TORSION AND EXCEPTIONAL UNITS

DINO LORENZINI

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve which has everywhere semi-stable reduction. We first prove that if $E(\mathbb{Q})_{tors}$ contains an element of order $N \geq 3$, then there exists a prime p where $E/\mathbb{Q}$ has split multiplicative reduction modulo p, thereby establishing a conjecture of Agashe. We consider then generalizations over number fields inspired by this result. Fix a degree d, and consider all number fields K of degree d. Fix a prime $N > 2d+1$, and consider all elliptic curves which have a K-rational torsion point of order N and such that the Tamagawa number $c(E/K)$ is coprime to N. When $d = 1, 2, 3$, we show that there exist only finitely many degree d fields K and finitely many such N-special elliptic curves E/K. Partial results are also obtained for $d = 4, 5$, and we conjecture that the statement holds when $d = 6, 7$. Fields K which support such elliptic curves are very structured, and we show in particular that their Lenstra constant $M(K)$ is bounded below by $(N-1)/2$ when $N \leq 23$. We conjecture that this statement holds for any prime N.

KEYWORDS Elliptic curve, number field, torsion subgroup, Tamagawa number, exceptional unit, Lenstra constant.

MSC: 11G05, 11G16, 11G40, 14G05, 11G10, 14G10

1. INTRODUCTION

Let K be a number field, and let E/K be an elliptic curve. We investigate in this article how the presence of a non-trivial torsion point in $E(K)$ affects the reduction properties of the curve E/K.

When $E/\mathbb{Q}$ has everywhere semi-stable reduction, the number of primes where the reduction is split multiplicative is an important invariant considered already by several authors (see, e.g., [44], Conjecture 4, [12] Theorem 3, or [65], Conjecture, page 30). Our first theorem answers positively a conjecture of Agashe in [1], Conjecture 2.2.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve which has everywhere semi-stable reduction, and assume that $E(\mathbb{Q})_{tors}$ contains an element of order $N \geq 3$. Then there exists a prime p where $E/\mathbb{Q}$ has split multiplicative reduction modulo p.*

We explain in Theorem 2.7 how Theorem 1.1 implies in fact a slightly stronger form of Agashe's Conjecture 2.2. The difficult cases in the above theorem are the cases where $N = 3$ and 4. The curve with Cremona label $37a1$ (resp. $102a1$, $210d2$) is an example of a semi-stable elliptic curve with $E(\mathbb{Q})_{tors}$ trivial (resp. isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) and with no place of split multiplicative reduction.

It is not immediately clear that a non-trivial generalization of Theorem 1.1 to elliptic curves over a number field $K/\mathbb{Q}$ of degree $d > 1$ can be found if we only replace in the statement of

Date: August 25, 2022.

Theorem 1.1 the hypothesis $N \geq 3$ with $N \geq g(d)$ for some appropriate function $g(d)$. We discuss this point further in Remark 6.12. To be able to formulate a statement for general number fields $K/\mathbb{Q}$ inspired by Theorem 1.1, we introduce the following terminology.

Let K_v be any discrete valuation field with ring of integers $\mathcal{O}_{K_v}$, uniformizer π_v, and residue field k_v of characteristic $p \geq 0$. Let E/K_v be an elliptic curve. Let $\mathcal{E}/\mathcal{O}_{K_v}$ denote the Néron model of E/K_v. The special fiber $\mathcal{E}_{k_v}/k_v$ of $\mathcal{E}$ is the extension of a finite étale group scheme Φ/k_v, called the *group of components*, by a connected smooth group scheme $\mathcal{E}^0_{k_v}/k_v$, the *connected component of* 0. The elliptic curve E/K_v has *multiplicative reduction* when $\mathcal{E}^0_{k_v}/k_v$ is a torus, and *split multiplicative reduction* when this torus is isomorphic to the multiplicative group $\mathbb{G}_{m,k_v}/k_v$. The order $c_v := |\Phi(k_v)|$ is called the *Tamagawa number* of E/K_v.

Let us now return to the case where K is a global field, and let v be a non-archimedean place of K, with completion K_v and residue field k_v. Let E/K be an elliptic curve. For each place v, let c_v denote the Tamagawa number of E_{K_v}/K_v, and let $c = c(E/K) := \prod_v c_v$.

Given a prime $N \geq 5$, we say that an elliptic curve E/K *is N-special* if

(a) E/K has a K-rational point of order N, and
(b) N does not divide $c(E/K)$.

We note in our next lemma that any elliptic curve E/K with $j(E) \in \mathcal{O}_K$ is N-special for any prime $N \geq 5$, and that if E/K is not N-special, then it has split multiplicative reduction at some place v of K.

Lemma 1.2. *Let K be a number field. Let E/K be an elliptic curve with a K-rational point of prime order $N \geq 5$.*

(i) *If N divides $c(E/K)$, then E/K has split multiplicative reduction at some place v of K.*
(ii) *If $j(E) \in \mathcal{O}_K$, then E/K is N-special.*

Proof. (i) Let v be a place of K, and let $\overline{k_v}$ denote an algebraic closure of k_v. The lemma follows immediately from the properties of the order $|\Phi(\overline{k_v})|$ of the component group: since N divides $c(E/K)$, there exists a place v of K where $|\Phi(\overline{k_v})| \geq 5$. When the reduction is additive, $|\Phi(\overline{k_v})| \leq 4$. In case of split multiplicative reduction, we have $\Phi(k_v) = \Phi(\overline{k_v})$ and this group is cyclic. When the reduction is multiplicative but not split, then $|\Phi(k_v)| = 1$ or 2, depending on whether $|\Phi(\overline{k_v})|$ is odd or even (see, e.g., [34], 10.2.24).

