SPLITTING OF PRIMES IN NUMBER FIELDS GENERATED BY POINTS ON SOME MODULAR CURVES

FILIP NAJMAN AND ANTONELA TRBOVIĆ

Abstract. We study the splitting of primes in number fields generated by points on modular curves. Momose [11] was the first to notice that quadratic points on $X_1(N)$ generate quadratic fields over which certain primes split in a particular way and his results were later expanded upon by Krumm [9]. We prove results about the splitting behaviour of primes in quadratic fields generated by points on the modular curves $X_0(N)$ which are hyperelliptic (except for $N = 37$) and in cubic fields generated by points on $X_1(2, 14)$.

1. Introduction

A famous and much-studied problem in the theory of elliptic curves, going back to Mazur's torsion theorem [10], is to determine the possible torsion groups of elliptic curves over K, for a given number field K or over all number fields of degree d. Here we are more interested in the inverse question:

Question 1. *For a given torsion group T and a positive integer d, for which and what kind of number fields K of degree d do there exist elliptic curves E such that $E(K) \simeq T$?*

To make Question 1 sensible, one should of course choose the group T in a such a way that the set of such fields should be non-empty and preferably infinite.

It has been noted already by Momose [11] in 1984 (see also [8]) that the existence of specific torsion groups T over a quadratic field K forces certain rational primes to split in a particular way in K. Krumm [9] in his PhD thesis obtained similar results about splitting of primes over quadratic fields K with $T \simeq \mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ and it was also proven by Bosman, Bruin, Dujella and Najman [2] and Krumm [9] independently that all such quadratic fields must be real.

The first such result over cubic fields was proven by Bruin and Najman [5], where it was shown for $T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ that all such cubic fields K must be cyclic. In this paper we explore this particular case further and prove in Section 3 that in such a field 2 always splits, giving the first description of a splitting behaviour forced by the existence of a torsion group of an elliptic curve over a cubic field. Furthermore, we show that all primes $q \equiv \pm 1 \pmod 7$ of multiplicative reduction for such curves split in K. The proof of these results turns out to be more intricate than in the quadratic case.

As Question 1 can equivalently be phrased as asking when the modular curve $X_1(M, N)$ parameterizing elliptic curves together with the generators of a torsion subgroup $T \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ has non-cuspidal points over K, one is naturally drawn to ask a more general question by replacing $X_1(M, N)$ by any modular curve X.

Question 2. *For a given modular curve X and a positive integer d, for which and what kind of number fields K of degree d do there exist non-cuspidal points in $X(K)$?*

The most natural modular curves to consider next are the classical modular curves $X_0(N)$ classifying elliptic curves with cyclic isogenies of degree N. Bruin and Najman [4] proved that quadratic fields K over which $X_0(N)$ for $N = 28$ and 40 have non-cuspidal points are always real. In this paper we prove the first results about splitting of certain primes over quadratic fields where some modular curves $X_0(N)$ have non-cuspidal points. We consider all the N such that $X_0(N)$ is hyperelliptic except for $N = 37$, in particular

$$N \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}. \quad (1)$$

The reason we exclude $N = 37$ is that the quadratic points on $X_0(37)$ cannot all be described (with finitely many exceptions) as inverse images of $\mathbb{P}^1(\mathbb{Q})$ with respect to the degree 2 hyperelliptic map

Date: March 2, 2021.

The authors 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) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.

$X_0(37) \to \mathbb{P}^1$. For more details about quadratic points on $X_0(37)$, see [3]. In Section 2 we prove a series of results about the splitting behaviour of various primes in quadratic fields generated by quadratic points on $X_0(N)$.

A difficulty in proving these results that one immediately encounters is that the methods of [8] and [11] cannot be adapted to $X_0(N)$ as the existence of a torsion point of large order forces bad reduction on the elliptic curve (see for example [11, Lemma 1.9]), while the existence of an isogeny does not. Hence we approach the problem via explicit equations and parameterizations of modular curves, more in the spirit of [2, 4, 9] instead of moduli-theoretic considerations as in [8, 11].

González [6] proved results about fields generated by j-invariants of $\mathbb{Q}$-curves. Since for the values N that we study almost all N-isogenies over quadratic fields come from $\mathbb{Q}$-curves, our results are reminiscent of his, but it turns out there is little overlap in the results that are proved. This is perhaps not very surprising as we do not use the fact that we are looking at $\mathbb{Q}$-curves at all.

The computations in this paper were executed in the computer algebra system Magma [1]. The code used in this paper can be found at `https://web.math.pmf.unizg.hr/~atrbovi/magma/magma2.htm`.

2. Splitting of primes in quadratic fields generated by points on $X_0(N)$

In this section we study the splitting behaviour of primes in quadratic fields over which the modular curves $X_0(N)$ have non-cuspidal points. Models for $X_0(N)$ have been obtained from the `SmallModularCurves` database in Magma and can be found in Table 1.

Following [9], on a hyperlliptic curve X with a model $y^2 = f(x)$, we say that the quadratic points on X of the form $(x_0, \sqrt{f(x_0)})$, where $x_0 \in \mathbb{Q}$, are *obvious*. The quadratic points that are not obvious are called *non-obvious*. By the results of [4], all non-cuspidal quadratic points on $X_0(N)$ are obvious, with finitely many explicitly listed exceptions.

Theorem 2.1. *Let $K = \mathbb{Q}(\sqrt{D})$, where D is squarefree, be a quadratic field over which $X_0(N)$ has an obvious non-cuspidal point.*

(a) For each N, columns 2-5 in the table below show the splitting behaviour in K of some of the small primes, as well as some properties of D.
(b) For the pairs of N and a indicated in the table, if a prime p ramifies in K, then a is a square modulo p.
(c) For the pairs of N and b indicated in the table, if $p \neq 2$ is a prime such that b is a square modulo p, then there exist infinitely many quadratic fields generated by a point on $X_0(N)$ in which p ramifies.

Remark 1. Before proceeding to prove Theorem 2.1, we mention two papers [6, 13] that have some overlap with ours and show which of our results can be proved using their methods.

Obvious points on curves $X_0(N)$ are of the form $(x, y\sqrt{d})$, where $x, y \in \mathbb{Q}$. This gives us the point (x, y) on the quadratic twist $X_0^d(N)(\mathbb{Q})$ and hence $X_0^d(N)(\mathbb{Q}_p) \neq \emptyset$. Now the underlined entries in Table 2 can be alternatively proved using the results of Ozman [13, Theorem 1.1]. Note that the facts in Table 2 which have been marked by * or ** do not follow from [13, Theorem 1.1].

Recall that a $\mathbb{Q}$-curve is an elliptic curve that is isogenous to all its Galois conjugates. The *degree* of a $\mathbb{Q}$-curve over a quadratic field is the degree of a cyclic isogeny to its Galois conjugate. González proves the following statement [6, Proposition 1.1]:

Assume that there exists a quadratic $\mathbb{Q}$-curve of degree d defined over some quadratic field K. Then every divisor $N_1 \mid d$ such that

$$N_1 \equiv 1 \pmod 4 \quad \text{or} \quad N_1 \text{ is even and } d/N_1 \equiv 3 \pmod 4$$

is a norm of the field K.

For our values of N all but finitely many known exceptions of elliptic curves with N-isogenies over quadratic fields are $\mathbb{Q}$-curves (as proved by Bruin and Najman [4]). Note that we do not use the fact that the curves we consider are $\mathbb{Q}$-curves in any essential way; we only use the fact that almost all the quadratic points on the modular curves $X_0(N) : y^2 = f_N(x)$ are of the form $(x_0, \sqrt{f_N(x_0)}$ for $x_0 \in \mathbb{Q}$ (and from this fact Bruin and Najman proved that the corresponding elliptic curves are $\mathbb{Q}$-curves).

