TAMAGAWA NUMBERS OF ELLIPTIC CURVES WITH PRESCRIBED TORSION SUBGROUP OR ISOGENY

ANTONELA TRBOVIĆ

Abstract. We study Tamagawa numbers of elliptic curves with torsion \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \) over cubic fields and of elliptic curves with an \( n \)–isogeny over \( \mathbb{Q} \), for \( n \in \{6, 8, 10, 12, 14, 16, 17, 18, 19, 37, 43, 67, 163\} \). Bruin and Najman \([3]\) proved that every elliptic curve with torsion \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \) over a cubic field is a base change of an elliptic curve defined over \( \mathbb{Q} \). We find that Tamagawa numbers of elliptic curves defined over \( \mathbb{Q} \) with torsion \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \) over a cubic field are always divisible by \( 14^2 \), with each factor 14 coming from a rational prime with split multiplicative reduction of type \( I_{4k} \), one of which is always \( p = 2 \). The only exception is the curve \([1922.e2]\) with \( c_E = c_2 = 14 \). The same curves defined over cubic fields over which they have torsion subgroup \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \) turn out to have the Tamagawa number divisible by \( 14^4 \). As for \( n \)–isogenies, Tamagawa numbers of elliptic curves with an \( 18 \)–isogeny must be divisible by 4, while elliptic curves with an \( n \)–isogeny for the remaining \( n \) from the mentioned set must have Tamagawa numbers divisible by 2, except for finite sets of specified curves.

1. Introduction

Let \( E \) be an elliptic curve over a number field \( K \) and denote by \( \Sigma \) the set of all finite primes of \( K \). For each \( v \in \Sigma \), the completion of \( K \) at \( v \) will be denoted by \( K_v \) and the residue field of \( v \) by \( k_v = \mathcal{O}_{K_v}/(\pi) \), where \( \mathcal{O}_{K_v} \) is the ring of integers of \( K_v \) and \( \pi \) is a uniformizer of \( \mathcal{O}_{K_v} \).

The subgroup \( E_0(K_v) \) of \( E(K_v) \) consists of all the points that reduce modulo \( \pi \) to a non-singular point of \( E(k_v) \). It is known that this group has finite index in \( E(K_v) \) so we can define the Tamagawa number \( c_v \) of \( E \) at \( v \) to be that index, i.e.,

\[
c_v := [E(K_v) : E_0(K_v)].
\]

In light of this, we define the Tamagawa number of \( E \) over \( K \) to be the product \( c_{E/K} := \prod_{v \in \Sigma} c_v \). We will write \( c_E \) instead of \( c_{E/K} \) wherever it does not cause confusion.

It makes sense to study how the value \( c_E \) depends on \( E(K)_{\text{tors}} \), since \( c_E/\#E(K)_{\text{tors}} \) appears as a factor in the leading term of the \( L \)–function of \( E/K \) in the conjecture of Birch and Swinnerton-Dyer (see, for example, \([7\] Conj. F.4.1.6)).

We start with some known results about Tamagawa numbers, first of which is given by Lorenzini in \([13]\) on Tamagawa numbers of elliptic curves defined over \( \mathbb{Q} \) with a specific torsion subgroup.

Proposition 1.1. \([13]\) Proposition 1.1] Let \( E/\mathbb{Q} \) be an elliptic curve with a \( \mathbb{Q} \)–rational point of order \( N \). The following statements hold at most five explicit exceptions for a given \( N \).

(a) If \( N = 4 \), then \( (N/2) \mid c_E \), except for \( E = [X_1(15) \, 15.a4 \, 17.a4] \) and \( [17,a4] \).
(b) If \( N = 5, 6 \) or 12, then \( N \mid c_E \), except for \( E = [X_1(11) \, X_1(14) \, 11.a4 \, 20.a3] \).
(c) If \( N = 10 \), then \( (N^2/2) \mid c_E \).
(d) If \( N = 7, 8 \) or 9, then \( N^2 \mid c_E \), except for \( E = [15.a8 \, 21.a3 \, 26.a2 \, 42.a5 \, 48.a6 \, 54.a2 \, 102.c3] \).

Without exception, \( N \mid c \) if \( N = 7, 8, 9, 10 \) or 12.

He also proved that the smallest possible ratio \( c_E/\#E(K)_{\text{tors}} \) for elliptic curves over \( \mathbb{Q} \) is 1/5, achieved only by the modular curve \( X_1(11) \). He gave as well some results about Tamagawa numbers of elliptic curves over quadratic extensions. Some of his results mentioned in Proposition \([13]\) were later expanded upon by Krumm in \([9]\) which are presented with the following result.

Proposition 1.2. \([9]\) Propositions 5.2.2, 5.2.3] Let \( E/\mathbb{Q} \) be an elliptic curve with a \( \mathbb{Q} \)–rational point of order \( N \).

(a) If \( N = 7 \), then \( 7 \mid c_2 \).
(b) If \( N = 9 \), then \( 9 \mid c_2 \) and \( 3 \mid c_3 \).
Furthermore, Krumm proved some results on Tamagawa numbers of elliptic curves with prescribed torsion over number fields of degree up to 5. He also conjectured that ord_{13}(c_E) is even for all elliptic curves defined over quadratic fields with a point of order 13 and the same conjecture was later proved by Najman in \([15]\). In their recent work \([4]\), Barrios and Roy explicitly classified Tamagawa numbers of elliptic curves defined over \(\mathbb{Q}\) with non-trivial torsion subgroups at primes of additive reduction.

The results mentioned in Propositions \([1.1\text{ and } 1.2]\) were the motivation to explore further the problem of finding Tamagawa numbers of elliptic curves with a certain torsion subgroup and at a certain prime. Bruin and Najman \([3]\) proved that every elliptic curve with torsion isogeny, for \(n\) prime, distinct from 2, at which the reduction is also split multiplicative of type \(I_{44}\). As a consequence of this result we get that elliptic curves defined over a cubic field with torsion subgroup \(Z/2Z \oplus Z/14Z\) have Tamagawa numbers divisible by \(14^3\). We mention the explicit results in the following section.

**Theorem 1.3.**

- Let \(E\) be an elliptic curve defined over \(\mathbb{Q}\) with torsion subgroup \(Z/2Z \oplus Z/14Z\) over a cubic field.
  - (a) The reduction at 2 is split multiplicative of type \(I_{44}\) and \(c_2 = 14k\), where \(k \in \mathbb{Z}\), \(k \geq 1\).
  - (b) There exist at least 2 rational primes with split multiplicative reduction of type \(I_{44}\), where \(k \in \mathbb{Z}\), \(k \geq 1\), one of which is always the prime 2, so \(14^2 \mid c_E\), except for the curve \(1922.e2\), where \(c_E = c_2 = 14\). For each such curve we prove that at \(p = 2\) the reduction is split multiplicative, so \(c_2 = 14k\), and there always exists one more prime, distinct from 2, at which the reduction is also split multiplicative of type \(I_{44}\).

- Let \(E\) be an elliptic curve defined over a cubic field \(K\) with torsion subgroup \(Z/2Z \oplus Z/14Z\). Let \(P\) be a prime of \(K\) over 2. Then the reduction at \(P\) is split multiplicative of type \(I_{44}\) and \(c_P = 14k\), where \(k \in \mathbb{Z}\), \(k \geq 1\). Furthermore, \(14^3 \mid c_E\). The proof of this theorem is given by the proofs of Propositions \([2.2, 2.6\text{ and Corollary 2.4}]\) in Section 2.

The question which naturally appears next is how does the Tamagawa number of an elliptic curve depend on the isogenies of that elliptic curve. In Section 3 we give a series of propositions which gives us our first results about Tamagawa numbers of elliptic curves with prescribed isogeny. For elliptic curves defined over \(\mathbb{Q}\), we were able to prove that if an elliptic curve has an \(N\)-isogeny, then its Tamagawa number is always divisible by 4, and if it has an \(n\)-isogeny, for \(n \in \{6,8,10,12,14,16,17,18,19,37,43,67,163\}\), then it has to be divisible by 2. There are finitely many exceptions for some of these results, all of which we list and give their Tamagawa numbers.