(ii) If $j(E) \in \mathcal{O}_K$, then E/K has everwhere potentially good reduction. Thus at any place v, the reduction is either good, or additive. In both cases, $|\Phi(\overline{k_v})| \leq 4$, and so N cannot divide c_v. □

Remark 1.3 The ratio $c(E/K)/|E(K)_{\mathrm{tors}}|$ is a factor appearing in the leading term of the L-function of E/K in the conjecture of Birch and Swinnerton-Dyer (see, e.g, [17], F.4.1.6). It is natural to wonder what are the possible denominators of this ratio. When $K = \mathbb{Q}$, $\frac{c(E/\mathbb{Q})}{|E(\mathbb{Q})_{\mathrm{tors}}|} \geq 1/5$, with equality only when $E = X_1(11)$ ([40], 2.23). See also [71] for a related question in a wider context. By definition, an N-special curve has a ratio $c(E/K)/|E(K)_{\mathrm{tors}}|$ whose denominator is divisible by N.

Fix an integer $d \geq 1$. Our goal in the remainder of this article is to find conditions on N such that there exist only finitely many N-special elliptic curves E/K over only finitely many number fields K of degree d. As is customary, $\mathbb{Q}(\zeta_n)$ denotes the n-th cyclotomic field generated by a primitive n-th root of unity ζ_n, and $\mathbb{Q}(\zeta_n)^+$ denotes its maximal totally real subfield.

Theorem. *Let $K/\mathbb{Q}$ be a number field of degree d. Let $N \geq 5$ be prime. Let E/K be an N-special elliptic curve.*

(a) (see 2.1) *Assume that $d = 1$ and $N \geq 5$. Then $N = 5$ and $E/\mathbb{Q} = X_1(11)/\mathbb{Q}$.*
(b) (see 3.3) *Assume that $d = 2$ and $N \geq 7$. Then $N = 7$ and E/K is one of four explicit exceptions over the fields $K = \mathbb{Q}(\zeta_5)^+$ and $\mathbb{Q}(\zeta_3)$.*
(c) (see 6.1) *Assume that $d = 3$ and $N \geq 11$. Then $N = 13$ and $K = \mathbb{Q}(\zeta_7)^+$, and E/K is unique, with j-invariant $-28672/3$ and Cremona label 147b1.*

Let us now state our results when $d \geq 4$. Recall that in a number field K, a unit $u \in \mathcal{O}_K^*$ is called *exceptional* if $1 - u$ is also a unit. The number of exceptional units in $\mathcal{O}_K$ is finite, and is bounded explicitly by $2^{8(r+1)}$, where r is the rank of the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$ (see, e.g., [3], 1.1).

A sequence $u_1, \ldots, u_m$ of elements in K such that all differences $u_i - u_j$ with $i \neq j$ are units in $\mathcal{O}_K^*$ is called an *exceptional sequence*. We can always find such a sequence with $m = 2$, taking $u_1 = 0$ and $u_2 = 1$. When $m \geq 2$, we can find a new such sequence $v_i := (u_i - u_1)/(u_2 - u_1)$ with $v_1 = 0$ and $v_2 = 1$, and such that $v_i \in \mathcal{O}_K^*$ when $i \geq 2$. The sequence $0, 1, u$ is exceptional if and only if u is an exceptional unit.

The integer m maximal with the property that there exists an exceptional sequence $u_1, \ldots, u_m$ in K is called the *Lenstra constant* $M(K)$ of K. Any exceptional sequence $0, 1, u_3, \ldots, u_m$ reduces to m distinct elements modulo any maximal ideal $\mathfrak{P}$ of $\mathcal{O}_K$. Thus, $m \leq 2^{[K:\mathbb{Q}]}$ and, better, $m \leq L(K)$, where $L(K)$ denotes the minimum of the norms $|\mathcal{O}_K/\mathfrak{P}|$ over all maximal ideals $\mathfrak{P}$ of $\mathcal{O}_K$.

Theorem 1.4. *Let $K/\mathbb{Q}$ be a quartic number field. Let $N \geq 11$ be prime. Let E/K be an N-special elliptic curve.*

(a) *Suppose that $\mathcal{O}_K^*$ has rank at most 2. Then K is one of only three different fields, listed in the table below. The possible N's are listed in the first column next to the defining polynomial of the field.*

N	field K (degree 4)	rk	#exu	$M(K)$	disc(K)
$11(2), 13(j = 0)$	$x^4 - x^3 - x^2 + x + 1$	1	20	6	117
$11(4)^*$	$x^4 - x^3 + 2x - 1$	2	54	9	-275
$11(2)$	$x^4 - x - 1$	2	54	7	-283
$11(2), 13, \mathbf{17}$	$x^4 - x^3 - 3x^2 + x + 1$	3	162	10 or 11	725