After noting that an obvious quadratic point on $X_0(N)$ corresponds to a $\mathbb{Q}$-curve of degree d, where d can be obtained from the tables in [4]), and applying González' proposition, we obtain p is not inert in a quadratic field $K := \mathbb{Q}(\sqrt{D})$ generated by an obvious point on $X_0(N)$ for the following pairs (N, p):

$$(N, p) \in \{(26, 13), (29, 29), (30, 5), (35, 5), (41, 41), (50, 5)\}.$$

In all of the pairs above we have $d = N$ except for $N = 30$, where $d = 15$. □

N	$f_N(x)$ from the equation $y^2 = f_N(x)$ for $X_0(N)$ and the factorization in $\mathbb{Q}[X]$
22	$x^6 - 4x^4 + 20x^3 - 40x^2 + 48x - 32$ $= (x^3 - 2x^2 + 4x - 4)(x^3 + 2x^2 - 4x + 8)$
23	$x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$ $= (x^3 - 8x^2 + 3x - 7)(x^3 - x + 1)$
26	$x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$
28	$4x^6 - 12x^5 + 25x^4 - 30x^3 + 25x^2 - 12x + 4$ $= (2x^2 - 3x + 2)(x^2 - x + 2)(2x^2 - x + 1)$
29	$x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$
30	$x^8 + 14x^7 + 79x^6 + 242x^5 + 441x^4 + 484x^3 + 316x^2 + 112x + 16$ $= (x^2 + 3x + 1)(x^2 + 6x + 4)(x^4 + 5x^3 + 11x^2 + 10x + 4)$
31	$x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3$ $= (x^3 - 6x^2 - 5x - 1)(x^3 - 2x^2 - x + 3)$
33	$x^8 + 10x^6 - 8x^5 + 47x^4 - 40x^3 + 82x^2 - 44x + 33$ $= (x^2 - x + 3)(x^6 + x^5 + 8x^4 - 3x^3 + 20x^2 - 11x + 11)$
35	$x^8 - 4x^7 - 6x^6 - 4x^5 - 9x^4 + 4x^3 - 6x^2 + 4x + 1$ $= (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1)$
39	$x^8 - 6x^7 + 3x^6 + 12x^5 - 23x^4 + 12x^3 + 3x^2 - 6x + 1$ $= (x^4 - 7x^3 + 11x^2 - 7x + 1)(x^4 + x^3 - x^2 + x + 1)$
40	$x^8 + 8x^6 - 2x^4 + 8x^2 + 1$
41	$x^8 - 4x^7 - 8x^6 + 10x^5 + 20x^4 + 8x^3 - 15x^2 - 20x - 8$
46	$x^{12} - 2x^{11} + 5 - x^{10} + 6x^9 - 26x^8 + 84x^7 - 113x^6 + 134x^5 - 64x^4 + 26x^3 + 12x^2 + 8x - 7$ $= (x^3 - 2x^2 + 3x - 1)(x^3 + x^2 - x + 7)(x^6 - x^5 + 4x^4 - x^3 + 2x^2 + 2x + 1)$
47	$x^{10} - 6x^9 + 11x^8 - 24x^7 + 19x^6 - 16x^5 - 13x^4 + 30x^3 - 38x^2 + 28x - 11$ $= (x^5 - 5x^4 + 5x^3 - 15x^2 + 6x - 11)(x^5 - x^4 + x^3 + x^2 - 2x + 1)$
48	$x^8 + 14x^4 + 1$ $= (x^4 - 2x^3 + 2x^2 + 2x + 1)(x^4 + 2x^3 + 2x^2 - 2x + 1)$
50	$x^6 - 4x^5 - 10x^3 - 4x + 1$
59	$x^{12} - 8x^{11} + 22x^{10} - 28x^9 + 3x^8 + 40x^7 - 62x^6 + 40x^5 - 3x^4 - 24x^3 + 20x^2 - 4x - 8$ $= (x^3 - x^2 - x + 2)(x^9 - 7x^8 + 16x^7 - 21x^6 + 12x^5 - x^4 - 9x^3 + 6x^2 - 4x - 4)$
71	$x^{14} + 4x^{13} - 2x^{12} - 38x^{11} - 77x^{10} - 26x^9 + 111x^8 + 148x^7 +$ $+x^6 - 122x^5 - 70x^4 + 30x^3 + 40x^2 + 4x - 11$ $= (x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11)(x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1)$

TABLE 1. Polynomials $f_N(x)$ in the equations $y^2 = f_N(x)$ for $X_0(N)$.

Many proofs will be similar for different values of N and before proceeding to a case-by-case study, we mention some general results which will be useful.

We fix the following notation throughout this section. Let N be one of the integers from (1) and write

$$X_0(N) : y^2 = f_N(x) = \sum_{i=0}^{\deg f_N} a_{i,N} x^i,$$

with $a_{i,N} \in \mathbb{Z}$. Note that in all instances $\deg f_N$ is even. As already stated, all non-cuspidal quadratic points on $X_0(N)$ are obvious, with finitely many exceptions. Those exceptions can be found listed in [4, Tables 1-18]. Let $(x_0, \sqrt{f_N(x_0)})$, for some $x_0 \in \mathbb{Q}$, be an obvious point on $X_0(N)$ and write $x_0 = m/n$, with m and n coprime integers. Let $d := f_N(x_0)$, $s := n^{\deg f_N} d$, and let D be the square-free part of d, i.e. the unique square-free integer such that $n^{\deg f_N} d = Ds^2$, for some $s \in \mathbb{Q}$. Since $\deg f_N$ is even, it

N	not inert	unramified	splits	D	a	b
22	$\underline{2}^*$					
26	$\underline{13}$			odd	13	
28	$3,7$	3	3	>0	-7^{***}	-7
29	$\underline{29}$			odd	29	
30	$\underline{2},\underline{3},\ \underline{5}^{**}$	$\underline{2},\underline{3}$	$\underline{2},\underline{3}$	odd	5	5
33	$2,\underline{11}$	$\underline{2}$	2	>0 odd	-11	-11
35	$\underline{5}^{**},\underline{7}$	$\underline{2},\underline{7}$	$\underline{7}$	odd	5	5
39	$3,\underline{13}$	$\underline{2},\underline{13}$	$\underline{13}$	odd	13	
40	$2,3,5$	$2,3,5$	$2,3,5$	>0 odd	$-1,5$	
41	$\underline{41}$				41	
46	2	$\underline{2}$	2	odd		
48	2	$2,3,5$	$2,3,5$	>0 odd	$-1,3$	
50	5			odd	5	

* -even more is true, $D \equiv 1,2,6 \pmod 8$
** -even more is true, $D \equiv 0,1 \pmod 5$
*** -the statement of (b) is true with the exception of $p=2$
_ -see Remark 1

TABLE 2.

follows that $s \in \mathbb{Z}$. We get the equality

$$n^{\deg f_N} d = Ds^2 = \sum_{i=0}^{\deg f_N} a_{i,N} m^i n^{deg f_N - i}. \tag{2}$$

The point $(x_0, \sqrt{f_N(x_0)})$ will be defined over $K := \mathbb{Q}(\sqrt{D})$.

We will prove part (a) of the theorem for each N separately. This proof can unfortunately not be generalized for each collumn of Table 2 as it can be for parts (b) and (c) of the theorem. However, we do mention a number of lemmas that describe the splitting behaviour of primes in K, which we will be using throughout. They are well-known or obvious, so we omit the proofs.