**Theorem 1.4.** Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with an \(N\)-isogeny.

- If \(N = 18\), then \(4c_E\), except for the curves \([14.a2, 14.a5, 14.a1, 14.a4]\) where \(c_E = 2\).
- If \(N = 10\), then \(2c_E\).
- If \(N = 8\), then \(2c_E\), except for the curves \([15.a4, 15.a7, 18.a5]\) where \(c_E = 1\).
- If \(N = 6\), then \(2c_E\), except for the curve \([20.a3]\) where \(c_E = 3\), and also the curves \([80.b3, 80.b1, 20.a1, 27.a4]\) and infinitely many twists of \([27.a4]\) for which \(c_E = 1\).
- If \(n \in \{14,17,19,37,43,67,163\}\), then \(2c_E\).

The proof of this theorem is given by the proofs of Propositions \([3.2, 3.3, 3.4, 3.5\text{ and } 3.7]\) in Section 3. Now let \(E\) be an elliptic curve defined over \(K_v\), given by a Weierstrass equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.
\]

with discriminant \(\Delta\), invariants \(c_4\) and \(c_6\), and \(j\)-invariant \(j_E = \frac{c_4^3}{c_6}\). It will be important for us to distinguish between different types of reductions at finite primes, especially to know when the reduction is multiplicative. For that, we will often use the following well known result.

**Proposition 1.5.** (see \([17, Proposition VII.5.1.b]\)) With the above notation, the curve \(E\) in its minimal model has multiplicative reduction at \(v\) of type \(I_k\) if and only if \(k := ord_v(\Delta) > 0\) and \(ord_v(c_4) = 0\).

As most Tamagawa numbers that we will consider in this paper are coming from primes of multiplicative reduction, it will be important to also distinguish between split and non-split multiplicative reductions and their Tamagawa numbers. One way to do that is by using the algorithm of Tate \([18, Sections 7,8]\) which works in any characteristic of \(k_v\). Going through the algorithm with a specific elliptic curve and a prime \(p\), we get the reduction type at \(p\), its Kodaira symbol and the Tamagawa number.
c_p. It turns out that in the case of split multiplicative reduction I_b we have c_v = k and in the case of non-split multiplicative reduction I_b we have c_v = 1 or c_v = 2, depending on the parity of k, as indicated in Table 1, where we can find all the Tamagawa numbers associated to different reduction types. For distinguishing reduction types in char(k_v) ≠ 2, 3 one can also use the tables in [17, Table 15.1] or [18, Section 6].

| reduction type at v | Kodaira symbol, k ≥ 1 | Tamagawa number at v |
|---------------------|------------------------|----------------------|
| good                | I_0                    | 1                    |
| split multiplicative| I_k                    | k                    |
| non-split multiplicative| I_{2k}                | 2                    |
| non-split multiplicative| I_{2k-1}             | 1                    |
| additive            | II, II*                | 1                    |
| additive            | III, III*              | 2                    |
| additive            | IV, IV*                | 1, 3                 |
| additive            | I_0                    | 1, 2, 4              |
| potentially multiplicative| I_{2k}                | 2, 4                 |
| potentially multiplicative| I_{2k-1}             | 2, 4                 |

Table 1. types of reduction and their Tamagawa numbers

The computations in this paper were executed in the computer algebra system Magma [2]. The code used in this paper can be found at https://web.math.pmf.unizg.hr/~atrpovic/magma/magma3.htm. Many of the proofs in this paper omit the information used in them, such as polynomials of very high degree or with large coefficients, but those can be computed with the given code. For the reader who wants to verify the calculations, we recommend that they go through the proofs and the code simultaneously. All of the specific curves will be mentioned using their LMFDB labels, with a clickable link to the corresponding webpage in [11].

2. TAMAGAWA NUMBERS OF ELLIPTIC CURVES WITH TORSION SUBGROUP $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

As already mentioned, Bruin and Najman [3] proved that every elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field is a base change of an elliptic curve defined over $\mathbb{Q}$. Filip Najman and the author have examined the reduction types at primes with multiplicative reduction of such elliptic curves defined over $\mathbb{Q}$ in [16, Prop. 3.1]. We will examine those primes further, as we want to be able to say more about their Tamagawa numbers. It was proved in [16, Prop. 3.2] that those elliptic curves always have multiplicative reduction of type $I_{14k}$ at the rational prime 2. In this section we are going to prove that the mentioned multiplicative reduction at 2 always has to be split multiplicative, giving the Tamagawa number $c_2 = 14k$, as shown in Table 1. We are also going to prove that there always exists one more prime p, with the exception of the curve [1922,2] at which we have split multiplicative reduction of type $I_{14t}$ and $c_p = 14t$, which means that the Tamagawa number of the elliptic curve contains the factor $14^2$. For the base change of every elliptic curve to a field $K$ over which they have torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ it turns out that their Tamagawa number is always divisible by $14^3$.

Bruin and Najman in [3] also showed that elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ are parameterized with $\mathbb{P}^1(\mathbb{Q})$, so we can write each such curve as $E_u$, for some $u \in \mathbb{Q}$. They also provided a model, which was used for obtaining the results of [16, §3]. We used a different model here, specifically, the one given by Jeon and Schweizer in [8, §2.4], since the one in [16] was dependant on 2 parameters. It did not impose a problem there, since we did not have the need to work with the coefficients of the curve. Even though Jeon and Schweizer do not state that their family consists of all elliptic curves over cubic fields with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, it turns out that it is the case and the reasoning behind it can be found in the accompanying Magma code. Briefly, we compute the isomorphism between different fields of definition of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, those are F and L given in [3] and [8, §2.4], respectively. With that isomorphism we map every curve from the family in [3] and we see that it is isomorphic to one of the curves from the family in [8, §2.4]. Since [3] gives us all of the elliptic curves with needed properties, we see that it suffices to only look at the family from [8, §2.4].

Jeon and Schweizer provided two models for $E_u$, one of which is

$$y^2 + xy = x^3 + A_2(u)x^2 + A_4(u)x + A_6(u),$$

where $u \in \mathbb{Q}$, and the other is

$$y^2 + xy = x^3 + B_2(u)x^2 + B_4(u)x + B_6(u),$$

where $u \in \mathbb{Q}$.
and its short Weierstrass model
\[ y^2 = x^3 + A(u)x + B(u), \]
where we omit \(A_2(u), A_4(u), A_6(u), A(u), B(u)\), since they are very large, but they can be found in the accompanying [Magma code] or in [3 §2.4]. We will be working with the long Weierstrass model when considering the reduction at the prime 2, but generally we will be using the short Weierstrass model, since it is easier to work with.

In Proposition 2.1 we mentioned a way of confirming whether the curve has multiplicative reduction at a finite prime. As already stated, it will be very important to distinguish between split and non-split multiplicative reduction, since the associated Tamagawa numbers are different (see Table I). The following lemma will be useful in differentiating between those, and it is taken directly from a step in Tate’s algorithm.

**Lemma 2.1.** ([13 §7. Case 2]) Let \(E\) be an elliptic curve and let \(p\) be a prime of multiplicative reduction of type \(I_1\) for \(E\). Let \(\text{ord}_p(a_i) > 0\), for \(i = 3, 4, 6, \) and \(\text{ord}_p(b_2) = 0\). If \(T^2 + a_1T - a_2\) splits over \(k_p\), then \(E\) has split multiplicative reduction at \(p\) and \(c_p = 1\).

As a part of the proof of the following proposition we will show that the reduction at the prime 2 is multiplicative of type \(I_{14k}\), which is already proved in [16 Proposition 3.2]. We had to include it here again and could not continue from there because of the already mentioned differences in the models we used.

**Proposition 2.2.** Let \(E\) be an elliptic curve defined over \(\mathbb{Q}\) with torsion subgroup \(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}\) over a cubic field. Then the reduction at 2 is split multiplicative of type \(I_{14k}\) and \(c_2 = 14k\), where \(k \in \mathbb{Z}, k \geq 1\).