(b) *Suppose that K has unit rank 3. Assume the conjecture that if $F/\mathbb{Q}$ is a quartic field, then $M(F) \leq 4$ except for finitely many explicit exceptions. Then K is the unique field with unit rank 3 appearing in the table above, and the possible N's are listed next to its defining polynomial.*

1.5 In the above table, we have listed the known quartic fields K where there exists at least one N-special elliptic curve E/K with $N \geq 11$. The first column lists all the N's for which such an elliptic curve exists over the field K. A number field K of degree d and signature (r_1, r_2) with $r_1 + 2r_2 = d$ has unit rank $r_1 + r_2 - 1$. The column 'rk' in the table gives the rank of the unit group $\mathcal{O}_K^*$. The column #exu gives the number of exceptional units in $\mathcal{O}_K^*$. The last column gives the discriminant $\mathrm{disc}(K)$ of K. Its sign is given by $(-1)^{r_2}$.

A notation of the form $N(c)$ is used to denote that exactly c non-isomorphic N-special elliptic curves were found over that field. The notation $N(c)^*$ indicates in addition that at least one of them has integral j-invariant. In the case of $11(4)^*$ above, exactly two of the four have this property, and are conjugated. They do not have complex multiplication. When the j-invariant of the curve is short to write down, we provide it, as in the notation $13(j = 0)$.

The reader will note that in the table above, the number of N-special elliptic curves E/K when $N = 11$ is always even. This is a general fact proved in Proposition 5.8 when K does not contain $\mathbb{Q}(\zeta_{11})^+$.

A completely analogous statement to Theorem 1.4 in the case of quintic fields can be found in Theorem 6.6 and Conjecture 6.7. The proofs of Theorem 1.4 and Theorem 6.6 are based on the following intrinsic property that a field K enjoys when there exists an N-special elliptic curve E/K.

Let $K/\mathbb{Q}$ be a number field. Let $N \geq 7$ be a prime. Let E/K be an N-special elliptic curve. *We conjecture under these hypotheses that $M(K) \geq (N-1)/2$, and we prove this conjecture for $N \leq 23$ in Theorem 4.3.* When E/K has potentially good reduction, this statement was proved by Mestre ([47], Théorème 1). When $N = 11$, the lower bound can be slightly improved, and we show in Theorem 4.3 (ii) that in this case $M(K) \geq 6$.

Theorem 4.3 can be made completely explicit. Recall that the modular curve $X_1(N)/\mathbb{Q}$ is birational to a plane curve given by an equation $F_N(r, s) = 0$ called the raw form equation of $X_1(N)$. Theorem 4.3 shows that when $N \geq 11$, an N-special elliptic curve E/K corresponds to a point (r_0, s_0) on the plane curve $F_N(r, s) = 0$ where both r_0 and s_0 are exceptional units in $\mathcal{O}_K^*$. This suggests the following algorithm for finding all the N-special curves over a given field K of low degree d. First, given d, Proposition 3.1 gives an explicit upperbound for N. For each allowed N, find all the points (r_0, s_0) with $F_N(r_0, s_0) = 0$, where both r_0 and s_0 are exceptional units in $\mathcal{O}_K^*$.

This algorithm works well for sextic and septic number fields, and we are able to check, using the tables of number fields in [21], that there are indeed surprisingly few N-special elliptic curves with $N \geq 17$ over such fields. We conjecture the finiteness of the number of N-special curves over such fields in 7.1 and 7.8. The data obtained for fields of degrees 8 through 12 is found in [41].

In view of Theorem 4.3, to prove the finiteness of the number of N-special elliptic curves E/K over all fields of degree d when $N > 2d + 1$, it would suffice to show that *there are only finitely many fields of degree d with $M(K) \geq d + 1$*. This statement is true for $d = 2, 3$. The data that we computed supports conjecturing that this statement is true when $d = 4$ or 5 (see 6.4 and 6.9). When $d = 7$, we prefer to call this statement a question (see 7.10). When $d = 6$, and in general when d is not prime, the finiteness when $M(K) \geq d+1$ does not hold and the bound needs to be adjusted (see 7.6). In the proofs of Theorem 1.4 in degree

4 and of Theorem 6.6 in degree 5, we use results of Leutbecher and Martinet on the Lenstra constant $M(K)$ when the unit rank is at most 2. We conclude this article in Section 8 with a discussion of N-special abelian varieties of higher dimension.

It is our pleasure to thank Christian Wuthrich for some Sage [61] advice, and Skip Garibaldi, David Krumm, Mentzelos Melistas, Jim Stankewicz, and Nicholas Triantafillou for helpful conversations.

2. Elliptic curves over $\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. Mazur [43] showed that $N = 1, \dots, 10$, or 12. The proof of Theorem 1.1 proceeds through a case-by-case analysis of each of the possible values of N.