Lemma 2.2. *An odd prime p ramifies in K if and only if $p \mid D$, splits in K if and only if $\left(\frac{D}{p}\right) = 1$ and is inert in K if and only if $\left(\frac{D}{p}\right) = -1$.*

Lemma 2.3. *Let p be an odd prime and assume that we have $Ds^2 \equiv ap^t \pmod{p^\ell}$ with $p \nmid a$ and $\ell > t$.*

- *a) If $t = 2k$ for some $k \in \mathbb{Z}_0^+$, then $v_p(s) = k$, $D \equiv a(p^k/s)^2 \pmod{p^{\ell - t}}$, and p splits in K if and only if a is a square modulo p.*
- *b) If $t = 2k+1$ for some $k \in \mathbb{Z}_0^+$, then $p|D$ and p ramifies in K.*

As previous lemmas stated results about splitting for odd primes, we include similar results for the prime $p = 2$.

Lemma 2.4. *The prime 2 ramifies in K if and only if $D \not\equiv 1 \pmod 4$, splits in K if and only if $D \equiv 1 \pmod 8$ and is inert in K if and only if $D \equiv 5 \pmod 8$.*

Lemma 2.5. *Assume that we have $Ds^2 \equiv 2^t a \pmod{2^\ell}$, with $2 \nmid a$ and $\ell > t$.*

- *(a) If $t = 2k$, for some $k \in \mathbb{Z}_0^+$, then $v_2(s) = k$ and $D \equiv a(2^k/s)^2 \pmod{2^{\ell - t}}$. If $a = 1$ and $\ell - t = 3$, then 2 splits in K.*
- *(b) If $t = 2k+1$, for some $k \in \mathbb{Z}_0^+$, then $D \equiv 2a \pmod{2^{\ell - 2k}}$.*

All of the computations done in the following proofs are listed in the accompanying Magma code.

Proof of Theorem 2.1 (a).
N= 22 : In the manner already described above, in (2) we get

$$n^6d = Ds^2 = m^6 - 4m^4n^2 + 20m^3n^3 - 40m^2n^4 + 48mn^5 - 32n^6.$$

Considering all of the possibilities of m and n modulo 512, we have that $Ds^2 \equiv 1 \pmod 8$, $Ds^2 \equiv 32 \pmod{64}$ or $Ds^2 \equiv 64 \pmod{512}$. Using Lemma 2.5 this becomes $D \equiv 1 \pmod 8$ or $D \equiv 2 \pmod 4$. In any case we have $D \equiv 1, 2, 6 \pmod 8$, so 2 is not inert, according to Lemma 2.4.

N= 26 : In (2) we get

$$n^6d = Ds^2 = m^6 - 8m^5n + 8m^4n^2 - 18m^3n^3 + 8m^2n^4 - 8mn^5 + n^6.$$

Looking at all the possibilities of m and n modulo 13^2, we see that $Ds^2 \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$ or $Ds^2 \equiv 4 \cdot 13, 9 \cdot 13 \pmod{13^2}$. It follows from Lemma 2.3 that $D \equiv 0, 1, 3, 4, 9, 10, 12 \pmod{13}$. Using Lemma 2.2 we immediately get that 13 is not inert.

Considering the possibilities of m and n modulo 128, we have that $Ds^2 \equiv 1 \pmod 2$, $Ds^2 \equiv 4 \pmod{16}$, $Ds^2 \equiv 16 \pmod{32}$ or $Ds^2 \equiv 64 \pmod{128}$. Using Lemma 2.5 this becomes $D \equiv 1 \pmod 2$ or $D \equiv 1 \pmod 4$, so D is always odd.

N= 28 : In (2) we get

$$n^6d = Ds^2 = 4m^6 - 12m^5n + 25m^4n^2 - 30m^3n^3 + 25m^2n^4 - 12mn^5 + 4n^6.$$

Considering the possibilities of m and n modulo 3, we get $Ds^2 \equiv 1 \pmod 3$, so from Lemma 2.3 we have $D \equiv 1 \pmod 3$, and the fact that 3 splits follows from Lemma 2.2.

Looking at all the possibilities of m and n modulo 7^2, we see that $Ds^2 \equiv 1, 2, 4 \pmod 7$ or $Ds^2 \equiv 14 \pmod{7^2}$. It follows from Lemma 2.3 that $D \equiv 0, 1, 2, 4 \pmod 7$ and from from Lemma 2.2 that 7 is not inert.

The proof of the fact that $D > 0$ can be found in [4, Theorem 4].

N= 29 : In (2) we get

$$n^6d = Ds^2 = m^6 - 4m^5n - 12m^4n^2 + 2m^3n^3 + 8m^2n^4 + 8mn^5 - 7n^6.$$

Considering the possibilities of m and n modulo 32, we have that $Ds^2 \equiv 1 \pmod 2$, $Ds^2 \equiv 12 \pmod{16}$ or $Ds^2 \equiv 16 \pmod{32}$. Using Lemma 2.5 this becomes $D \equiv 1 \pmod 2$ or $D \equiv 3 \pmod 4$, so D is always odd.

We write $D = 29^a \cdot p_1 \cdot ... \cdot p_k$, where $a \in \{0, 1\}$ and $p_i \neq 2$, since D is odd. If $a = 1$, then $D \equiv 0 \pmod{29}$. If $a = 0$, then $\left(\frac{D}{29}\right) = \left(\frac{p_1}{29}\right) \cdot ... \cdot \left(\frac{p_k}{29}\right)$, which is equal to 1 after using the part (b) of this theorem for $N = 29$. In this case we have that $\left(\frac{D}{29}\right) = 1$, and Lemma 2.2 says that 29 is not inert.

N= 30 : In (2) we get

$$n^8d = Ds^2 = m^8 + 14m^7n + 79m^6n^2 + 242m^5n^3 + 441m^4n^4 + 484m^3n^5 + 316m^2n^6 + 112mn^7 + 16n^8.$$

Considering the possibilities of m and n modulo 128, we have that $Ds^2 \equiv 16 \pmod{128}$ or $Ds^2 \equiv 1 \pmod 8$. Using Lemma 2.5 we get $D \equiv 1 \pmod 8$, and from Lemma 2.4 we conclude that 2 splits.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$, and from Lemma 2.3 we conclude that $D \equiv 1 \pmod 3$. The fact that 3 splits follows from Lemma 2.2.

Looking at all the possibilities of m and n modulo 25, we see that $Ds^2 \equiv 1 \pmod 5$ or $Ds^2 \equiv 5 \pmod{25}$. Using Lemma 2.3 we get $D \equiv 0, 1, 4 \pmod 5$ and from Lemma 2.2 we see that 5 is not inert. Furthermore, we want to eliminate the possibility $D \equiv 4 \pmod 5$. If it were true, then for s in $n^8d = Ds^2$ it holds $s^2 \equiv 4 \pmod 5$, so s would be divisible by a prime p such that $p \equiv 2, 3 \pmod 5$, i.e. $\left(\frac{5}{p}\right) = -1$.

The expression $n^8d = Ds^2$ above factorizes as

$$n^8d = Ds^2 = \left(m^2 + 6nm + 4n^2\right)\left(m^2 + 3nm + n^2\right)\left(m^4 + 5m^3n + 11m^2n^2 + 10mn^3 + 4n^4\right),$$

so p has to divide one of the 3 factors on the right.

- If p divides $m^2 + 6nm + 4n^2 = (m + 3n)^2 - 5n^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.
- If p divides the second factor, it also divides $4(m^2+3nm+n^2) = (2m+3n)^2 - 5n^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.

- If p divides $m^4+5m^3n+11m^2n^2+10mn^3+4n^4 = (2m^2+5mn+4n^2)^2+3m^2n^2$, then $\left(\frac{-3}{p}\right) = 1$. The third factor can also be written as $(2m^2+5mn+m^2)^2+15(n^2+mn)^2$, so we alse have $\left(\frac{-15}{p}\right) = 1$. Combining these two facts, we get $\left(\frac{5}{p}\right) = 1$, which is also a contradiction.

