem 1, we will find the fields K of prime degree over which $X_1(m,n)(K)_{tors}$ is strictly larger than $X_1(m,n)(\mathbb{Q})_{tors}$, where (m,n) is a pair from the list (1).

Proof of Theorem 1. Before proceeding with the details of the proof, we sketch the strategy of the proof.

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Let l be an odd prime such that the Galois representation ρ_l is surjective. This implies that the division polynomial ψ_l is irreducible. The field of definition F of a torsion point of order l has to contain the field obtained by adjoining a root of ψ_l to $\mathbb{Q}$, which is a field of degree $(l^2 - 1)/2$. In particular, the degree of F must be divisible by 4. It follows that if K is any number field of prime degree then $E(K)$ cannot contain a point whose order is divisible by any odd prime l for which ρ_l is surjective.

If $E(\mathbb{Q})$ has at least one point of order 2 and K is a number field of odd degree, then by [13, Lemma 1], the 2-Sylow subgroup of $E(K)$ is equal to the 2-Sylow subgroup of $E(\mathbb{Q})$. Suppose now $E(\mathbb{Q})[2] = 0$. One can then write $E(\mathbb{Q})$ in short Weierstrass form $y^2 = f(x)$, where $f(x)$ is an irreducible degree

4

3 polynomial, and conclude that any number field containing a point of order 2 has to have the field obtained by adjoining a root of f to $\mathbb{Q}$ as a subfield. Thus $E(\mathbb{Q})[2] = 0$ implies $E(K)[2] = 0$ when the degree of K is not divisible by 3.

Combining these two cases, we see that for any number field K of degree coprime to 6, the 2-Sylow subgroup of $E(K)$ is equal to the 2-Sylow subgroup of $E(\mathbb{Q})$.

As the $X_1(m, n)$ we study do not have complex multiplication, it follows that condition (C2) can be true only if there exists a prime l such that ρ_l is non surjective and a prime degree field K contains a root of ψ_l.

For all the $X_1(m, n)$-s we study, we list the primes (computed in SAGE) for which the Galois representation ρ_l is not surjective in the table below.

Modular curve	Cremona Label [2]	primes l for which ρ_l is not surjective
$X_1(11)$	11a3	5
$X_1(14)$	14a4	2, 3
$X_1(15)$	15a8	2
$X_1(2, 10)$	20a2	2, 3
$X_1(2, 12)$	24a4	2

Table 1.

We start with $X_1(11)$ and the prime 5. The curve elliptic curve $X_1(11)$ has the following Weierstrass model

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

and $X_1(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$ and all the rational torsion points are cusps. Since no number field of odd degree contains $\mathbb{Q}(\zeta_5)$ as a subfield, $X_1(11)(F)[5] \simeq \mathbb{Z}/5\mathbb{Z}$, for all number fields F of odd degree. We now factor the 25-division polynomial of $X_1(11)$ and obtain the factorization

$$\psi_{25} = \psi_5 f_5 g_5 f_{20} g_{20} f_{250},$$

where f_n and g_n are irreducible polynomials of degree n. We need to examine only the fields generated by f_5 and g_5, as the zeroes of ψ_5 correspond to the points of order 5, which are either rational (and thus cusps) or are defined over a field of even degree, and as f_{20}, g_{20} and f_{250} generate fields of even degree.

We compute that f_5 and g_5 generate the same field, $\mathbb{Q}(\zeta_{11})^+$. We compute $X_1(11)(\mathbb{Q}(\zeta_{11})^+)_{tors} \simeq \mathbb{Z}/25\mathbb{Z}$ and $rank(X_1(11)(\mathbb{Q}(\zeta_{11})^+)) = 0$ (via 2-descent). The curve $X_1(11)$ has 10 cusps over $\mathbb{Q}(\zeta_{11})^+$ (see [3, Example 9.3.5]), thus there are 15 non-cuspidal points on $X_1(11)(\mathbb{Q}(\zeta_{11})^+)$. As $\mathbb{Z}/11\mathbb{Z}$ has 10 generators and each point on $X_1(11)(\mathbb{Q}(\zeta_{11})^+)$ corresponds to a pair $(E, \pm P)$, where P is a point of order 11, we see that this implies that there are $15/5 = 3$ elliptic curves with a point of order 11 over $\mathbb{Q}(\zeta_{11})^+$. We also conclude that $\mathbb{Q}(\zeta_{11})^+$ is the only quintic field K such that there is a positive finite number of elliptic curves with a K-rational point of order 11 and that if K is a number field of degree not divisible by 2, 3 or 5 (as to not contain $\mathbb{Q}(\zeta_{11})^+$) then there are either none or infinitely many elliptic curves with a K-rational point of order 11.