Proposition 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N.*

(a) *If $\mathbf{N = 7}$, then 7^2 divides $c(E/\mathbb{Q})$, except for the curve $26b1$ in [8], which has 7 dividing $c(E/\mathbb{Q})$. In particular, $E/\mathbb{Q}$ is not N-special.*

(b) *If $\mathbf{N = 5}$, then 5 divides $c(E/\mathbb{Q})$, except for the curve $11a3$ in [8] which has split multiplicative reduction at $p = 11$ but has $c_{11} = 1$. In particular, $E/\mathbb{Q}$ is N-special only when $E = X_1(11)$.*

Proof. (a) Follows directly from [40], 2.10. Part (b) follows immediately from [40], 2.7, after verifying that the curve $11a3$ in [8] has split multiplicative reduction at $p = 11$ with $c_{11} = 1$. □

Note that it follows from Proposition 2.1 that if $E/\mathbb{Q}$ is an elliptic curve with integral j-invariant, then it cannot have a $\mathbb{Q}$-rational torsion point of order $N = 5$ or 7. This statement was proved already in [16], page 6.

2.2 For our next two propositions, we will use the following notation. Let K be any field. Let E/K be an elliptic curve and $P \in E(K)$. We first translate so that $P = (0, 0)$ and E/K can be given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$

Then $[-1]P = (0, -a_3)$, and P has order 2 if and only if $a_3 = 0$. When $a_3 \neq 0$, we can make the change of variables $y = Y + a_4/a_3$ and assume that we have an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Since $[2]P = (-a_2, a_1a_2 - a_3)$, we find that P has order 3 if and only of $a_2 = 0$.

Assume that P has order 3, so that $a_2 = 0$. Then $c_4 = a_1(a_1^3 - 24a_3^3)$ and $\Delta = a_3^3(a_1^3 - 27a_3^3)$. We find that either $a_1 = 0$, in which case the j-invariant of E is 0, and thus E/K has everywhere potentially good reduction, or $a_1 \neq 0$, and we can renormalize so that the equation is

$$y^2 + xy + \lambda y = x^3$$

for some $\lambda \in K$.

Assume now that P does not have order 2 or 3. Then we can renormalize so that the equation has the form

$$E(b, c): \quad y^2 + (1 - c)xy - by = x^3 - bx^2 \tag{2.1}$$

We have $[-1]P = (0, b)$, $[-2]P = (b, 0)$, $[2]P = (b, bc)$, and $[3]P = (c, b - c)$. We find that P has order 4 if and only if $b \neq 0$ and $(0, b) = (c, b - c)$ or, in other words, if $c = 0$.

The Weierstrass equation for $E(b, c)$ is called *Kubert $E(b, c)$-normal form* in [48], section 3, page 111, as its first appearance in print is found in [24], Table 3, page 217.

Proposition 2.3 (Case N=4). *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 4$. Assume that $E/\mathbb{Q}$ has semi-stable reduction. Then there exists at least one prime ideal (p) where $E/\mathbb{Q}$ has split multiplicative reduction.*

Proof. Let K be any field. It follows from the above discussion in 2.2 that there exists $\lambda \in K$ such that an elliptic curve E/K with a point of order $N = 4$ can be given by a Weierstrass equation of the form

$$E_\lambda : \quad y^2 + xy - \lambda y = x^3 - \lambda x^2$$

with $P = (0, 0)$. The invariants of E_λ are:

$$\begin{aligned} \Delta(\lambda) &= \lambda^4(1 + 16\lambda), \\ c_4(\lambda) &= 16\lambda^2 + 16\lambda + 1. \end{aligned}$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is of type I_{4m}. It is split because the reduction of the equation modulo $\mathfrak{P}$ clearly has two distinct tangent lines at the singular point $(0, 0)$.

We are now reduced to consider only the case where $\mu := 1/\lambda \in \mathcal{O}_K$. The statement of the proposition may fail to hold when $\mathbb{Q}$ is replaced by a number field K with infinitely many units. Indeed, when $\mu \in \mathcal{O}_K^*$, we find that the curve E_λ has multiplicative reduction at each prime $\mathfrak{P}$ which contains the discriminant $\lambda^4(1 + 16\lambda)$, since one easily checks that in this case $c_4 \notin \mathfrak{P}$. It is possible to find examples where the reduction at all such $\mathfrak{P}$ is not split multiplicative. On the other hand, when $K = \mathbb{Q}$, we need only consider $\mu = \pm 1$. When $\mu = 1$, we obtain the curve $17a4$, with split multiplicative reduction at $p = 17$, and when $\mu = -1$, we obtain the curve $15a8$, with split multiplicative reduction at $p = 5$.

Let us return to the case where K is a general number field, and assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\mu) > 0$. Let π denote a uniformizer of the local ring $\mathcal{O}_{K,\mathfrak{P}}$, and write $\mu = u\pi^m$, with $u \in \mathcal{O}_{K,\mathfrak{P}}^*$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equations are:

$$\begin{aligned} \text{If } m = 2z : &\quad y^2 + u\pi^z xy - u^2\pi^z y = x^3 - ux^2, \\ \text{If } m = 2z + 1 : &\quad y^2 + u\pi^{z+1} xy - u^2\pi^{z+2} y = x^3 - u\pi x^2. \end{aligned} \tag{2.2}$$