***N*= 33** : In (2) we get

$$n^8d = Ds^2 = m^8 + 10m^6n^2 - 8m^5n^3 + 47m^4n^4 - 40m^3n^5 + 82m^2n^6 - 44mn^7 + 33n^8.$$

Considering the possibilities of m and n modulo 8, we have that $Ds^2 \equiv 1 \pmod 8$, so from Lemma 2.5 we conclude that $D \equiv 1 \pmod 8$ and from Lemma 2.4 that the prime 2 splits.

We write $D = 11^a \cdot p_1 \cdot \ldots \cdot p_k$, where $a \in \{0,1\}$ and $p_i \neq 2$, since $D \equiv 1 \pmod 8$. If $a = 1$, then $D \equiv 0 \pmod{11}$. If $a = 0$, then $\left(\frac{D}{11}\right) = \left(\frac{p_1}{11}\right) \cdot \ldots \cdot \left(\frac{p_k}{11}\right)$, which is equal to 1 after using the part (b) of this theorem for $N = 33$. In this case we have that $\left(\frac{D}{11}\right) = 1$, therefore 11 is not inert in K.

A point of the form $(x_0, \sqrt{f_{33}(x_0)})$ with $x_0 \in \mathbb{Q}$ is clearly defined over a real quadratic field, since $f_{33}(x_0) = x_0^8 + 10x_0^6 - 8x_0^5 + 47x_0^4 - 40x_0^3 + 82x_0^2 - 44x_0 + 33 > 0$, for every x_0. Therefore, $D > 0$.

***N*= 35** : In (2) we get

$$n^8d = Ds^2 = m^8 - 4m^7n - 6m^6n^2 - 4m^5n^3 - 9m^4n^4 + 4m^3n^5 - 6m^2n^6 + 4mn^7 + n^8.$$

Considering the possibilities of m and n modulo 4, we have that $Ds^2 \equiv 1 \pmod 4$ and from Lemma 2.5 we conclude $D \equiv 1 \pmod 4$. The fact that 2 is unramified now follows from Lemma 2.4.

Looking at all the possibilities of m and n modulo 25, we see that $Ds^2 \equiv 1 \pmod 5$ or $Ds^2 \equiv 5 \pmod{25}$. It follows from Lemma 2.3 that $D \equiv 0, 1, 4 \pmod 5$ and from Lemma 2.2 that 5 is not inert. Now want to eliminate the possibility $D \equiv 4 \pmod 5$. If it were true, then for s in $n^8d = Ds^2$ it holds $s^2 \equiv 4 \pmod 5$, so s would be divisible by a prime p such that $p \equiv 2, 3 \pmod 5$, i.e. $\left(\frac{5}{p}\right) = -1$.

The expression $n^8d = Ds^2$ above factorizes as

$$n^8d = Ds^2 = \left(-m^2 - mn + n^2\right)\left(-m^6 + 5m^5n + 9m^3n^3 + 5mn^5 + n^6\right),$$

so p has to divide one of the 2 factors on the right.

- If p divides the first factor, it also divides $4(-m^2 - nm + n^2) = (2m - n)^2 - 5m^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.
- If p divides the second factor, it also divides $4(-m^6 + 5m^5n + 9m^3n^3 + 5mn^5 + n^6) = (2n^3 + 5n^2m + 5nm^2 + 4m^3)^2 - 5(3n^2m + nm^2 + 2m^3)^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.

And in the end, considering the possibilities of m and n modulo 7, we have that $Ds^2 \equiv 1, 2, 4 \pmod 7$. It follows from Lemma 2.3 that $D \equiv 1, 2, 4 \pmod 7$ and from Lemma 2.2 that 7 splits.

***N*= 39** : In (2) we get

$$n^8d = Ds^2 = m^8 - 6m^7n + 3m^6n^2 + 12m^5n^3 - 23m^4n^4 + 12m^3n^5 + 3m^2n^6 - 6mn^7 + n^8.$$

Considering the possibilities of m and n modulo 4, we have that $Ds^2 \equiv 1 \pmod 4$ and from Lemma 2.5 we conclude $D \equiv 1 \pmod 4$. The fact that 2 is unramified now follows from Lemma 2.4.

We have that the right side of $n^8d = Ds^2$ above is congruent to $m^8 - 2m^4n^4 + n^8 = (m^4 - n^4)^2$ modulo 3.

Suppose first that $m \not\equiv n \pmod 3$. If $n \not\equiv 0 \pmod 3$ then D is a square modulo 3 and if $n \equiv 0 \pmod 3$ then it follows that $D \equiv 1 \pmod 3$ so D is again a square modulo 3.

Suppose now that $m \equiv n \pmod 3$. Then we run through all the possibilities of m and n modulo 81 and note that either Ds^2 is divisible by an odd power of 3, so $D \equiv 0 \pmod 3$, or $Ds^2 \equiv 9k \pmod{81}$, where $k \not\equiv 0 \pmod{81}$ and k is a square modulo 9. Using the Lemma 2.3 we get that $D \equiv k \pmod 9$, where k is a square modulo 9. Hence, in all cases we have $D \equiv 0, 1 \pmod 3$ and from Lemma 2.4 we immediately see that 3 is not inert.

Considering the possibilities of m and n modulo 13, we have that $Ds^2 \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$, and from Lemma 2.3 we conclude $D \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$. The fact that 13 splits now follows from Lemma 2.2.

***N*= 40** : In (2) we get

$$n^8d = Ds^2 = m^8 + 8m^6n^2 - 2m^4n^4 + 8m^2n^6 + n^8.$$

We write $n^8 d = Ds^2$ as

$$n^8 d = Ds^2 = (m^4 - n^4)^2 + 8m^2 n^2 (m^4 + n^4).$$

The integer n has to be odd (otherwise m and n would both be even), and if m is even, then Ds^2 is an odd square modulo 8. It follows from Lemma 2.5 that $D \equiv 1 \pmod 8$ and from Lemma 2.4 that 2 splits.

If m and n are both odd, then $Ds^2 \equiv 16m^2n^2 \pmod{128}$. From Lemma 2.5 we get that D is an odd square modulo 8, i.e. $D \equiv 1 \pmod 8$. The fact that 2 splits now follows from Lemma 2.4.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$. Using Lemma 2.3 we get $D \equiv 1 \pmod 3$, and from Lemma 2.2 we conclude that 3 splits.

Looking at all the possibilities of m and n modulo 5, we see that $Ds^2 \equiv 1, 4 \pmod 5$. Using Lemma 2.3 we get $D \equiv 1, 4 \pmod 5$, and from Lemma 2.2 we conclude that 5 splits.

The proof of the fact that $D > 0$ can be found in [4, Theorem 4].

***N*= 41** : In (2) we get

$$n^8 d = Ds^2 = m^8 - 4m^7 n - 8m^6 n^2 + 10m^5 n^3 + 20m^4 n^4 + 8m^3 n^5 - 15m^2 n^6 - 20mn^7 - 8n^8.$$

We write $D = 41^a \cdot p_1 \cdot \ldots \cdot p_k$, where $a \in \{0, 1\}$. If $a = 0$, then $D \equiv 0 \pmod{41}$. If $a = 1$, then $\left(\frac{D}{41}\right) = \left(\frac{p_1}{41}\right) \cdot \ldots \cdot \left(\frac{p_k}{41}\right)$, which is equal to 1 after using the part (b) of this theorem, and the fact that $\left(\frac{2}{41}\right) = 1$, in case one of the p_i is 2. In this case we have that $\left(\frac{D}{41}\right) = 1$, and Lemma 2.2 says that 41 is not inert.