**Proof.** From the long Weierstrass model of \(E_n\) from [3 §2.4] we get the associated discriminant
\[ \Delta(u) = \frac{2^{14}(u - 1)^{14}(u + 1)^{14}f_1(u)}{f_2(u)} \]
and the \(c_4\)-invariant \(c_4(u)\), which can be computed with the accompanying [Magma code]. The polynomials \(f_i(u), i = 1, 2\), are monic polynomials in \(\mathbb{Z}[u]\). We will go through all of the possibilities of the prime 2 dividing \(u\) and see that the reduction at 2 in all of those cases is split multiplicative and \(14 \mid c_2\).

1. If \(\text{ord}_2(u) > 0\), we compute \(\text{ord}_2\left(\frac{\Delta(u)}{f_2(u)}\right) = \text{ord}_2(c_4(u)) = 0\) and from Proposition 2.1 we conclude that the reduction at 2 is multiplicative of type \(I_{14}\). We compute \(a_1 = 1\) and \(\text{ord}_2(a_2) > 0\) and since our model satisfies the conditions of Lemma 2.1 we get that \(c_2 = 14\).

2. If \(\ell := \text{ord}_2(u) < 0\), then we make the substitution \(u \mapsto \frac{1}{m}\) so \(\text{ord}_2(m) > 0\), and in the new model we get the discriminant
\[ \Delta(m) = \frac{2^{14}(m - 1)^{14}m^{14}(m + 1)^{14}g_1(m)}{g_2(m)} \]
and the \(c_4\)-invariant \(c_4(m)\), which can be computed with the accompanying [Magma code]. The polynomials \(g_i(m), i = 1, 2\), are monic polynomials in \(\mathbb{Z}[m]\). Using the fact that \(\text{ord}_2(m) > 0\), we compute \(\text{ord}_2\left(\frac{\Delta(m)}{g_2(m)}\right) = \text{ord}_2(c_4(m)) = 0\) and as in the previous case, using Proposition 2.1 and Lemma 2.1 we get that the reduction at 2 is split multiplicative of type \(I_{14(\ell+1)}\) and \(c_2 = 14(\ell+1)\).

3. If \(\text{ord}_2(u) = 0\), then \(\ell := \text{ord}_2(u - 1) > 0\). After the substitution \(u - 1 \mapsto m\) we have \(\ell = \text{ord}_2(m) > 0\), the discriminant
\[ \Delta(m) = \frac{2^{14}m^{14}(m + 2)^{14}h_1(m)}{h_2(m)} \]
and the \(c_4\)-invariant \(c_4(m)\), which can be computed with the accompanying [Magma code]. The polynomials \(h_i(m), i = 1, 2\), are monic polynomials in \(\mathbb{Z}[m]\). We can divide both the numerator and the denominator of \(\Delta(m)\) by \(2^{48}\) and we get that \(\text{ord}_2(\Delta(m)) = 14(\ell - 1)\) and if we divide the numerator and the denominator of \(c_4(m)\) by \(2^{24}\) we get that \(\text{ord}_2(c_4(m)) = 0\). So if \(\ell > 1\), by Proposition 2.1 we have that the reduction at 2 is multiplicative of type \(I_{14(\ell - 1)}\). We compute \(a_1 = 1\) and \(\text{ord}_2(a_2) > 0\) (after dividing both numerator and the denominator by \(2^{12}\)) and since our model satisfies the conditions of Lemma 2.1 we get that \(c_2 = 14(\ell - 1)\).

Obviously we have to look at the case \(\ell = 1\) separately. This means that \(u = 2n + 1\), where \(\text{ord}_2(n) = 0\). After the substitution \(u \mapsto 2n + 1\) we have the discriminant
\[ \Delta(n) = \frac{n^{14}(n + 1)^{14}p_1(n)}{p_2(n)} \]
and the $c_4$–invariant $c_4(n)$, which can be computed with the accompanying Magma code. The polynomials $p_i(n)$, $i = 1, 2$, are monic polynomials in $\mathbb{Z}[n]$. Since $\text{ord}_2(n) = 0$, we have $t := \text{ord}_2(n + 1) > 0$ and $\text{ord}_2(p_i(n)) = 0$, for each $i$, so $\text{ord}_2(\Delta(n)) = 14t$ and $\text{ord}_2(c_4(n)) = 0$. By Proposition 1.4 we see that the reduction at 2 is multiplicative of type $I_{4k}$ and similarly as in previous cases, Lemma 2.4 gives that the reduction is split multiplicative with $c_2 = 14t$.

\[\Box\]

Example 2.3. As it was verified in part (1) of the proof of Proposition 2.2, if $\text{ord}_2(u) > 0$, then the reduction at 2 is multiplicative of type $I_{14}$ with $c_2 = 14$. This allows us to generate an infinite family of elliptic curves that have torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field and Tamagawa number exactly 14 at the prime 2, i.e., $c_2 = 14$. Namely, if we put $u = 2^k$, for any $k \in \mathbb{Z}$, $k \geq 1$, in the long Weierstrass model of $E_u$ from $[8$, §2.4] we get an elliptic curve with $c_2 = 14$. For example, with $k = 1$ (which gives $u = 2$) we get a curve whose minimal model is defined by

$$y^2 + xy = x^3 - 31714388875x + 2132064170125553,$$

with $c_2 = 14$ and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over the field $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $3x^3 - 4x^2 - 27x + 4$.

In a similar manner, part (2) of the proof of Proposition 2.2 allows us to generate an infinite family of examples of elliptic curves that have torsion curves that have torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field and Tamagawa number $c_2 = 14t$, where $t > 1$. When $k := \text{ord}_2(u) < 0$, the long Weierstrass model of $E_u$ from $[8, §2.4]$ gives us an elliptic curve with $c_2 = 14(k + 1)$ and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field. Namely, if we specify $u = \frac{1}{2^k}$, $k \geq 1$, we get a family of elliptic curves with Tamagawa number $c_2 = 14(k + 1)$. For example, with $k = 1$ (which gives $u = \frac{1}{4}$) we get a curve whose minimal model is defined by

$$y^2 + xy = x^3 - 35365397163613670x + 2559848051274532647229668,$$

with $c_2 = 28$ and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over the field $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $-6x^3 - 47x^2 + 54x + 47$.

All of the statements regarding specific elliptic curves in this example can be verified using the accompanying Magma code.

Corollary 2.4. Let $E$ be an elliptic curve defined over a cubic field $K$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. Let $\mathfrak{P}$ be a prime of $K$ over 2. Then the reduction at $\mathfrak{P}$ is split multiplicative of type $I_{14k}$ and $c_{\mathfrak{P}} = 14k$, where $k \in \mathbb{Z}$, $k \geq 1$. Furthermore, $14^3 \mid c_E$.

Proof. Recall that $E$ is an elliptic curve defined over $\mathbb{Q}$. We will denote by $E_K$ the base change of $E$ to $K$. From $[16$, Proposition 3.6$]$ we know that 2 splits completely in $K$, i.e., $2O_K = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3$. This means that the residue field $k_{\mathfrak{P}_i} = O_K/\mathfrak{P}_i$, where $\mathfrak{P}_i$, is a prime lying over 2, $i = 1, 2, 3$, is isomorphic to $k_2$. For each $\mathfrak{P}_i$, we have that $E_K \mod \mathfrak{P}_i = E \mod 2$ and hence $c_{\mathfrak{P}_i} = c_2 = 14k$, for $i = 1, 2, 3$, where $k \in \mathbb{Z}$, $k \geq 1$.

In the following proposition we will deal with primes distinct from 2, for which we have a simpler way of determining split multiplicative reduction than going through Tate’s algorithm as we did in Proposition 2.2.

Lemma 2.5. ([1, Lemma 2.2]) Let $p \neq 2$ be a prime and let $E$ be an elliptic curve defined over $\mathbb{Q}_p$ with multiplicative reduction at $p$. The reduction is split multiplicative if and only if $-c_4$ is a square in $\mathbb{F}_p^\times$.

Proposition 2.6. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field. Then there exist at least 2 rational primes with split multiplicative reduction of type $I_{14k}$, where $k \in \mathbb{Z}$, $k \geq 1$, one of which is always the prime 2, so $14^2 \mid c_E$, except for the curve $[19, 2, 22]$ where $c_{10} = c_2 = 14$.