The discriminant of the second equation is $u^7\pi^{2z+7}(u\pi^{2z+1} + 16)$. We claim that the case $m = 2z+1$ cannot happen when $\mathfrak{P}$ is coprime to 2. Indeed, the second equation is such that over $K(\sqrt{\pi})$, the change of variables $X = x\sqrt{\pi}^{-2}$ and $Y = y\sqrt{\pi}^{-3}$ produces a new equation

$$Y^2 + u\sqrt{\pi}^{2z+1} XY - u^2\sqrt{\pi}^{2z+1} Y = X^3 - uX^2.$$

It is clear that since $\mathfrak{P}$ is coprime to 2, reducing this equation modulo $\sqrt{\pi}$ produces a plane curve with a node, so that the reduction is multiplicative. One checks with Tate's algorithm [66] that this curve has in fact reduction of type I_{4z+2}. It follows that over K, the reduction of the elliptic curve is either of type I_{2z+1}, or of type I_n^* for some $n > 0$. The former case is

not possible, since the discriminant of the Weierstrass equation over K is exactly divisible by π^{2z+7}. It follows that when m is odd, the reduction at $\mathfrak{P}$ is not semi-stable, and this case cannot happen under our hypotheses.

Let now $K = \mathbb{Q}$. Our previous discussion implies that we can assume that we are in one of the following cases (a), (b), or (c).

Case (a): *Either* $\mu = \pm(2^z u)^2$, *with* $u > 1$ *odd and* $z \geq 0$, *or* $\mu = 2^{2z}$ *with* $z > 0$. In these cases, $\mu = \pm\nu^2$ with $\nu \in \mathbb{Z}$, and the curve can be given by the integral Weierstrass equation

$$y^2 + \nu xy - (\pm\nu)y = x^3 - (\pm x^2).$$

Let p be an odd prime that divides u. If $\mu < 0$, we find by reducing the above equation modulo p that the reduction is split multiplicative. Assume now that $\mu = \nu^2 > 0$. The discriminant of the equation $y^2 + \nu xy - \nu y = x^3 - x^2$ is $\mu(\mu + 16)$, with $c_4 = \mu^2 + 16\mu + 16$. Since the odd prime p divides μ, we find that there exists at least one odd prime q that divides $\mu + 16$. In case $\mu = 2^{2z}$, we similarly find that there exists at least one odd prime q that divides $\mu + 16$, unless $\mu = 16$. When $\mu = 16$, the curve is $32a4$ and has additive reduction at 2.

We claim that the reduction at q is split. Indeed, since q cannot divide c_4, we first find that the reduction at q is multiplicative. Since $P = (0, 0)$ and $[2](P) = (1, 0)$ do not reduce to the singular point modulo q, we find that the connected component of zero of the Néron model contains a k-point of order 4. On the other hand, any odd prime q dividing $\nu^2 + 16$ is such that -1 is a square modulo q. Thus, $q \equiv 1 \pmod 4$. It follows that the connected component of zero has order $|k| - 1$ if it has a point of order 4, and thus the reduction must be split.

Case (b): $\mu = -2^{2z}$ *for some* $z > 0$. We claim that the reduction of such a curve is split multiplicative at 2 when $z \geq 5$. When $z = 1$ or 3, the curves are $24a4$ and $24a3$, and are not semi-stable at 2. When $z = 2$, the equation does not define an elliptic curve, and when $z = 4$, the curve is $15a7$, and has split multiplicative reduction at 5 only.

Note that in this family of elliptic curves, there are examples where the curve has split multiplicative reduction only at 2, such as the curve $42a4$ when $z = 5$, and $2046g4$ when $z = 7$. This happens every time $2^{2z-4} - 1$ is divisible only by primes that are congruent to 3 modulo 4.

Let $\nu = 2^z$ with $z \geq 5$. We start with the equation $y^2 - \nu xy - \nu y = x^3 + x^2$ and following Tate's algorithm [66], we make the change of variables $y = Y + x$, giving us a new equation $Y^2 + (2 - \nu)xY - \nu Y = x^3 + \nu x^2 + \nu x$. This equation is not minimal, and we can now make the change of variable $v = Y/8$ and $u = x/4$ to obtain the minimal equation at 2:

$$v^2 + (1 - \nu/2)uv - (\nu/8)v = u^3 + (\nu/4)x^2 + (\nu/16)x.$$

Since $z \geq 5$, we find that the reduction modulo 2 is $v^2 + uv = u^3$, showing split multiplicative reduction at 2, as desired.

Case (c): $\mu = 2^{2z+1}u$ *with* u *odd and* $z \geq 0$. We claim that the reduction of such a curve is not semi-stable at (2). We start by recalling that

$$j(E_\lambda) = \frac{(16\lambda^2 + 16\lambda + 1)^3}{\lambda^4(1 + 16\lambda)} = \frac{(16 + 16\mu + \mu^2)^3}{\mu(\mu + 16)}$$

An explicit computation of the valuation at (2) of the j-invariant of E shows that if $\mathrm{ord}_2(\mu) > 8$, then E_λ has potentially multiplicative reduction at (2) since $\mathrm{ord}_2(j) < 0$. In this case, we apply Tate's algorithm [66] starting with the equation (2.2) at Second Branch 7) on page 50, and find that the reduction at (2) is of type I_n^* for some $n > 0$ and is thus not semi-stable.