***N*= 46** : In (2) we get

$$\begin{aligned} n^{12} d = Ds^2 = &m^{12} - 2m^{11} n + 5m^{10} n^2 + 6m^9 n^3 - 26m^8 n^4 + \\ &+ 84m^7 n^5 - 113m^6 n^6 + 134m^5 n^7 - 64m^4 n^8 + 26m^3 n^9 + 12m^2 n^{10} + 8mn^{11} - 7n^{12}. \end{aligned}$$

Considering the possibilities of m and n modulo 512, we have that $Ds^2 \equiv 64 \pmod{512}$ or $Ds^2 \equiv 1 \pmod 8$. Using Lemma 2.5, in both cases we get $D \equiv 1 \pmod 8$, and from Lemma 2.4 we conclude that 2 splits.

***N*= 48** : In (2) we get

$$n^8 d = Ds^2 = m^8 + 14m^4 n^4 + n^8.$$

We write $n^8 d = Ds^2$ as

$$n^8 d = Ds^2 = (m^4 + n^4)^2 + 12m^4 n^4.$$

If either m or n is even (forcing the other to be odd), then Ds^2 is an odd square modulo 8. It follows from Lemma 2.5 that $D \equiv 1 \pmod 8$ and from Lemma 2.4 that 2 splits.

If m and n are both odd, then $Ds^2 \equiv 16 \pmod{128}$. It follows from Lemma 2.5 that $D \equiv 1 \pmod 8$ and from Lemma 2.4 that 2 splits.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$. Using Lemma 2.3, we get $D \equiv 1 \pmod 3$, and from Lemma 2.2 we conclude that 3 splits.

Looking at all the possibilities of m and n modulo 5, we see that $Ds^2 \equiv 1 \pmod 5$. Using Lemma 2.3, we get $D \equiv 1, 4 \pmod 5$, and from Lemma 2.2 we conclude that 5 splits.

A point of the form $(x_0, \sqrt{f_{48}(x_0)})$ with $x_0 \in \mathbb{Q}$ is clearly defined over a real quadratic field, since $f_{48}(x_0) = x_0^8 + 14x_0^4 + 1 > 0$, for every x_0. Therefore, $D > 0$.

***N*= 50** : In (2) we get

$$n^6 d = Ds^2 = m^6 - 4m^5 n - 10m^3 n^3 - 4mn^5 + n^6.$$

Considering the possibilities of m and n modulo 5, we have that $Ds^2 \equiv 0, 1, 4 \pmod 5$. Using Lemma 2.3, we get $D \equiv 0, 1, 4 \pmod 5$, and from Lemma 2.2 we conclude that 5 is not inert.

We have

$$n^6 d = Ds^2 \equiv (m^3 - n^3)^2 \pmod 4.$$

If either m or n is even it follows that D is odd. If m and n are both odd, we have $Ds^2 \equiv 4 \pmod{16}, Ds^2 \equiv 16 \pmod{32}$ or $Ds^2 \equiv 64 \pmod{128}$. Using Lemma 2.5, in all cases we get that D is odd. ☐

We now prove two lemmas that will be useful in the proof of part (b) of the theorem.

Lemma 2.6. *Suppose f_N factorizes as $f_N = \prod_{i \in I} f_{N,i}$, where $f_{N,i} \in \mathbb{Z}[x]$ are irreducible factors of degree 2 or 3 and $p \nmid a_{0,N}$. If p ramifies in K, then there exists an $i \in I$ such that $\Delta(f_{N,i})$ is a square modulo p.*

Proof. Assume that p ramifies in K; then by Lemma 2.2 it follows that $p|D$. If $p|n$, then it would follow that $p|m$, which is a contradiction, so we conclude that $p \nmid n$. Dividing out (2) by n, we see that m/n is a root of f_N modulo p and hence there exists an $i \in I$ such that m/n is a root of $f_{N,i}$ modulo p.

If $f_{N,i}$ is of degree 2 or 3, the formulas for the roots of quadratic and cubic polynomials imply that $\sqrt{\Delta(f_{N,i})}$ is defined over $\mathbb{F}_p$, which proves the statement. □

Remark 2. Note that the statement of part (b) of the theorem can be proved with the previous lemma only for $(N, a) = (28, -7)$. We have $f_{28}(x) = (2x^2 - 3x + 2)(x^2 - x + 2)(2x^2 - x + 1)$ and $\Delta(f_{28,i}) = -7$, for each i.

As mentioned in the remark, Lemma 2.6 is not enough to prove all of the statements in (b), so we provide a generalization.

Lemma 2.7. *Let $f_N = \prod_{i\in I} f_{N,i}$ be the decomposition into irreducible factors, with $f_{N,i} \in \mathbb{Z}[x]$. Assume that there exists a quadratic field K_0 such that each $f_{N,i}$ becomes reducible in $K_0[x]$ and let p be an odd prime such that $(p, \Delta(f_{N,i})) = 1$ for all i. Then if p ramifies in K it follows that $\Delta(K_0)$ is a square modulo p, i.e. p is not inert in K_0.*

Proof. Let σ be the generator of $\mathrm{Gal}(K_0/\mathbb{Q})$ and $f_{N,i,K_0} \in K_0[x]$ an irreducible factor of $f_{N,i}$. Then we obviously have

$$f_{N,i,K_0}(f_{N,i,K_0})^\sigma = f_{N,i}. \tag{3}$$

Assume that p ramifies in K. We will prove the lemma by contradiction, so we assume that p is inert in K_0. As in the proof of Lemma 2.6 we conclude that $f_{N,i}$ has a root a in $\mathbb{F}_p$ for some i. Hence a is a root of one of the factors on the left in (3). Assume without loss of generality that a is a root of $f_{N,i}$ in $\mathbb{F}_p$.

Let $\mathfrak{p}$ be the prime of K above p and denote by $\mathbb{F}_\mathfrak{p} := \mathcal{O}_{K_0}/\mathfrak{p}$ the residue field of $\mathfrak{p}$. Let $\tau = \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ and denote by $\overline{f}$ the reduction of a polynomial $f \in K_0[x]$ modulo $\mathfrak{p}$; then we have $\overline{f^\sigma} = \overline{f}^\tau$. Hence a^τ is a root of $\overline{f}^\tau_{N,i}$. But since $a \in \mathbb{F}_p$, it follows that $a = a^\tau$ and hence from (3) it follows that a is a double root of $f_{N,i}$ over $\mathbb{F}_p$ and hence $\Delta(f_{N,i})$ is divisible by p, which is in contradiction with the assumption $(p, \Delta(f_{N,i})) = 1$. □

Proof of Theorem 2.1 (b). Let $f_N = \Pi_i f_{N,i}$ be the factorization of f_N in $\mathbb{Z}[X]$, as in Table 1. Table 3, which can be computed with the accompanying Magma code, contains for each N the number a such that every $f_{N,i}$ becomes reducible in $\mathbb{Q}(\sqrt{a})$, the factorization in $\mathbb{Q}(\sqrt{a})$ and discriminants of each $f_{N,i}$. Using the Lemma 2.7 we immediately get that if an odd prime p such that $(p, \Delta(f_{N,i})) = 1$ ramifies in K, then a is a square modulo p. For $p = 2$ and p that are not coprime to every $\Delta(f_{N,i})$ and can ramify (this can be checked in Theorem 2.8, which is proved independently) we can explicitly verify that $\left(\frac{a}{p}\right) \neq -1$. □