Proof. In Proposition 2.2 we have already seen that the reduction at 2 is split multiplicative of type $I_{14k}$ and therefore $c_2 = 14k$. It remains to prove that there exists one more prime with the same property for each of those curves.

From the short Weierstrass model of $E_u$ from $[8, §2.4]$ we get the associated discriminant

$$\Delta(u) = 2^{14}(u - 1)^{14}(u + 1)^{14}f(u)$$

and the $c_4$–invariant $c_4(u)$, which can be computed with the accompanying Magma code. The polynomial $f(u)$ is a monic polynomial in $\mathbb{Z}[u]$. The
Assume that there exists a prime $p$ such that $k := \text{ord}_p(u - 1) > 0$. Let $\text{res}(q, r)$ denote the resultant of two arbitrary polynomials $q$ and $r$. We compute

$$\text{res}\left(u - 1, -\frac{\Delta(u)}{(u - 1)^2}\right) = 2^{82},$$

$$\text{res}\left(u - 1, c_4(u)\right) = 2^{32}.$$

For $p \neq 2$ this means that $p^{14k} | \Delta(u)$ and $p \nmid c_4(u)$ and from Proposition 1.5 we find that the reduction of $E$ at $p$ is multiplicative of type $I_{14k}$. We want to see that $c_p = 14k$, i.e., that the reduction at $p$ is split multiplicative. According to Lemma 2.3 it will suffice to check the value of $-c_0$ modulo $p$. Having in mind that $u \equiv 1 \pmod{p}$, we compute that $-c_0 \equiv 2^{48} \pmod{p}$, which is a square mod $p$.

Assume now that there exists a prime $p$ such that $k := \text{ord}_p(u - 1) < 0$. We put $m := \frac{1}{u^\tau}$ so $\text{ord}_p(m) = k > 0$ and we get an elliptic curve with the discriminant

$$\Delta(m) = \frac{1}{27}m^{14}(m + 1/2)^{14}g(m)$$

and the $c_4$-invariant $c_4(m)$, which can be computed with the accompanying Magma code. The polynomial $g(m)$, $i = 1, 2$, is a monic polynomial in $\mathbb{Z}[u]$. We compute

$$\text{res}\left(m, -\frac{\Delta(m)}{m^{1/2}}\right) = 2^{-82},$$

$$\text{res}\left(m, c_4(m)\right) = 2^{-32}.$$

For $p \neq 2$ this means that $p^{14k} | \Delta(m)$ and $p \nmid c_4(m)$ and from Proposition 1.5 we find that the reduction of $E$ at $p$ is multiplicative of type $I_{14k}$. Having in mind that $m \equiv 0 \pmod{p}$, we get that $-c_0 \equiv 2^{-48} \pmod{p}$, which is a square mod $p$, so by Lemma 2.3 we have $c_p = 14k$.

So far we have proved that if we have a prime $p \neq 2$ and $k := \text{ord}_p(u - 1) \neq 0$, then we have split multiplicative reduction at $p$ with $c_p = 14[k]$. We have several possibilities when $\text{ord}_p(u - 1) = 0$ and those are $u - 1 = 0$ or $u - 1 = \pm 2^k$, $k \in \mathbb{Z}$.

When $u - 1 = \pm 2^k$, $k \neq 0, 1$, then $\text{ord}_p(u + 1) > 0$, for some prime $p \neq 2$. In the cases $u - 1 = \pm 2^k$, $k = 0, 1$, or $u - 1 = 0$ we get that $u \in \{0, \pm 1, 3\}$. For $u = \pm 1$ we get a singular curve and for $u \in \{0, 3\}$ we get the same curve, $1922.c2$, with $c_E = c_2 = 14$.

Therefore, if we have a curve distinct from $1922.c2$, it certainly has a prime $p$ such that $\text{ord}_p(u - 1) \neq 0$ or $\text{ord}_p(u + 1) > 0$. It remains to see what happens in the case $\text{ord}_p(u + 1) > 0$.

Assume that there exists a prime $p$ such that $k := \text{ord}_p(u + 1) > 0$. We compute

$$\text{res}\left(u + 1, -\frac{\Delta(u)}{(u + 1)^2}\right) = 2^{82},$$

$$\text{res}\left(u + 1, c_4(u)\right) = 2^{32}.$$

For $p \neq 2$ this means that $p^{14k} | \Delta(u)$ and $p \nmid c_4(u)$ and from Proposition 1.5 we find that the reduction of $E$ at $p$ is multiplicative of type $I_{14k}$. Having in mind that $u \equiv -1 \pmod{p}$, we get that $-c_0 \equiv 2^{48} \pmod{p}$, which is a square mod $p$, so by Lemma 2.3 we have $c_p = 14k$.

\[\square\]

Remark 1. In Proposition 2.3 we proved that $c_E = 14$ is the least possible value of the Tamagawa number of an elliptic curve defined over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over some cubic field. This is true only for elliptic curve $E = 1922.c2$. Consequently, for the same curve we get the least possible value amongst those curves of the ratio $c_E/\#E(\mathbb{Q})_{\text{tors}}$ which appears as a factor in the leading term of the $L$-function of $E/\mathbb{Q}$ in the conjecture of Birch and Swinnerton-Dyer, in this case it is $c_E/\#E(\mathbb{Q})_{\text{tors}} = \frac{14}{1} = 14$, since the curves defined over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over some cubic field have trivial torsion over $\mathbb{Q}$.

Similarly, using Corollary 2.3 we see that the value of the Tamagawa number of an elliptic curve defined over a cubic field with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ is always divisible by $14^3$. The value $c_E = 14^3$ is actually a possible value, and it is achieved for the curve $E = 1922.c2$, which has the mentioned torsion over the cubic field $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $x^3 + 2x^2 - 9x - 2$. This gives the smallest possible ratio of $c_E/\#E(K)_{\text{tors}} = 98$ for all such curves.
3. Tamagawa numbers of elliptic curves with prescribed isogeny

In [13] Table 3] we can find the $j$–invariants of elliptic curves parameterized by points on modular curves $X_0(n)$ defined over $\mathbb{Q}$, for $X_0(n)$ of genus 0, and in [13] Table 4] there are $j$–invariants of elliptic curves parameterized by points on modular curves $X_0(n)$ defined over $\mathbb{Q}$, with genus of $X_0(n)$ larger than 0. In this section we will examine the properties of Tamagawa numbers of elliptic curves defined over $\mathbb{Q}$ with an $n$–isogeny, i.e., the properties of Tamagawa numbers of elliptic curves obtained from the mentioned $j$–invariants.

In Section 2 we worked with a specific model for the curve $X_1(2,14)$. However, the points on $X_0(n)$ give us $j$–invariants of curves with an $n$–isogeny, which give us elliptic curves up to a twist, so now, as opposed to the situation in Section 2, we also have to take into consideration the twists of the curves we get from those $j$–invariants. Therefore, we will be interested in how the reduction types at primes $p \in \mathbb{Q}$ change under the twisting of the curve.

Let $E$ be an elliptic curve, which will always be defined over $\mathbb{Q}$ in this section. Denote by $E^d$ its quadratic twist by $d$, where $d$ is a squarefree integer. When $p \neq 2$, the reduction type change is quite straightforward, and is presented in Table 2. In essence, if $p \nmid d$, the reduction type does not change, and when $p | d$, reduction types change as indicated in the third column.

| reduction type of $E$ at $p$ | reduction type of $E^d$ at $p \nmid d$ | reduction type of $E^d$ at $p | d$ |
|-----------------------------|---------------------------------|---------------------------------|
| $I_0$                       | $I_0$                           | $I_0^*$                         |
| $I_m$                       | $I_m$                           | $I_m^*$                         |
| $II$                        | $II$                            | $IV^*$                          |
| $III$                       | $III$                           | $III^*$                         |
| $IV$                        | $IV$                            | $II^*$                          |
| $I_0^*$                     | $I_0^*$                         | $I_0$                           |
| $I_m^*$                     | $I_m^*$                         | $I_m$                           |
| $IV^*$                      | $IV^*$                          | $II$                            |
| $III^*$                     | $III^*$                         | $III$                           |
| $II^*$                      | $II^*$                          | $IV$                            |

Table 2. change of reduction types at $p \neq 2$ under twisting [5 Prop.1]

When $p = 2$, the situation gets more complicated. As most of the relevant Tamagawa numbers we will have in the following proofs come from primes of multiplicative reduction, we give a lemma that will be especially useful for dealing with quadratic twists of a large family of elliptic curves with multiplicative reduction at $p = 2$.