We move on to $X_1(14)$ and the prime 3. The elliptic curve $X_1(14)$ has a Weierstrass model

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

and $X_1(14)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, where all the rational torsion points are cusps. We factor its 9-division polynomial ψ_9 and obtain

$$\psi_9 = \psi_3 f_3 f_6 f_{27},$$

where f_n is an irreducible polynomial of degree n. As in the previous case, the zeroes of ψ_3 do not concern us. From the factorization of ψ_9, we see that there are no points on $X_1(14)$ of order 9 over any number field of degree not divisible by 3. Thus $X_1(14)$ has no non-rational torsion points over any number field of degree not divisible by 2 or 3. Note that points on $X_1(m,n)$ over cubic fields have already been dealt with in [13].

The case $X_1(2,10)$ and the prime 3 remain. The elliptic curve $X_1(2,10)$ has a Weierstrass model

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

and $X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, where all the rational torsion points are cusps. We factor its 9-division polynomial ψ_9 and obtain

$$\psi_9 = \psi_3 f_9 f_{27},$$

where f_n is an irreducible polynomial of degree n. Similarly as in the previous case we can conclude that there are no points on $X_1(2,10)$ of order 9 over any number field of degree not divisible by 9. Thus $X_1(2,10)$ has no non-rational torsion points over any number field of degree not divisible by 2 or 9.

Combining all the cases we have proven Theorem 1. $\qquad\square$

Remark 2. Let α be the root of the polynomial $x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1$ which generates $\mathbb{Q}(\zeta_{11})^+$. The 3 elliptic curves over $\mathbb{Q}(\zeta_{11})^+$ with a point of order 11 are

$$y^2 + \frac{4\alpha^4 - 73\alpha^3 + 150\alpha^2 - 96\alpha + 27}{11}xy + \frac{3\alpha^4 - 19\alpha^3 + 19\alpha^2 - 6\alpha + 1}{11}y =$$

$$= x^3 + \frac{3\alpha^4 - 19\alpha^3 + 19\alpha^2 - 6\alpha + 1}{11}x^2, \tag{6}$$

$$y^2 + \frac{2\alpha^4 - 32\alpha^3 + 68\alpha - 8}{11}xy + \frac{-6\alpha^4 + 111\alpha^3 - 261\alpha^2 + 190\alpha - 33}{11}y =$$

$$= x^3 + \frac{-6\alpha^4 + 111\alpha^3 - 261\alpha^2 + 190\alpha - 33}{11}x^2 \tag{7}$$

and

$$y^2 + \frac{xy}{11}(45\alpha^4 - 799\alpha^3 + 1379\alpha^2 - 372\alpha - 179) + \frac{y}{11}(372\alpha^4 - 6605\alpha^3 +$$

$$11404\alpha^2 - 3157\alpha - 1519) = x^3 + \frac{x^2}{11}(372\alpha^4 - 6605\alpha^3 + 11404\alpha^2 - 3157\alpha - 1519).$$
(8)

The curves (6), (7), (8) have j-invariants $-11 \cdot 131^3$, -2^{15} and -11^2 respectively. The curve (7) has complex multiplication by the ring of integers $\mathbb{Q}(\sqrt{-11})$, while the other two curves do not have complex multiplication. The elliptic curves above were constructed using the formulas from [17].