Proof of Theorem 2.1 (c). For all pairs of N and b, in Table 3 we have the factorizations of f_N where some of the factors are linear over $\mathbb{Q}(\sqrt{b})$. Therefore, f_N has a root over each $\mathbb{F}_p$ such that $\sqrt{b}$ is defined modulo p, i.e. such that b is a square modulo p.
If $x_0 \in \mathbb{Z}$ is a root of f_N such that $f_N(x_0) \equiv 0 \pmod{p}$, then $f_N(x_0 + kp) \equiv 0 \pmod{p}$, $k = 0, ..., p-1$. If $p > \deg f_N$, we have $f_N(x_0 + kp) \not\equiv 0 \pmod{p^2}$ for at least one value of k. Now we know that for $p > \deg f_N$ there exists $a \in \mathbb{Z}$ be such that $f_N(a) \equiv 0 \pmod{p}$ and $f_N(a) \not\equiv 0 \pmod{p^2}$. For smaller values of p, with exception of $p = 2$, one can explicitly check that this claim remains true. Therefore, p ramifies in $\mathbb{Q}(\sqrt{f_N(a)})$.
It remains to show that there are infinitely many quadratic fields such that p ramifies. Let $S = \{u \in \mathbb{Z} : u \equiv a \pmod{p^2}\}$. Obviously $f_N(u) \equiv 0 \pmod{p}$ and $f_N(u) \not\equiv 0 \pmod{p^2}$ for all $u \in S$. Let d_u be the squarefree part of $f_N(u)$; the quadratic point $(u, \sqrt{f_N(u)})$ will be defined over $\mathbb{Q}(\sqrt{d_u})$. After writing $f_N(u) = d_u s_u^2$ for some $s_u \in \mathbb{Z}$, we observe that (u, s_u) is a rational point on the quadratic twists $C_N^{d_u}$ of $X_0(N)$,

$$C_N^{d_u} : d_u y^2 = f_N(x).$$

Since each $C_N^{d_u}$ is of genus ≥ 2, by Faltings' theorem it follows that $C_N^{d_u}(\mathbb{Q})$ is finite and hence $\{d_u : u \in S\}$ is infinite, proving the claim. □

$\boldsymbol{N}$	a	factorization of $\boldsymbol{f_N}$ in $\mathbb{Q}(\sqrt{\mathbf{a}})$	$\Delta(\boldsymbol{f_{N,i}})$
26	13	$\Big((x^3+(-\sqrt{13}-4)x^2+\frac{1}{2}(\sqrt{13}+5)x+\frac{1}{2}(-3\sqrt{13}-11)\Big)\times$ $\times\Big(x^3+(\sqrt{13}-4)x^2+\frac{1}{2}(-\sqrt{13}+5)x+\frac{1}{2}(3\sqrt{13}-11)\Big)$	$2^{20}\cdot 13^3$
28	-7	$(x+\frac{1}{2}(-\sqrt{-7}-1))\,(x+\frac{1}{4}(-\sqrt{-7}-3)\times$ $\times(x+\frac{1}{4}(-\sqrt{-7}-1))\,(x+\frac{1}{4}(\sqrt{-7}-3))\times$ $\times(x+\frac{1}{4}(-\sqrt{-7}-1))\,(x+\frac{1}{2}(\sqrt{-7}-1))$	-7 -7 -7
29	29	$\Big(x^3+(-\sqrt{29}-2)x^2+\frac{1}{2}(\sqrt{29}+13)x+\frac{1}{2}(-\sqrt{29}-1)\Big)\times$ $\times\Big(x^3+(\sqrt{29}-2)x^2+\frac{1}{2}(-\sqrt{29}+13)x+\frac{1}{2}(\sqrt{29}-1)\Big)$	$2^{12}\cdot 29^5$
30	5	$\Big(x-\sqrt{5}+3\Big)\Big(x+\frac{1}{2}(-\sqrt{5}+3)\Big)\times$ $\times\Big(x+\frac{1}{2}(\sqrt{5}+3)\Big)\Big(x+\sqrt{5}+3\Big)\times$ $\times\Big(x^2+\frac{1}{2}(-\sqrt{5}+5)x-\sqrt{5}+3\Big)\Big(x^2+\frac{1}{2}(\sqrt{5}+5)x+\sqrt{5}+3\Big)$	5 $2^2\cdot 5$ $2^2\cdot 3^2\cdot 5^2$
33	-11	$(x+\frac{1}{2}(-\sqrt{-11}-1))\,(x+\frac{1}{2}(\sqrt{-11}-1))\times$ $\times(x^3+\frac{1}{2}(-\sqrt{-11}+1)x^2+\frac{1}{2}(\sqrt{-11}+5)x-\sqrt{-11})\times$ $\times(x^3+\frac{1}{2}(\sqrt{-11}+1)x^2+\frac{1}{2}(-\sqrt{-11}+5)x+\sqrt{-11})$	-11 $-2^8\cdot 3^6\cdot 11^5$
35	5	$\Big(x+\frac{1}{2}(-\sqrt{5}+1)\Big)\Big(x+\frac{1}{2}(\sqrt{5}+1)\Big)\times$ $\times\Big(x^3+\frac{1}{2}(-3\sqrt{5}-5)x^2+\frac{1}{2}(\sqrt{5}+5)x-\sqrt{5}-2\Big)\times$ $\times\Big(x^3+\frac{1}{2}(3\sqrt{5}-5)x^2+\frac{1}{2}(-\sqrt{5}+5)x+\sqrt{5}-2\Big)$	5 $2^8\cdot 5^7\cdot 7^2$
39	13	$\Big(x^2+\frac{1}{2}(-\sqrt{13}-7)x+1\Big)\Big(x^2+\frac{1}{2}(-\sqrt{13}+1)x+1\Big)\times$ $\times\Big(x^2+\frac{1}{2}(\sqrt{13}-7)x+1\Big)\Big(x^2+\frac{1}{2}(\sqrt{13}+1)x+1\Big)$	$-3^3\cdot 13^2$ $-3\cdot 13^2$
40	-1	$(x^4-2\sqrt{-1}x^3+2x^2+2\sqrt{-1}x+1)\times$ $\times(x^4+2\sqrt{-1}x^3+2x^2-2\sqrt{-1}x+1)$	$2^{40}\cdot 5^4$
	5	$\Big(x^4+(-2\sqrt{5}+4)x^2+1\Big)\Big(x^4+(2\sqrt{5}+4)x^2+1\Big)$	
41	41	$\Big(x^4-2x^3+(-\sqrt{41}-6)x^2+(-\sqrt{41}-7)x+\frac{1}{2}(-\sqrt{41}-3)\Big)\times$ $\times\Big(x^4-2x^3+(\sqrt{41}-6)x^2+(\sqrt{41}-7)x+\frac{1}{2}(\sqrt{41}-3)\Big)$	$-2^{16}\cdot 41^6$
48	-1	$(x^2+(-\sqrt{-1}-1)x-\sqrt{-1})\,(x^2+(-\sqrt{-1}+1)x+\sqrt{-1})\times$ $\times(x^2+(\sqrt{-1}-1)x+\sqrt{-1})\,(x^2+(\sqrt{-1}+1)x-\sqrt{-1})$	$2^8\cdot 3^2$ $2^8\cdot 3^2$
	3	$\Big(x^2+(-\sqrt{3}-1)x+\sqrt{3}+2\Big)\Big(x^2+(-\sqrt{3}+1)x-\sqrt{3}+2\Big)\times$ $\times\Big(x^2+(+\sqrt{3}-1)x-\sqrt{3}+2\Big)\Big(x^2+(\sqrt{3}+1)x+\sqrt{3}+2\Big)$	
50	5	$\Big(x^3+(-\sqrt{5}-2)x^2+\frac{1}{2}(-\sqrt{5}+1)x+\frac{1}{2}(-\sqrt{5}-3)\Big)\times$ $\times\Big(x^3+(\sqrt{5}-2)x^2+\frac{1}{2}(\sqrt{5}+1)x+\frac{1}{2}(\sqrt{5}-3)\Big)$	$2^{16}\cdot 5^5$

TABLE 3. Factorizations of f_N in $\mathbb{Q}(\sqrt{\mathbf{a}})$, and the discriminants of $f_{N,i}$ defined in the statement of Lemma 2.7.