**Lemma 3.1.** ([6 Thm.A.5], [12 Thm.2.8]) Let $E$ be an elliptic curve with multiplicative reduction of type $I_n$ at $p = 2$. Denote by $E^d$ the twist of $E$ by $d$, where $d$ is a squarefree integer.

(a) If $d \equiv 2,3 \pmod{4}$, then the reduction of $E^d$ at $p$ is of type $I_n^*$.  
(b) If $d \equiv 1 \pmod{4}$, then the reduction of $E^d$ at $p$ is of type $I_n$.

For other types of reduction, some results can also be found in [5 Section 2]. Since we will deal here with only finitely many explicitly known elliptic curves with non-multiplicative reduction at $p = 2$, for those curves we can simply check all of the possibilities for reduction type at $p = 2$ of quadratic twists, since $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 = \langle -1,2,5 \rangle$.

**Proposition 3.2.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with an $18$–isogeny. Then $4|c_E$, except for the curves [14a214a514a114a4] where $c_E = 2$.

**Proof.** From [14 Table 3] we take the parameterization of the $j$–invariants of the curves that are non-cuspidal points on $X_0(18)$,

$$j(h) = \frac{(h^3 - 2)^3(h^9 - 6h^6 - 12h^3 - 8)^3}{h^6(h^3 - 8)(h^3 + 1)^2}, h \in \mathbb{Q}.$$  

From it we can acquire the discriminant

$$\Delta(h) = (h - 2)h^9(h + 1)^2(h^2 - h + 1)^2(h^2 + 2h + 4)f(h)$$
and the $c_4$–invariant $c_4(h)$ of the minimal model up to a twist, which can be computed with the accompanying [Magma code]. The polynomial $f(h)$ is a monic polynomial in $\mathbb{Z}[h]$.

Assume that there exists a prime $p$ such that $k := \text{ord}_p(h + 1) > 0$. We compute

$$\text{res}(h + 1, \frac{\Delta(h)}{(h + 1)^2}) = 3^{34},$$

$$\text{res}(h + 1, c_4(h)) = 3^{12}.$$

If $p \neq 3$, this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, so from Proposition [14.45] we find that the reduction of $E$ at $p$ is multiplicative of type $I_{2k}$, and therefore $c_4$ is even (see Table [1]). If there exists a second prime $p'$ distinct from $p$ and $3$ with $k' := \text{ord}_{p'}(h + 1) > 0$, then we have another prime with multiplicative reduction of type $I_{2k'}$ and therefore with even $c_{p'}$.

Assume now that there exists a prime $p$ such that $k := \text{ord}_p(h + 1) < 0$. We put $m := \frac{h + 1}{k}$ and after the substitution $x \mapsto x \cdot 3^{-6}, y \mapsto y \cdot 3^{-9}$ we get an elliptic curve with the discriminant

$$\Delta(m) = (m - 1)^9(3m - 1)m^{18}(3m^2 - 3m + 1)^2(3m^2 + 1)g(m)$$

and the $c_4$–invariant $c_4(h)$ up to a twist, which can be computed with the accompanying [Magma code]. The polynomial $g(m)$ is a monic polynomial in $\mathbb{Z}[m]$.

We compute

$$\text{res}\left( m, \frac{\Delta(m)}{m^{18}} \right) = 1,$$

$$\text{res}\left( m, c_4(m) \right) = 1.$$

We see from Proposition [14.45] that the reduction at $p$ is multiplicative of type $I_{18k}$, with even $c_p$ (see Table [1]). If we have another prime $p' \neq p$ with $k' := \text{ord}_{p'}(h + 1) < 0$, then the reduction at $p'$ is also multiplicative of type $I_{18k}$ with even $c_{p'}$.

Assume now that there exists at most one prime $p$ such that $\text{ord}_p(h + 1) \neq 0$. That means that either $h + 1 = \pm p^k$, where $k \in \mathbb{Z}$, $k \geq 0$, or $m = \frac{1}{k + 1} = \pm p^k$, where $k \in \mathbb{Z}$, $k > 0$. We consider the following cases:

(1) If $h + 1 = \pm p^k$, $p \neq 3$, we have $\text{ord}_p(h^2 - h + 1) = 0$, since $\text{res}(h + 1, h^2 - h + 1) = 3$, where $h^2 - h + 1$ is one of the factors in the discriminant. Then there exists $p' \neq p, 3$ such that $\text{ord}_{p'}(h^2 - h + 1) > 0$, unless we have $h^2 - h + 1 \in \{\pm 1, \pm 3\}$, i.e., $h \in \{0, \pm 1, 2\}$. For $h = 1$ we get a twist of the curve [14.45] which has $c_E = 2$, while for $h = 0, -1, 2$ we do not get an elliptic curve (look at the $j$-invariant).

(2) Suppose $h + 1 = \pm 3^k$. If $k = 0$ we have $h + 1 = \pm 1$, i.e., $h \in \{0, -2\}$. We already know that $h$ cannot be $0$, but for $h = -2$ we get a twist of the curve [14.44] for which we have $c_E = 2$. When $k = 1$ we have $h + 1 = \pm 3$, i.e., $h \in \{-4, 2\}$. For $h = -4$ we get a twist of [14.41] with $c_E = 2$, and $h = 2$ cannot happen. Assume now that $h + 1 = \pm 3^k, k > 1$. Counting the multiplicities of $3$ in $\Delta(h)$ and $c_4(h)$ we get that the factor $3^{2k - 2k'}$ appears in the $j$-invariant. Furthermore, if we write $\pm 3^k - 1$ instead of $h$ in the equation for $E$ and make the substitution $x \mapsto x \cdot 3^6, y \mapsto y \cdot 3^9$, we get a model where $\text{ord}_3(c_4) = 0$, and it follows from Proposition [14.25] that for $k > 1$ we have multiplicative reduction $I_{2k-2}$ at $3$, with $c_3$ being even (see Table [1]). Note that in any case we also have a prime $p \neq 3$ dividing $h^2 - h + 1$ in $\Delta(h)$ with multiplicative reduction $I_{2n}$, which makes $c_E$ divisible by 4.

(3) If $m = \frac{h}{k + 1} = \pm p^k$, for some prime $p$, and clearly $\text{ord}_p(3m^2 - 3m + 1) = 0$, since $\text{res}(m, 3m^2 - 3m + 1) = 1$. Then there exists $p' \neq p$ such that $\text{ord}_{p'}(3m^2 - 3m + 1) > 0$. Otherwise, we have $3m^2 - 3m + 1 \in \{\pm 1\}$, i.e., $m \in \{0, 1\}$ which only makes sense for $h = 0$ but, as noted earlier, $h$ cannot be 0.

The only thing left to consider is when we have only 2 primes with $\text{ord}_p(h + 1) \neq 0$, one of which is 3 and divides the numerator; in other words the cases $h + 1 = \pm 3^k p^l$ and $h + 1 = \pm \frac{3}{p}, p \neq 3, k, l > 0$. From the reasoning in (2) above, it is clear that if $k > 1$, we have multiplicative reduction at 3 and from the part of the proof where we had $\text{ord}_p(h + 1) < 0$ we see that the reduction is multiplicative at $p$ as well, which gives us $c_E$ that is divisible by 4. For $k = 1$, we have $h + 1 = \pm 3p^l$ or $h + 1 = \pm \frac{3}{p}$.