When $0 < \mathrm{ord}_2(\mu) < 8$, we find that $\mathrm{ord}_2(j) > 0$. In these cases where $\mathrm{ord}_2(j) > 0$, the reduction at (2) is potentially good, and we argue as follows to show that at (2) the reduction cannot be good and thus is additive. Assume that the curve has good reduction at (2). The curve contains a K-rational torsion point of order 4, and modulo 2, this point cannot be contained in the kernel of the reduction. Thus the reduction modulo (2) is a curve with a k-rational torsion point of order 2 and, hence, it is ordinary. Over $\mathbb{F}_2$, only the curve with j-invariant 0 is supersingular. Thus, we find that $\mathrm{ord}_2(j(E_\lambda)) = 0$, a contradiction. □

Proposition 2.4 (Case N=3). *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 3$. Assume that $E/\mathbb{Q}$ has semi-stable reduction. Then there exists at least one prime ideal (p) where $E/\mathbb{Q}$ has split multiplicative reduction.*

Proof. Let K be any field. Let E/K be an elliptic curve E/K with j-invariant not equal to 0 and with a point P of order 3. It follows from the discussion in 2.2 that there exists $\lambda \in K$ such that E/K can be given by a Weierstrass equation of the form

$$E_\lambda : \quad y^2 - xy - \lambda y = x^3$$

with $P = (0, 0)$. The invariants of E_λ are:

$$\begin{aligned} \Delta(\lambda) &= \lambda^3(1 - 27\lambda), \\ c_4(\lambda) &= 1 - 24\lambda. \end{aligned}$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is of type I_{3m}. It is split because the reduction of the equation modulo $\mathfrak{P}$ clearly has two distinct tangent lines at the singular point $(0, 0)$.

We are now reduced to consider only the case where $\mu := 1/\lambda \in \mathcal{O}_K$. The Weierstrass equation E_λ might not be integral, but the following one is:

$$y^2 - \mu xy - \mu^2 y = x^3. \tag{2.3}$$

The new discriminant is $\mu^8(\mu - 27)$, with $c_4 = \mu^3(\mu - 24)$. The statement of the proposition may fail to hold when $\mathbb{Q}$ is replaced by a number field K with infinitely many units. Indeed, when $\mu \in \mathcal{O}_K^*$, we find that the curve E_λ has multiplicative reduction at each prime $\mathfrak{P}$ which contains the discriminant $\mu^8(\mu - 27)$, since one easily checks that in this case $c_4 \notin \mathfrak{P}$. It is possible to find examples where the reduction at all such $\mathfrak{P}$ is not split multiplicative. On the other hand, when $K = \mathbb{Q}$, we need only consider $\mu = \pm 1$. When $\mu = 1$, we obtain the curve $26a3$, with split multiplicative reduction at $p = 13$, and when $\mu = -1$, we obtain the curve $14a4$, with split multiplicative reduction at $p = 7$.

Let us return to the case where K is a general number field and assume now that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\mu) > 0$. Let π denote a uniformizer of the local ring $\mathcal{O}_{K,\mathfrak{P}}$, and write $\mu = u\pi^m$, with $u \in \mathcal{O}_{K,\mathfrak{P}}^*$. We claim that if m is not divisible by 3, then the reduction modulo π is not semi-stable, and thus we need not consider this case any further.

More precisely, it follows from Tate's Algorithm [66] that when $m \equiv 1 \pmod 3$, then the reduction is of type IV, and when $m \equiv 2 \pmod 3$, then the reduction is of type IV*.

To prove this, write $m = 3s + i$, with $i = 0, 1$, or 2, and $s \geq 0$. In general, the equation (2.3) is not minimal, and we can make the following change of variables: $Y := y/\pi^{6s}$ and $X := x/\pi^{4s}$. The new equation is still integral, and has the form

$$Y^2 - u\pi^{s+i}XY - u^2\pi^{2i}Y = X^3. \tag{2.4}$$

When $i = 2$, the above equation is still not minimal, and we make the further change of variables $Y' := Y/\pi^3$ and $X' := X/\pi^2$ to get

$$Y'^2 - u\pi^{s+i-1}X'Y' - u^2\pi^{2i-3}Y' = X'^3. \tag{2.5}$$

When $i = 1$, the equation (2.4) is minimal and Tate's algorithm [66] shows that the reduction is of type IV. When $i = 2$, the equation (2.5) is minimal and Tate's algorithm shows that the reduction is of type IV*.

Let us assume now that $K = \mathbb{Q}$. We are reduced to consider the case where $\mu = t^3$ for some $t \in \mathbb{Z}$. The curve $y^2 - \mu xy - \mu^2 y = x^3$ can be given by the equation $y^2 - txy - y = x^3$, with discriminant $(t^3 - 27)$, and $c_4 = t(t^3 - 24)$. Let τ be a prime that divides $(t^3 - 27)$. If τ also divides c_4, then τ divides $3t$. It follows in this case that $\tau = 3$. Thus, unless $\tau = 3$, we find that $E/\mathbb{Q}$ has multiplicative reduction at τ.

Suppose that there exists a prime $\tau \neq 3$ which divides $t^2 + 3t + 9 = (t^3 - 27)/(t - 3)$. We claim that in this case the reduction at τ is split multiplicative. Indeed, in the residue field $\mathbb{F}_\tau$, we find that we have a non-trivial third root of unity, since the class of $\tau/3$ satisfies the equation $z^2 + z + 1$. It follows that 3 divides $\tau - 1$. Now consider the reduction of the 3-torsion point $(0, 0)$ modulo τ. The reduced Weiestrass equation shows that the reduction is not singular. Thus the point $(0, 0)$ reduces to a point of order 3 in the connected component of the Néron model. The set of $\mathbb{F}_\tau$-rational points of the connected component has order $\tau - 1$ in the split case, and $\tau + 1$ in the non-split case. Since 3 divides $\tau - 1$, we find that the connected component of the Néron model cannot have order $\tau + 1$. In other words, the connected component of the Néron model must be $\mathbb{G}_m/\mathbb{F}_\tau$, as claimed.