3 Number of elliptic curves with a cyclic n-isogeny

As we are studying elliptic curves with a cyclic n-isogeny, we are led to the study of the modular curves $X_0(n)$.

If $X_0(n)$ is of genus 0 (when $n \leq 10$, $n = 12$, 13, 16, 18 or 25), then there are already infinitely many elliptic curves with a cyclic n-isogeny over $\mathbb{Q}$.

Let S be the set of n-s such that $X_0(n)$ is of genus 1, i.e.

$$S = \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}.$$
(9)

Note that the Cremona label of $X_0(n)$ is $na1$ and, as listed in Cremona's tables [2], the curves $X_0(n)$ have rank 0 over $\mathbb{Q}$ and hence $|Y_0(n)(\mathbb{Q})|$ is finite for all $n \in S$. The curve $Y_0(n)(\mathbb{Q})$ has 1 point for $n = 19$ and 27, 2 points for $n = 14$ and 17, 3 points for $n = 11$, 4 points for $n = 15$ and 21 and 0 points for the remaining genus 1 cases [11].

To count the number of points on $Y_0(n)$, it will be important to know the number of cusps. For every positive integer $d|n$, $X_0(n)$ has a collection of $\phi(\gcd(d, n/d))$ cusps defined over $\mathbb{Q}(\zeta_{\gcd(d,n/d)})$ [5].

As in the previous section, we will be interested in finding the fields K of prime degree for which the elliptic curve $X_0(n)$ has larger torsion than over $\mathbb{Q}$, but still has rank 0.

We state our results in the following theorem.

Theorem 3. *The only pairs (n, K), where $n \in S$ and K is a number field of prime degree such that $|Y_0(n)(\mathbb{Q})| < |Y_0(n)(K)| < +\infty$ are listed in the table below. The number fields $K = \mathbb{Q}(\alpha)$ are given by the minimal polynomial f of α.*

n	f	$|Y_0(n)(K)|$
11	$x^3 - 13392x - 1080432$	8
14	$x^2 + 7$	8
14	$x^2 + 3$	14
15	$x^2 - 5$	12
15	$x^2 + 1$	12
19	$x^3 - 12096x - 544752$	4
20	$x^2 + 1$	6
21	$x^2 + 3$	12
27	$x^2 + 3$	3
27	$x^3 - 314928$	4
49	$x^2 + 7$	2

Table 2.

Proof. As the general strategy of the proof is similar as the proof of Theorem 1, we will leave some details out. We will not explicitly write the Weierstrass models of $X_0(n)$, but note that they can be found in [19].

The proof will be different for elliptic curves with complex multiplication and those without. We first deal with those without complex multiplication using the same general strategy as in the proof of Theorem 1.

We first deal with the cases when $X_0(n)$ does not have complex multiplication, i.e. $n \in \{11, 14, 15, 17, 19, 20, 21, 24\}$. As in the proof of Theorem 1, for each $X_0(n)$ we compute primes l for which the Galois representation ρ_l is not surjective. We list the obtained results in the table below.

Modular curve	primes l for which ρ_l is not surjective
$X_0(11)$	5
$X_0(14)$	2, 3
$X_0(15)$	2
$X_0(17)$	2
$X_0(19)$	3
$X_0(20)$	2, 3
$X_0(21)$	2
$X_0(24)$	2

Table 3.

First note that if $X_0(n)(\mathbb{Q})$ has no 2-torsion, then $X_0(n)$ gains non-trivial 2-torsion over one cubic field (we count number fields up to isomorphism). This is the field obtained by adjoining a root of $f(x)$, where $y^2 = f(x)$ is a short Weierstrass model for $X_0(n)$. The curves $X_0(n)$ for $n = 11, 19$ and 27 have no 2-torsion and all of them have rank 0 over the cubic field over which they gain 2-torsion.

We now prove that there is no other number field K of prime degree such that $|X_0(11)(\mathbb{Q})| < |X_0(11)(K)| < +\infty$. We factor the 5-division polynomial of

$X_0(11)$ and obtain that $x^2 + x - 29/5$ is the only factor of prime degree, but $X_0(11)(\mathbb{Q}(\sqrt{5})) = X_0(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$.