- If $h + 1 = \pm 3p^l$, we have another prime $p' \neq p, 3$ dividing $h^2 - h + 1$ in the discriminant (similarly as in (1)) with multiplicative reduction.
- If $h + 1 = \frac{3}{p} = \pm \frac{3}{p}$, we also have another prime $p' \neq p$ dividing the numerator of $3m^2 - 3m + 1$ in the discriminant (as in (3)) with multiplicative reduction, except possibly when $3m^2 - 3m + 1 = \ldots$
For the proof above come from multiplicative reductions \( III \), \( E \) curve, and for the values \( c \) we compute \( p \) if \( c \) and the \( \Delta(h) \) we see by Proposition 1.5 that the reduction at \( p \) when \( c \) and \( \Delta(h) \) we get a twist of the elliptic curve \( 14.a2 \) with \( c_E = 2 \), and for \( h = -\frac{1}{2} \) we get a curve that already has 2 primes of reduction type \( I_{2k} \), namely 2 and 13.

To prove the proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions \( I_{2n} \) at primes \( p \), so by using Table 1 Table 2 and Lemma 3.1, we conclude that all reduction types of twists at \( p \) are either \( I_{2n} \) or \( I_{2n}^* \), so the Tamagawa numbers stay even.

As for the curves \( 14.a2, 14.a5, 14.a1 \) and \( 14.a4 \), they have \( c_E = 2 \). By using the fact that \( \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = (-1, 2, 5) \), we explicitly compute all possible reduction types of quadratic twists at \( p \) and conclude that for every twist of those curves \( 4 \mid c_E \).

Proposition 3.3. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) with a 10−isogeny. Then \( 2|c_E \).

Proof. From [14] Table 3 we take the parameterization of the \( j \)−invariants of the curves that are noncuspidal points on \( X_0(10) \),

\[
j(h) = \frac{(h^6 - 4h^5 + 16h + 16)^3}{(h + 1)^2(h - 4)h^5}, h \in \mathbb{Q}.
\]

From it we can acquire the discriminant

\[
\Delta(h) = (h - 4)h^5(h + 1)^3(h^2 - 2h - 4)^6(h^2 - 2h + 2)^6f(h)
\]

and the \( c_4 \)−invariant \( c_4(h) \) up to a twist, which can be computed with the accompanying Magma code.

The polynomial \( f(h) \) is a monic polynomial in \( \mathbb{Z}[h] \).

Assume that there exists a prime \( p \) such that \( k := \text{ord}_p(h + 1) > 0 \). We compute

\[
\text{res}\left(h + 1, \frac{\Delta(h)}{(h + 1)^2}\right) = 5^{22},
\]

\[
\text{res}(h + 1, c_4(h)) = 5^8.
\]

If \( p \neq 5 \), this means that \( p^{2k} \mid \Delta(h) \) and \( p \nmid c_4(h) \), and we find from Proposition 1.5 that the reduction of \( E \) at \( p \) is multiplicative of type \( I_{2k} \), and therefore \( c_p \) is even (see Table 1).

For the case \( h + 1 = \pm 5^k \), after the change of variables \( x \mapsto x \cdot 5^4, y \mapsto y \cdot 5^6 \), counting the multiplicities of 5 in \( \Delta(h) \) and \( c_4(h) \) we get that the factor \( 5^{2k} \cdot 2^{k} \) appears in the \( j \)−invariant, with \( 5 \nmid c_4(h) \). Therefore, when \( k > 1 \), by Proposition 1.5 we have multiplicative reduction at 5 of type \( I_{2k-2} \), with even \( c_p \) (see Table 1). For \( k \in \{0, 1\} \) we have \( h \in \{-6, -2, 0, 4\} \). For the values \( h \in \{-6, -2\} \) we do not have an elliptic curve, and for the values \( h \in \{-6, -2\} \) we get twists of curves \( 768.h1 \) and \( 768.h3 \), which have \( c_E = 2 \), both with bad prime 2 with reduction type \( II \), so \( c_2 = 2 \).

Assume now that there exists a prime \( p \) such that \( k := \text{ord}_p(h + 1) < 0 \). We put \( m := \frac{1}{h + 1} \) and after the substitution \( x \mapsto x \cdot 5^{-4}, y \mapsto y \cdot 5^{-6} \) we get an elliptic curve with the discriminant

\[
\Delta(m) = (m - 1)^5(5m - 1)^m(5m^2 - 2m + 1)^6(5m^2 - 2m + 1)^6g(m)
\]

and the \( c_4 \)−invariant \( c_4(m) \) up to a twist, which can be computed with the accompanying Magma code.

The polynomial \( g(m) \) is a monic polynomial in \( \mathbb{Z}[m] \).

We compute

\[
\text{res}\left(m, \frac{\Delta(m)}{m^{10}}\right) = 1,
\]

\[
\text{res}(m, c_4(m)) = 1.
\]

We see by Proposition 1.5 that the reduction at \( p \) is multiplicative of type \( I_{10k} \), with even \( c_p \) (see Table 1).

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions \( I_{2n} \) at primes \( p \), so by using Table 1 Table 2 and Lemma 3.1, we conclude that all reduction types of twists at \( p \) are either \( I_{2n} \) or \( I_{2n}^* \), so the Tamagawa numbers stay even.
Proposition 3.4. Let \( R \) be an elliptic curve over \( \mathbb{Q} \) with an \( 8 \)-isogeny. Then \( 2 | c_E \), except for the curves 15.a4, 15.a7, 48.a5, where \( c_E = 1 \).

Proof. From \cite{14} Table 3 we take the parameterization of the cuspidal points on \( X_0(8) \),

\[
j(h) = \frac{(h^4 - 16h^2 + 16)^3}{(h^2 - 16)h^2}, \quad h \in \mathbb{Q}.
\]

From it we can acquire the discriminant

\[
\Delta(h) = (h - 4)h^2(h + 4)f(h)
\]

and the \( c_4 \)-invariant \( c_4(h) \) up to a twist, which can be computed with the accompanying Magma code.

The polynomial \( f(h) \) is a monic polynomial in \( \mathbb{Z}[h] \).

Assume that there exists a prime \( p \) such that \( k := \text{ord}_p(h) > 0 \). We compute

\[
\text{res} \left( h, \frac{\Delta(h)}{h^2} \right) = 2^{64},
\]

\[
\text{res} \left( h, c_4(h) \right) = 2^{24}.
\]

If \( p \neq 2 \), then this means that \( p^{2k} | \Delta(h) \) and \( p \nmid c_4(h) \), and from Proposition 1.5 we find that the reduction of \( E \) at \( p \) is multiplicative of type \( I_{2k} \), and therefore \( c_p \) is even (see Table 1).

For the case \( h = \pm 2^k \), after the change of variables \( x \mapsto x \cdot 2^{12}, y \mapsto y \cdot 2^{18} \), counting the multiplicities of 2 in \( \Delta(h) \) and \( c_4(h) \) we get that the factor \( 2^{n-2k} \) appears in the \( j \)-invariant, with \( 2 \nmid c_4(h) \). Therefore, when \( k > 4 \), we have multiplicative reduction at 2 of type \( I_{2k-8} \) with even \( c_p \), by Proposition 1.5 and Table 1. For \( k = 0 \) we have \( h = \pm 1 \) and for the both values we get a twist of the curve 15.a7 with \( c_E = 1 \). For \( k = 1 \) we have \( h = \pm 2, \) i.e., a curve 48.a5 up to a twist, with \( c_E = 1 \). When \( k = 2 \) we do not get a curve and, for \( k = 3 \) and \( h = \pm 8 \) we have a twist of 24.a2, where \( c_E = 2 \), and finally for \( k = 4 \) and \( h = \pm 16 \) we have a twist of 15.a4, where \( c_E = 1 \).

Assume now that there exists a prime \( p \) such that \( k := \text{ord}_p(h) < 0 \). We put \( m := \frac{1}{k} \) and after the substitution \( x \mapsto x \cdot 2^{-12}, y \mapsto y \cdot 2^{-18} \) we get an elliptic curve with the discriminant

\[
\Delta(m) = -(4m - 1)m^6(4m + 1)g(m)
\]

and the \( c_4 \)-invariant \( c_4(m) \) up to a twist, which can be computed with the accompanying Magma code.

The polynomial \( g(m) \) is a monic polynomial in \( \mathbb{Z}[m] \).

We compute

\[
\text{res} \left( m, \frac{\Delta(m)}{m^6} \right) = 1,
\]

\[
\text{res} \left( m, c_4(m) \right) = 1.
\]

We see from Proposition 1.5 and Table 1 that the reduction at \( p \) is multiplicative of type \( I_{8k} \), with even \( c_p \).