Theorem 2.8. *In Table 4 below, we list the primes $p \leq 100$ which are unramified for all quadratic fields generated by quadratic points $X_0(N)$, for $N \in \{22, 23, 26, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$.*

N	unramified primes
22	$3, 5, 23, 31, 37, 59, 67, 71, 89, 97$
23	$2, 3, 13, 29, 31, 41, 47, 71, 73$
26	$3, 5, 7, 11, 17, 19, 31, 37, 41, 43, 47, 59, 67, 71, 73, 83, 89, 97$
28	$3, 5, 13, 17, 19, 31, 41, 47, 59, 61, 73, 83, 89, 97$
29	$3, 5, 11, 13, 17, 19, 31, 37, 41, 43, 47, 53, 61, 73, 79, 89, 97$
30	$2, 3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97$
31	$2, 5, 7, 19, 41, 59, 71, 97$
33	$2, 7, 13, 17, 19, 29, 41, 43, 61, 73, 79, 83$
35	$2, 3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97$
39	$2, 5, 7, 11, 13, 19, 31, 37, 41, 47, 59, 61, 67, 71, 73, 79, 83, 89, 97$
40	$2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 97$
41	$3, 5, 7, 11, 13, 17, 19, 29, 37, 47, 53, 61, 67, 71, 73, 79, 89, 97$
46	$2, 3, 13, 29, 31, 41, 47, 71, 73$
47	$2, 3, 7, 17, 37, 53, 59, 61, 71, 79, 89, 97$
48	$2, 3, 5, 7, 11, 17, 19, 23, 29, 31, 41, 43, 47, 53, 59, 67, 71, 79, 83, 89$
50	$3, 7, 11, 13, 17, 19, 23, 37, 41, 43, 47, 53, 67, 73, 83, 89, 97$
59	$3, 5, 7, 19, 29, 41, 53, 79$
71	$2, 3, 5, 19, 29, 37, 43, 73, 79, 83, 89$

TABLE 4. Primes up to 100 that do not ramify in quadratic fields over which $X_0(N)$ has a point.

Proof. The proofs of all the facts listed are easy and all basically the same; take some prime p in the table above. Using the notation as in 2, we run through all m and n in the appropriate equation modulo p and we get that $n^{2k}d \not\equiv 0 \pmod p$ for some positive integer k, which gives us that $D \not\equiv 0 \pmod p$ and hence p is unramified. □

3. Splitting of 2 in cubic fields generated by cubic points of $X_1(2, 14)$

Let us fix the following notation for the remainder of this section. Denote $X := X_1(2, 14)$ and $Y := Y_1(2, 14)$. Let $\phi : X_1(2, 14) \to X_1(14)$ be the forgetful map sending $(E, P, Q, R) \in X$ with P and Q of order 2 and R of order 7 to $(E, P, R) \in X_1(14)$. Let K be a cubic number field over which X has a non-cuspidal point $x = (E, P, Q, R)$ and let $\mathfrak{P}$ be a prime above p. By [5, Theorem 1.2], K is a cyclic cubic field. Denote by $\overline{x}$ the reduction of x mod $\mathfrak{P}$.

In this section we are going to prove that the prime 2 always splits in a cubic field over which X has a non-cuspidal point. Furthermore, we will show the same statement for all primes $p \equiv \pm 1 \pmod 7$ for which E has multiplicative reduction.

The curve X has the following model [5, Proposition 3.7] in $\mathbb{P}^1_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$:

$$X : f(u, v) = (u^3 + u^2 - 2u - 1)v(v + 1) + (v^3 + v^2 - 2v - 1)u(u + 1) = 0. \tag{4}$$

The curve X has 18 cusps, 9 of which are defined over $\mathbb{Q}$ and 9 over $\mathbb{Q}(\zeta_7)^+$, forming 3 Galois orbits.

Let τ and ω be automorphisms of X, where the moduli interpretation of τ is that it acts as a permutation of order 3 on the points of order 2 of E and trivially on the point of order 7, and where the moduli interpretation of ω is that it acts trivially on the points of order 2 and as multiplication by 2 on the point of order 7. Let $\alpha := \omega\tau$ and $\beta := \omega\tau^2$.

From [5, Chapter 3] it follows that the only maps of degree 3 from X to $\mathbb{P}^1$ are quotienting out by subgroups generated by α and β (an automorphism of X interchanges these two maps) and that all non-cuspidal cubic points on X are inverse images of $\mathbb{P}^1(\mathbb{Q})$ with respect to these maps. Also, both α and β act without fixed points on the cusps.

As it has already been mentioned, the results of [5] tell us that elliptic curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ torsion over a cubic field are parameterized by $\mathbb{P}^1(\mathbb{Q})$, so one can write every such curve as E_u for some $u \in \mathbb{Q}$. We do not display the model for E_u as it contains huge coefficients, but it can be found in the accompanying Magma code. In [5] it is proved that the curve $E := E_u$ is a base change of an elliptic curve defined over $\mathbb{Q}$.

We have

$$j(u) = \frac{(u^2+u+1)^3(u^6+u^5+2u^4+9u^3+12u^2+5u+1)f_{12}(u)^3}{u^{14}(u+1)^{14}(u^3+u^2-2u-1)^2},$$

where

$$f_{12}(u) = u^{12}+4u^{11}+3u^{10}-4u^9+6u^7-17u^6-30u^5+6u^4+34u^3+25u^2+8u+1,$$

and

$$\Delta(u) = \frac{u^{14}(u+1)^{14}(u^3+u^2-2u-1)^2}{h_{12}(u)^{12}},$$

$$c_4(u) = \frac{g_2(u)g_6(u)g_{12}(u)}{h_{12}(u)^4},$$

where g_i are polynomials in u of degree i, for $i = 2, 6, 12$, and h_{12} is of degree 12.

Let $\operatorname{res}(f, g)$ denote the resultant of the polynomials f and g. If $v_p(h_{12}(u)) > 0$, then E does not have multiplicative reduction at p, since $\operatorname{res}(h_{12}(u), g_\Delta(u)) = \operatorname{res}(h_{12}(u), g_{c_4}(u)) = 1$, where g_Δ is the numerator of $\Delta(u)$ and g_{c_4} is the numerator of $c_4(u)$, and therefore $v_p(j(u)) = 0$. There are several possibilities for the elliptic curve E to have multiplicative reduction:

- If $v_p(u) =: k > 0$, then using the fact that
$$\operatorname{res}\left(u, \frac{\Delta(u)}{u^{14}}\right) = \operatorname{res}(u, c_4(u)) = 1,$$
we conclude that reduction mod p will be of type I_{14k}.
- If $v_p(u) =: -k < 0$, with the change of variables $v := \frac{1}{u}$ we get a similar situation as above, with
$$\operatorname{res}\left(v, \frac{\Delta(v)}{v^{14}}\right) = \operatorname{res}(v, c_4(v)) = 1,$$
so the reduction mod p will be of type I_{14k}.
- If $v_p(u) = 0$ and $v_p(u+1) := k > 0$, then using the fact that
$$\operatorname{res}\left(u+1, \frac{\Delta(u)}{(u+1)^{14}}\right) = \operatorname{res}(u+1, c_4(u)) = 1,$$
we conclude that the reduction mod p is of type I_{14k}.
- The only other possibility for multiplicative reduction is $v_p(u^3+u^2-2u-1) =: k > 0$. Note that a root α of $f(u) := u^3+u^2-2u-1$ generates the ring of integers $\mathbb{Z}[\alpha]$ of $\mathbb{Q}(\zeta_7)^+$. The fact that $p|f(u)$ implies that $f(u)$ has a root in $\mathbb{F}_p$ and hence p splits in $\mathbb{Q}(\zeta_7)^+$, implying $p \equiv \pm 1 \pmod 7$ or $p = 7$. Since
$$\operatorname{res}\left(u^3+u^2-2u-1, \frac{\Delta(u)}{(u^3+u^2-2u-1)^2}\right) = 7^{30}$$
and
$$\operatorname{res}\left(u^3+u^2-2u-1, c_4(u)\right) = 7^{12},$$
it follows that there can be cancellation with the numerator only in the case $p = 7$.
- Suppose $p = 7$, $v_7(u) = 0$ and $v_7(u^3+u^2-2u-1) = k > 0$. An easy computation shows that $u \equiv 2 \pmod 7$ and $k = 1$, and that the numerator will be divisible by a higher power of 7 than u^3+u^2-2u-1, which show that the reduction will not be multiplicative.

In the discussion above we have proved the following two results:

Proposition 3.1. *Suppose E has multiplicative reduction at a rational prime p. Then either the reduction is of type I_{14k} for some k, or $p \equiv \pm 1 \pmod 7$, in which case the reduction is I_{2k}.*

Remark 3. As it has been mentioned, E is a base change of an elliptic curve over $\mathbb{Q}$, so in Proposition 3.1 and in the remainder of the section, when we consider the reduction of E (and also X and $X_1(14)$) modulo a rational prime, we will consider E to be defined over $\mathbb{Q}$ and when we consider it modulo a prime of K we consider its base change to K.

Proposition 3.2. *The curve E has multiplicative reduction of type I_{14k} at 2.*

Proof. This follows from the observation that $v_2(u) \neq 0$ or both $v_2(u) = 0$ and $v_2(u+1) > 0$, from which it follows, by what we have already proved, that in both cases the reduction type of E_u at 2 is I_{14k}. □

We now prove 3 useful lemmas.

Lemma 3.3. *Let $x \in Y(K)$ and let $\mathfrak{P}$ be a prime of K over 2. Then x modulo $\mathfrak{P}$ is defined over $\mathbb{F}_2$.*

Proof. As mentioned above, the results of [5] imply that a non-cuspidal cubic point on $x \in X$ given by the equation $f(u,v) = 0$ in (4) satisfies either $u \in \mathbb{P}^1(\mathbb{Q})$ or $v \in \mathbb{P}^1(\mathbb{Q})$. Over $\mathbb{F}_2$, the polynomial f factors as

$$f(u,v) = (u+v)(uv+v+1)(uv+v+1),$$

which implies that if one of u or v is $\in \mathbb{P}^1(\mathbb{F}_2)$, then so is the other. This implies that the reduction of x modulo $\mathfrak{P}$ is defined over $\mathbb{F}_2$. □

Lemma 3.4. *Let $F = \mathbb{Q}(\zeta_7)^+$, let C be a cusp of X whose field of definition is F and let q be a rational prime. Then the field of definition of the reduction of C in $\overline{\mathbb{F}}_q$ is $\mathbb{F}_{q^3}$ if $q \not\equiv \pm 1 \pmod 7$ and $\mathbb{F}_q$ if $q \equiv \pm 1 \pmod 7$.*

Proof. We have $[k(C) : \mathbb{F}_q] = [\mathbb{Q}_q(\zeta_7 + \zeta_7^{-1}) : \mathbb{Q}_q]$ from which the claim follows. □

Lemma 3.5. *Let $q \equiv \pm 1 \pmod 7$ be a rational prime such that E has multiplicative reduction over q and let $\mathfrak{P}$ be a prime of K over q. Then the reduction of $x \in X$ modulo $\mathfrak{P}$ corresponding to the curve E is $\mathbb{F}_q$.*

Proof. Since x modulo $\mathfrak{P}$ is a cusp, the statement follows from Lemma 3.4. □

Proposition 3.6. *Let $q = 2$ or $q \equiv \pm 1 \pmod 7$ be a rational prime such that E has multiplicative reduction in q. Then q splits in K.*

Proof. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ (recall that K is Galois over $\mathbb{Q}$) and suppose q is inert in K. As the degree 3 map $X \to \mathbb{P}^1$ is quotienting by α, it follows that

$$\left\{x, x^{\sigma}, x^{\sigma^2}\right\} = \left\{x, \alpha(x), \alpha^2(x)\right\},$$

so we can suppose without loss of generality that $x^{\sigma} = \alpha(x)$ and $x^{\sigma^2} = \alpha^2(x)$. Let $\overline{x} = \overline{C_0}$, for some cusp $C_0 \in X$. It follows that $\overline{\alpha(x)} = \overline{\alpha(C_0)}$ and $\overline{\alpha^2(x)} = \overline{\alpha^2(C_0)}$. Denote by $C_1 := \alpha(C_0)$ and by $C_2 := \alpha^2(C_0)$; all C_i are distinct as α acts without fixed points on the cusps. By Lemma 3.3 and Lemma 3.5, all $\overline{C_i}$ are defined over $\mathbb{F}_q$.

Denote by $K_i := \phi(C_i)$ and by $y = \phi(x) \in Y_1(14)$. Descending everything to $X_1(14)$, we have $\overline{y} = \overline{K_0}$, $\overline{y^{\sigma}} = \overline{K_1}$, $\overline{y^{\sigma^2}} = \overline{K_2}$. By Lemma 3.3 and Lemma 3.5, all $\overline{C_i}$ and hence all $\overline{K_i}$ are defined over $\mathbb{F}_q$.

Using the same arguments as in [12, Proposition 3.1] we get that $\overline{K_0} = \overline{K_1} = \overline{K_2}$. Reduction modulo q is injective on the torsion of $X_1(14)$ by [7, Appendix] for $q > 2$ and by explicitly checking injectivity for $q = 2$. Now from the fact that the rank of $X_1(14)(\mathbb{Q}(\zeta_7)^+)$ is 0, we conclude $K_0 = K_1 = K_2$. This is impossible since C_0, C_1, C_2 are distinct and ϕ is a degree 2 map. □

Acknowledgments. We thank Andrej Dujella for helpful comments.

References

[1] 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/`) 2

[2] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Notices 2014 (2014), 2885–2923. 1, 2

[3] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. to appear. 2

[4] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015) 578–602. 1, 2, 3, 5, 7

[5] P. Bruin and F. Najman, *Fields of definition of elliptic curves with prescribed torsion*, Acta Arith. **181** (2017), 85–96. 1, 10, 11, 12

[6] J. González, *On the j-invariants of the quadratic $\mathbb{Q}$-curves*, J. Lond. Math. Soc. **63** (2001), 52–68. 2

[7] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502. 12

[8] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 1, 2

[9] D. Krumm, Quadratic Points on Modular Curves, PhD thesis, University of Georgia, 2013. 1, 2

[10] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186. 1

[11] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J. **96** (1984), 139–165. 1, 2

[12] F. Najman, *Tamagawa numbers of elliptic curves with C_{13} torsion over quadratic fields,* Proc. Amer. Math. Soc. **145** (2017), 3747–3753. 12

[13] E. Ozman, *Points on quadratic twists of $X_0(N)$,* Acta Arith. **152** (2012), 323–348. 2

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

Email address: fnajman@math.hr

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

Email address: antonela.trbovic@math.hr