The 25-division polynomial of $X_0(11)$ has no factors of prime degree, except the ones corresponding to the 5-division polynomial. Thus, we have dealt with $X_0(11)$.

By examining $X_0(14)$ over the number fields generated by the factors of prime degree of the 4-division and 9-division polynomials, we obtain

$$X_0(14)(\mathbb{Q}(\sqrt{-7}))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \text{ and } X_0(14)(\mathbb{Q}(\sqrt{-3}))_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

and $X_0(14)(K)_{tors} = X_0(14)(\mathbb{Q})_{tors}$ for all other fields K of prime degree. We compute that the rank of $X_0(14)$ over both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$ is 0. Thus $Y_0(14)(\mathbb{Q}(\sqrt{-7}))$ has 8 points ($|X_0(14)(\mathbb{Q}(\sqrt{-7}))|$ minus the 4 rational cusps) and $Y_0(14)(\mathbb{Q}(\sqrt{-3}))$ has 14 points.

By examining $X_0(15)$ over the number fields generated by the factors of prime degree of the 8-division polynomial, we obtain

$$X_0(15)(\mathbb{Q}(i))_{tors} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \text{ and } X_0(15)(\mathbb{Q}(\sqrt{5}))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

and $X_0(15)(K)_{tors} = X_0(15)(\mathbb{Q})_{tors}$ for all other fields K of prime degree. We compute that the rank of $X_0(15)$ over both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ is 0. Thus, by removing the 4 rational cusps of $X_0(15)$, we obtain that $Y_0(15)(\mathbb{Q}(i))$ and $Y_0(15)(\mathbb{Q}(\sqrt{5}))$ have 12 points.

We factor the 8-division polynomial of $X_0(17)$ and obtain that the only number field K of prime degree such that $X_0(17)$ has torsion points defined over K, but not over $\mathbb{Q}$, is $K = \mathbb{Q}(i)$. But we compute that the rank of $X_0(17)(\mathbb{Q}(i))$ is 1, and hence there are infinitely many elliptic curves with a cyclic 17-isogeny over $\mathbb{Q}(i)$.

We factor the 9-division polynomial of $X_0(19)$ and obtain as a candidate only the number field $K = \mathbb{Q}(\sqrt{-3})$. But, as in the previous case, the rank of $X_0(19)(\mathbb{Q}(\sqrt{-3}))$ is 1, and hence there are infinitely many elliptic curves with a cyclic 19-isogeny over $\mathbb{Q}(\sqrt{-3})$.

By examining $X_0(20)$ over the number fields generated by the factors of prime degree of the 4-division and 9-division polynomials, we obtain

$$X_0(20)(\mathbb{Q}(i))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

and $X_0(20)(K)_{tors} = X_0(20)(\mathbb{Q})_{tors}$ for all other fields K of prime degree. We compute that the rank of $X_0(20)$ over $\mathbb{Q}(i)$ is 0, and hence $Y_0(20)(\mathbb{Q}(i))$ has 6 points (we subtract the 6 rational cusps of $X_0(20)$).

In a similar manner we obtain that the only field of prime degree K such that $X_0(21)$ has torsion points defined over K, but not over $\mathbb{Q}$, is $K = \mathbb{Q}(\sqrt{-3})$, and that the rank of $X_0(21)(K)$ is 0. Hence $Y_0(21)(\mathbb{Q}(\sqrt{-3}))$ has 12 points (we subtract the 4 rational cusps of $X_0(21)$).

By examining $X_0(24)$ over the number fields generated by the factors of prime degree of the 8-division, we obtain that $X_0(24)(K)_{tors} = X_0(24)(\mathbb{Q})_{tors}$ for all number fields of prime degree.

For the remaining cases $n \in S$, $X_0(n)$ is a curve with complex multiplication, so we cannot apply the same methods as before. Instead we use following theorem which give a good description of the behavior of the torsion of an elliptic curve with complex multiplication defined over $\mathbb{Q}$ upon extensions.