When $K = \mathbb{Q}$, and $\mu = t^3 \in \mathbb{Z}$, we leave it to the reader to check that the solutions to the equation $t^2 + 3t + 9 = \pm 3^s$ with $t \in \mathbb{Z}$ and $s \in \mathbb{Z}_{\geq 0}$, are $(t, s) = (0, 2), (3, 3), (-3, 2)$, and $(-6, 3)$. The case where $t = 3$ does not correspond to an elliptic curve. The cases $t = 0$, $t = -3$, and $t = -6$ produce the elliptic curves $27a3$, $54a3$, and $27a4$, respectively, with additive reduction at $p = 3$. Thus when the reduction of $E/\mathbb{Q}$ is everywhere semi-stable as we assume, we always find a prime of split multiplicative reduction among the divisors of $t^2 + 3t + 9$. □

Proof of Theorem 1.1. When $N = 3, 4$, Theorem 1.1 follows directly from 2.4 and 2.3. When $N = 5, 7$, Theorem 1.1 follows from 2.1, using Lemma 1.2 (i). Finally, if $N > 7$ is prime, and $E/\mathbb{Q}$ does not have a place of split multiplicative reduction, then Lemma 1.2 (i) shows that $E/\mathbb{Q}$ is N-special. This contradicts Proposition 3.1. □

Before we give the proof of Agashe's Conjecture in Theorem 2.7, we briefly consider the elliptic curves over $\mathbb{Q}$ which have a $\mathbb{Q}$-rational point of order $N = 2$ and *prime* conductor p. When $p \neq 2, 3, 17$, such curves are studied in [62], Thm. 2. Such a curve exists if and only if $p = A^2+64$ for some integer A. When p is of that form and we choose $A \equiv 1 \pmod 4$, exactly

two such elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ exist, with E having equation $y^2 = x^3 + Ax^2 - 16x$, and E' is isomorphic to $E/ < (0,0) >$, with equation $y^2 = x^3 - 2Ax^2 + px$. As a complement to Theorem 1.1, we note:

Proposition 2.5. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 2$ and prime conductor p. Then E has split multiplicative reduction at p.*

Proof. We use the modularity of elliptic curves over $\mathbb{Q}$ to find that there are no such curves with conductor 2 or 3, and exactly four curves of conductor 17. One checks directly that for these curves, the reduction is split at $p = 17$. When $p \neq 2, 3$ and 17, we apply the results of [62] recalled above. When $p = A^2 + 64$, it is clear that $p \equiv 1 \pmod 8$, and the proposition follows then from Lemma 2.6 (b) for the equation $y^2 = x^3 + Ax^2 - 16x$. For the equation $y^2 = x^3 - 2Ax^2 + px$, one can check directly that $-2A$ is a square in $\mathbb{Z}/p\mathbb{Z}$, showing that the reduction is split. □

Lemma 2.6. *Let K be any number field, and let $A \in \mathcal{O}_K$ and $u \in \mathcal{O}_K^*$. Consider the elliptic curve E/K with equation $y^2 = x^3 + Ax^2 + 16ux$. Let $\mathfrak{P}$ denote a prime ideal of $\mathcal{O}_K$ which divides $A^2 - 64u$ and is coprime to (2). Write $|\mathcal{O}_K/\mathfrak{P}| = p^f$. Then E/K has multiplicative reduction at $\mathfrak{P}$. Moreover,*

(a) *If $u = 1$, then the reduction is split multiplicative at $\mathfrak{P}$ if $p^f \equiv 1 \pmod 4$.*
(b) *If $u = -1$, then the reduction is split multiplicative at $\mathfrak{P}$ if and only if $p^f \equiv 1 \pmod 8$.*

Proof. Working in $\mathcal{O}_{K_\mathfrak{P}}$, we can make the change of variables $X = x + A/2$, and reducing modulo $\mathfrak{P}$, we find an equation of the form $y^2 = X^3 - \overline{A/2}X^2$. Note that $\mathfrak{P}$ is coprime to (A). Hence, the reduction is multiplicative, and it is split multiplicative if and only if $-\overline{A/2}$ is a square in $\mathcal{O}_K/\mathfrak{P}$.

(a) When $\mathfrak{P}$ divides $A^2 - 64$, it must divide either $A - 8$ or $A + 8$. Therefore, either $-(A/2) \equiv 2^2$, or $-(A/2) \equiv -2^2$ modulo $\mathfrak{P}$. In the latter case, when $p^f \equiv 1 \pmod 4$, then -1 is a square in $\mathcal{O}_K/\mathfrak{P}$ and in that case also, $-\overline{A/2}$ is a square in $\mathcal{O}_K/\mathfrak{P}$, as desired.