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions \( I_{2n} \) at primes \( p \), so by using Table 1 Table 2 and Lemma 1.4, we conclude that all reduction types of twists at \( p \) are either \( I_{2n} \) or \( I_{2n}^* \), so the Tamagawa numbers stay even.

As for the curves 15.a4, 15.a7 and 48.a5 they have \( c_E = 1 \). By using the fact that \( \mathbb{Q}_p^* / (\mathbb{Q}_p^*)^2 = (-1, 2, 5) \), we explicitly compute all possible reduction types of quadratic twists at \( p = 2 \) and conclude that for every twist of those curves \( 2 \nmid c_E \). Lastly, for every twist of the curve 24.a2 we have \( 2 \nmid c_E \).

Proposition 3.5. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) with a 6-isogeny. Then \( 2 | c_E \), except for the curve 20.a3, where \( c_E = 3 \), and also the curves 80.b3, 80.b1, 20.a1, 27.a4 and infinitely many twists of 27.a4, for which \( c_E = 1 \).
Proof. From [14, Table 3] we take the parameterization of the $j$–invariants of the curves that are non-cuspidal points on $X_0(6)$,

$$j(h) = \frac{(h + 6)^3(h^3 + 18h^2 + 84h + 24)^3}{h(h + 8)(h + 9)^2}, h \in \mathbb{Q}.$$ 

From it we can acquire the discriminant

$$\Delta(h) = h(h + 6)^6(h + 8)^3(h + 9)^2 f(h),$$

and the $c_4$–invariant $c_4(h)$ up to a twist, which can be computed with the accompanying [Magma code].

The polynomial $f(h)$ is a monic polynomial in $\mathbb{Z}[h]$.

Assume that there exists a prime $p$ such that $k := \text{ord}_p(h + 9) > 0$. We compute

$$\text{res}(h + 9, \frac{\Delta(h)}{(h + 9)^2}) = 3^{32},$$

$$\text{res}(h + 9, c_4(h)) = 3^{12}.$$

If $p \neq 3$, this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, and from Proposition [1.6] we find that the reduction of $E$ at $p$ is multiplicative of type $I_{2k}$, and therefore $c_p$ is even (see Table [1]).

For the case $h + 9 = \pm 3^k$, after the change of variables $x \mapsto x \cdot 3^k, y \mapsto y \cdot 3^k$, counting the multiplicities of $3$ in $\Delta(h)$ and $c_4(h)$ we get that the factor $3^{3–2k}$ appears in the $j$–invariant, with $3 \nmid c_4(h)$. Therefore, when $k > 2$, we have multiplicative reduction at $3$ of type $I_{2k–4}$ with even $c_p$, by Proposition [1.6] and Table [1]. For $k = 0$ we have $h \in \{-10, -8\}$. With $h = -10$ we have a twist of the elliptic curve $20.a3$ which has $c_E = 3$, coming from the reduction at 2 of type $IV$, and $h = -8$ does not give us an elliptic curve. For $k = 1$ we have $h \in \{-12, -6\}$. For $h = -12$ we get the curve $36.a2$ with $c_E = 6$ and for $h = -6$ we have $27.a4$, where $c_E = 1$. Lastly, if $k = 2$, then $h \in \{-18, 0\}$. For $h = 0$ we do not get an elliptic curve, but for $h = -18$ we get a twist of the curve $80.b1$ with $c_E = 1$.

Assume now that there exists a prime $p$ such that $k := \text{ord}_p(h + 9) < 0$. We put $m := \frac{1}{p^{k+9}}$ and after the substitution $x \mapsto x \cdot 3^{-6}, y \mapsto y \cdot 3^{-9}$ we get an elliptic curve with the discriminant

$$\Delta(m) = (m – 1)^3(3m – 1)^6(9m – 1)^9g(m)$$

and the $c_4$–invariant $c_4(m)$ up to a twist, which can be computed with the accompanying [Magma code].

The polynomial $g(m)$ is a monic polynomial in $\mathbb{Z}[m]$.

We compute

$$\text{res}(m, \frac{\Delta(m)}{m^6}) = 1,$$

$$\text{res}(m, c_4(m)) = 1.$$ 

We see that the reduction at $p$ is multiplicative of type $I_{6k}$, with even $c_p$, by Proposition [1.6] and Table [1].

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions $I_{2n}$ at primes $p$, so by using Table [1] Table 2 and Lemma [3.1] we conclude that all reduction types of twists at $p$ are either $I_{2n}$ or $I_{2n}^*$, so the Tamagawa numbers stay even.

The curve $36.a2$ already has reduction type $III^*$ at 3, which stays the same under twisting or changes to $III^*$, as stated in Table [2]. In any case we get $c_3 = 2$ (see Table [1]).

As for the curve $20.a3$, we examine all twists by $d$ such that there exists a prime $p \mid d$ such that $20.a3$ has good reduction at $p$, i.e., $p \neq 2, 5$. At such $p$ we have reduction type $I_0$, and after twisting by $p$ we get that the reduction type of the twist at $p$ is $I_0^*$, as stated in Table [2].

By Tate’s algorithm [13], Case 6) we get that $c_p = 1 + \text{number of roots of } P(T) \text{ in } k_p$, where $P(T) = T^3 + T^2 – T = T(T^2 + T – 1)$. Polynomial $T^2 + T – 1$ has roots modulo $p$ if and only if $5$ is a quadratic residue modulo $p$. Therefore, we get

$$c_p = \begin{cases} 2, & \text{if } p \equiv 2, 3 \pmod{5} \\ 4, & \text{if } p \equiv 1, 4 \pmod{5} \end{cases}.$$ 

It remains to see what happens with the twists by $d$, where $d$ has no divisors of good reduction for the curve $20.a3$. Since the only primes of bad reduction are 2 and 5, by explicitly computing all possible twists we get that $20.a3$ where $c_E = 3$ and $80.b3$ where $c_E = 1$, are the only possible twists for which $2 \nmid c_E$.

We use the same approach with the curve $80.b1$, which has $c_E = 1$. We examine all twists by $d$ such that there exists a prime $p \mid d$ such that $80.b1$ has good reduction at $p$, i.e., $p \neq 2, 5$. At such $p$ we have reduction type $I_0$, and after twisting by $p$ we get that the reduction type of the twist at $p$ is $I_0^*$, as stated in Table [2].
in Table [2] By Tate’s algorithm [15 §8. Case 6]) we get that \( c_p = 1 + \text{number of roots of } P(T) \text{ in } k_p \), where \( P(T) = T^3 - T^2 - 41T + 116 = (T - 4)(T^2 + 3T - 29) \). Polynomial \( T^2 + 3T - 29 \) has roots modulo \( p \) if and only if \( 5 \) is a quadratic residue modulo \( p \). Therefore, we get
\[
c_p = \begin{cases} 
2, & \text{if } p \equiv 2, 3 \pmod{5} \\
4, & \text{if } p \equiv 1, 4 \pmod{5} 
\end{cases}
\]
It remains to see what happens with the twists by \( d \), where \( d \) has no divisors of good reduction for the curve 80.a8. Since the only primes of bad reduction are 2 and 5, by explicitly computing all possible twists we get that 80.a8 and 20.a1, where \( c_E = 1 \), are the only possible twists for which \( 2 \nmid c_E \).

For the curve 27.a4 which has \( c_E = 1 \), the situation is more complicated, and we will prove that the curve has infinitely many twists with Tamagawa number 1.

For 27.a4 we have that \( c_E = c_3 = 1 \), where 3 is the only prime of bad reduction. Similarly as for the curves 20.a3 and 80.a1, we are interested in what happens with the Tamagawa numbers of twists \( E^d \) when \( p \mid d \), for some prime \( p \) of good reduction for \( E \), in this case \( p = 3 \). At such \( p \) we have reduction type \( I_0^* \), and after twisting by \( d \) we get that the reduction type of the twist at \( p = I_0^* \), as stated in Table [2] By Tate’s algorithm [15 §8. Case 6]) we get that \( c_p = 1 + \text{number of roots of } P(T) \text{ in } k_p \), where \( P(T) = T^3 + 11664 \). The Tamagawa number at \( p \) when the reduction type is \( I_0^* \) can be 1, 2 or 4 (see Table 1). As opposed to the aforementioned two curves, all of those cases are possible here, as noted in Table 1.