Theorem 4. *[4, Theorem 2] Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ and p an odd prime not dividing D. Let F be a Galois number field not containing K. Then $E(F)[p]$ is trivial.*

We have already shown that $X_0(27)$ gains non-trivial 2-torsion over a cubic field, so by Theorem 4 and from the fact that $X_0(27)(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, we need to check only its 3-division polynomial and 9-division polynomial. The 9-division polynomial gives us no new fields and from the 3-division polynomial we obtain that $X_0(27)(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. However, $X_0(27)$ has 6 cusps over $\mathbb{Q}(\sqrt{-3})$, which gives $|Y_0(27)(\mathbb{Q}(\sqrt{-3}))| = 3$.

To find all the number fields K of prime degree such that $|X_0(32)(\mathbb{Q})| < |X_0(32)(K)| < +\infty$, by Theorem 4, we just need to check the 8-division polynomial of $X_0(32)$ and determine $X_0(32)(\mathbb{Q}(i))$. We obtain that the only field K with the desired property is $K = \mathbb{Q}(i)$, and

$$X_0(32)(\mathbb{Q}(i))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

The curve $X_0(32)$ has 8 cusps over $\mathbb{Q}(i)$, so all of the $\mathbb{Q}(i)$-rational points are cusps.

Similarly, for $X_0(36)$, by Theorem 4, we need to check the 9-division polynomial and $X_0(36)(\mathbb{Q}(\sqrt{-3}))$. The 9-division polynomial gives no new points and we obtain

$$X_0(36)(\mathbb{Q}(\sqrt{-3}))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

and $X_0(36)(K)_{tors} = X_0(36)(\mathbb{Q})_{tors}$ for all other fields K of prime degree. The curve $X_0(36)$ has 12 cusps over $\mathbb{Q}(\sqrt{-3})$, so all of the $\mathbb{Q}(\sqrt{-3})$-rational points are cusps.

Finally, for $X_0(49)$, by Theorem 4, we need to check the 4-division and 7-division polynomials and $X_0(49)(\mathbb{Q}(\sqrt{-7}))$. We obtain

$$X_0(49)(\mathbb{Q}(\sqrt{-7}))_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

and $X_0(49)(K)_{tors} = X_0(49)(\mathbb{Q})_{tors}$ for all other fields K of prime degree. The rank of $X_0(49)(\mathbb{Q}(\sqrt{-7}))$ is 0, and hence $Y_0(49)(\mathbb{Q}(\sqrt{-7}))$ has 2 points. $\qquad\square$

References

[1] A. C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, With an appendix by E. Kani, Canad. Math. Bull. **48** (2005), 16-31.

[2] J. Cremona, Algorithms for modular elliptic curves, Cambridge University Press (1992).

[3] F. Diamond, J. Im, *Modular forms and modular curves*, in V. Kumar Murty (ed.), Seminar on Fermat's last theorem, AMS, Providence, 1997.

[4] L. Dieulefait, E. González-Jiménez, J. Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), 1961-1969.

[5] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II Univ. Antwerp, Antwerp, 1972, pp. 143–316.

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[7] D. Jeon, C.H. Kim, E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.

[8] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), 291–305.

[9] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[10] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1978), 33–186.

[11] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[12] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575.

[13] F. Najman, *Torsion of elliptic curves over cubic fields*, J. Number Theory **132** (2012), 26-36.

[14] F. Najman, *Exceptional elliptic curves over quartic fields*, Int. J. Number Theory, **8** (2012), 1231–1246.

[15] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–311.

[16] W. A. Stein et al., *Sage Mathematics Software (Version 4.7.1)*, The Sage Development Team, 2011, http://www.sagemath.org.

[17] A. Sutherland, *Constructing elliptic curves with prescribed torsion over finite fields*, Math. Comp. **81** (2012), 1131–1147.

[18] L. Washington, Elliptic Curves. Number Theory and Cryptography, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2003.

[19] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ZAGREB,
BIJENIČKA CESTA 30,
10000 ZAGREB, CROATIA
E-mail: fnajman@math.hr