Furthermore, the Galois group of the polynomial \( P \) is \( S_3 \), hence non-abelian, which means that we have no straightforward description in terms of congruences of the primes \( p \) for which there is a root modulo \( p \) [19, pp.576]. However, using Frobenius’ density theorem [10, pp.32] we know that the density of all primes \( p \) such that \( P \) remains irreducible modulo \( p \) is \( \frac{1}{2} \). That means that we have infinitely many primes \( p \) such that \( c_p = 1 \). It remains to see that \( c_E = 1 \) as well.

The prime \( 3 \) is the only prime of bad reduction for \( E \) and the reduction type of \( E \) at \( 3 \) is \( II \). The reduction type at 3 of \( E^d \) when \( 3 \nmid d \) stays the same (see Table 2) and hence the Tamagawa number at 3 stays 1. As for the prime \( p = 2 \), by using the fact that \( \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \equiv (-1, 2, 5) \), we explicitly compute all possible reduction types of quadratic twists at \( p = 2 \) and conclude that for every twist of those curves \( c_2 = 1 \).

Therefore, we have that \( c_E = c_2 = 1 \) for \( d \) in the set of primes for which \( P \bmod p \) stays irreducible.

\section*{Example 3.6.}

Denote by \( E \) the curve 27.a4. We have that \( c_E = c_3 = 1 \), where 3 is the only prime of bad reduction. As noted in the proof of Proposition 3.5 if \( p \) is a prime of good reduction for \( E \), then by Tate’s algorithm [15 §8. Case 6]) we get that the Tamagawa number of \( E^d \) at \( p \) such that \( p \nmid d \) is \( c_p = 1 + \text{number of roots of } P(T) \text{ in } k_p \), where \( P(T) = T^3 + 11664 \). The curve \( E^d \) has reduction type \( I_0^* \) at \( p \) and the Tamagawa number at \( p \) can be 1, 2 or 4 (see Table 1), depending on the number of roots of \( P \bmod p \). All of those cases are possible here, and they are presented in Table 3.

| twist of 27.a4 by d | curve | reduction type at d | \( c_2 \) | \( c_E \) |
|---------------------|-------|---------------------|-------|-------|
| \( d = 7 \)         | 21168.bv4 | \( I_0^* \)        | 1    | 1    |
| \( d = 5 \)         | 675.e4   | \( I_0^* \)        | 2    | 2    |
| \( d = 31 \)        | 4415152.ci4 | \( I_0^* \)    | 4    | 4    |

Table 3. Some twists of 27.a4 and their Tamagawa numbers

All computations made in this example can be verified using the accompanying \text{Magma code}.

\section*{Proposition 3.7.}

Let \( E \) be an elliptic curve over \( \mathbb{Q} \) with an \( n \)-isogeny, \( n \in \{14, 17, 19, 37, 43, 67, 163\} \). Then \( 2|c_E \).

\section*{Proof.}

For each value of \( n \), from [14] Table 4] we took all the possible \( j \)-invariants. They can be found in Table 2 in the second column. In the third column we have a Cremona label of one of the curves in the class of twists represented by each \( j \)-invariant. For each of those curves in the fourth column we have a prime of bad reduction of type \( III \). That reduction can only change to \( III^* \), and vice versa, after twisting, as we see in Table 2. Table 1 tells us that the Tamagawa number at primes of reduction type \( III \) and \( III^* \) is always 2, so the claim follows.
TAMAGA NUMBERS OF ELLIPTIC CURVES WITH PRESCRIBED TORSION SUBGROUP OR ISOGENY

| $n$ | $j$-invariant | Cremona label | bad prime with reduction type III |
|-----|---------------|---------------|----------------------------------|
| 14  | $-3^3 \cdot 5^3$ | 49.a4         | 7                                |
|     | $3^3 \cdot 5^3 \cdot 17^2$ | 49.a3 | 7                                |
| 17  | $-17^2 \cdot 101^2$ | 14450.b2 | 5                                |
|     | $-17 \cdot 101^3$ | 14450.b1 | 5                                |
| 19  | $-2^{15} \cdot 3^3$ | 360.a2 | 19                               |
| 37  | $-7 \cdot 11^3$ | 1225.b2 | 5                                |
|     | $-7 \cdot 137^2 \cdot 2083^3$ | 1225.b1 | 5                                |
| 43  | $-2^{18} \cdot 3^3 \cdot 5^3$ | 1849.b2 | 43                               |
| 67  | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | 4489.b2 | 67                               |
| 163 | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 26569.a2 | 163                              |

Table 4. $j$-invariants of the curves $X_0(n)$; their Cremona labels are representatives in the class of twists of least conductor with reduction type III at some prime

Acknowledgments. The author would like to thank Filip Najman for comments and helpful discussions.

References

[1] A. J. Barrios, M. Roy, Local data of rational elliptic curves with non-trivial torsion, preprint, [https://arxiv.org/abs/2104.10337](https://arxiv.org/abs/2104.10337)

[2] W. Bosma, J. Cannon and C. Playoust: The Magma Algebra System I: The User Language, J. Symb. Comp. 24 (1997), 235-265. (See also [http://magma.maths.usyd.edu.au/magma/](http://magma.maths.usyd.edu.au/magma/)).

[3] P. Bruin, F. Najman, Fields of definition of elliptic curves with prescribed torsion, Acta Arith. 181 (2017), 85-96.

[4] B. Conrad, C. Conrad, H. Helfgott, Root numbers and ranks in positive characteristic, Advances in Math. 198 (2005) 684-731.

[5] S. Comalada, Twists and reduction of an elliptic curve, Journal of Number Theory 49 (1994) 45-62.

[6] T. Dokchitser, V. Dokchitser, Local invariants of isogenous elliptic curves, Trans. Amer. Math. Soc. 367 (2015) 4339-4358.

[7] M. Hindry, J.H. Silverman, Diophantine geometry, Grad. Text Math. 201, Springer, New York, 2000.

[8] D. Jeon, A. Schweizer, Torsion of rational elliptic curves over different types of cubic fields, Int. J. Number Theory, 16 (2020), 1307-1323.

[9] D. Krumm, Quadratic Points on Modular Curves, Doctoral thesis, Athens, Georgia, 2013.

[10] H. W. Lenstra, P. Stevenhagen, Chebotarév and his density theorem, The Mathematical Intelligencer, 18 2, 26-37.

[11] The LMFDB Collaboration, The $L$-functions and Modular Forms Database, [http://www.lmfdb.org](http://www.lmfdb.org), 2021, [Online; accessed 8 February 2021].

[12] D. Lorenzini, Models of Curves and Wild Ramification, Pure and Applied Mathematics Quarterly, Volume 6 (2010) no. 1, p. 41-82.

[13] D. Lorenzini, Torsion and Tamagawa numbers, Annales de l’Institut Fourier, Volume 61 (2011) no. 5, p. 1995-2037.

[14] Á. Lozano-Robledo, On the field of definition of $p$-torsion points on elliptic curves over the rationals, Mathematische Annalen, Vol 357, Issue 1 (2013) 279-305.

[15] F. Najman, Tamagawa Numbers of elliptic curves with $C_{13}$ torsion over quadratic fields, Proc. Amer. Math. Soc. 145 (2017), 3747-3753.

[16] F. Najman, A. Trbović, Splitting of primes in number fields generated by points on some modular curves, preprint, [https://arxiv.org/abs/2009.02485](https://arxiv.org/abs/2009.02485).

[17] J. H. Silverman, The arithmetic of elliptic curves, Second Edition, Springer, 2009.

[18] J. Tate, Algorithm for determining the type of the singular fiber in an elliptic pencil, in Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, p. 33-52. Lecture Notes in Math., Vol. 476.

[19] B. F. Wyman, What is a Reciprocity Law?, The American Mathematical Monthly, 79, No. 6 (1972), 571-586.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: antonela.trbovic@math.hr