(b) We always have $(A/2)^2 \equiv 16u \mod \mathfrak{P}$. When $u = -1$, then $-A/2 \equiv c^2$ implies that $(A/2)^2 \equiv c^4 \equiv -16$. It follows that the equation $x^4 = -1$ has a root in $\mathcal{O}_K/\mathfrak{P}$ and, thus, 8 divides $p^f - 1$. Assume now that 8 divides $p^f - 1$, and let d be such that $d^4 \equiv -1$. Then we find that $-A/2 \equiv (2d)^2$ or $(2d^3)^2$. □

Theorem 2.7. *Agashe's Conjecture* 2.2 *in* [1] *is true, even without the hypothesis that $E/\mathbb{Q}$ be optimal.*

Proof. Agashe's Conjecture 2.2 in [1] is phrased in terms of root numbers as follows:

Let $E/\mathbb{Q}$ be an optimal elliptic curve with squarefree conductor. Assume that the odd part of $E(\mathbb{Q})_{tors}$ is not trivial. Then the root number w_p at p equals -1 for at least one prime p that divides the conductor of E.

Let K be a number field, and let v denote a place of K. Recall that when E_{K_v}/K_v has semi-stable reduction and v is non-archimedean, $w_v = 1$ if the reduction is good or the torus $\mathcal{E}^0_{k_v}/k_v$ is not split, and $w_v = -1$ when $\mathcal{E}^0_{k_v}/k_v$ is split (see, e.g., [11], Thm 3.1).

The hypothesis that $E/\mathbb{Q}$ be optimal is not needed to apply Theorem 1.1. The hypothesis that $E/\mathbb{Q}$ has squarefree conductor is equivalent to the fact that $E/\mathbb{Q}$ has everywhere semi-stable reduction. Thus Theorem 1.1 implies that there exists a prime p where $E/\mathbb{Q}$ has split multiplicative reduction modulo p, i.e., that there exists a prime p with $w_p = -1$. □

3. Elliptic curves over quadratic fields

Let N be prime. The condition that an elliptic curve E/K is N-special implies an upper-bound for N in terms of $d := [K : \mathbb{Q}]$, as we now explain.

Proposition 3.1. *Let $N \geq 5$ be prime. Let $K/\mathbb{Q}$ be a number field of degree d. Let E/K be an N-special elliptic curve. Then $N \leq 2^d + 1 + 2\sqrt{2^d}$.*

In particular, when $d = 1$, $N \leq 5$, when $d = 2$, $N \leq 7$, and when $d = 3$, $N \leq 13$. If in addition $d = 4$, then $N \leq 17$. If $d = 5$, then $N \leq 19$, or $N = 31$ or 41. If $N = 23$, then $d \geq 7$.

Proof. When $N \geq 5$, the reduction of E/K cannot be additive at any prime $\mathfrak{P}$ of $\mathcal{O}_K$ above a prime p, except possibly when $p = N$. Indeed, the component group in the presence of additive reduction has order bounded by 4. Since a torsion point of order prime to p reduces injectively in the special fiber of the Néron model, and since an additive group in characteristic p contains only torsion points of order p, we find that if the reduction is additive, we must have $p = N$.

When N does not divide $c(E/K)$, the point of order $N \geq 5$ cannot reduce injectively in the component group at any place of bad reduction. Thus the order of the group of $k_{\mathfrak{P}}$-rational points on the connected component of the Néron model must be divisible by N. In case of multiplicative reduction, we find that $N \leq |k_{\mathfrak{P}}| + 1$, and in the case of good reduction, we can use the Weil bound $N \leq |k_{\mathfrak{P}}| + 1 + 2\sqrt{|k_{\mathfrak{P}}|}$. Thus, when N does not divide $c(E/K)$ and $N \geq 5$, we can apply this discussion with $p = 2$ and we find that $N \leq 2^d + 1 + 2\sqrt{2^d}$.

Assume now that $d = 4$. We have $N \leq 2^d + 1 + 2\sqrt{2^d} = 25$, and thus we need to show that the cases $N = 19$ or $N = 23$ cannot occur. If the reduction is multiplicative at any prime above (2), the bound $N \leq 17$ holds. Assume then that there exists a unique maximal ideal $\mathfrak{P}$ above (2) with residue field of size $q := 2^4$. An elliptic curve $\mathcal{E}_{\mathbb{F}_q}/\mathbb{F}_q$ cannot have an $\mathbb{F}_q$-rational point of order 19 or 23. This follows immediately from the list of possible orders for $|\mathcal{E}_{\mathbb{F}_q}(\mathbb{F}_q)|$ given in [70], Theorem 4.1. Indeed, the order of $|\mathcal{E}_{\mathbb{F}_q}(\mathbb{F}_q)|$ can only be an integer in the interval $[9, 25]$ of the form $17 + a$ with either a odd, or $a = 0, \pm 4, \pm 8$.

When $N = 23$ and $d = 5, 6$ we argue in the same way. First we can check that there exists a unique maximal ideal $\mathfrak{P}$ above (2) with residue field of size $q := 2^d$. An elliptic curve $\mathcal{E}_{\mathbb{F}_q}/\mathbb{F}_q$ cannot have an $\mathbb{F}_q$-rational point of order 23. Indeed, when $d = 5$, the order of $|\mathcal{E}_{\mathbb{F}_q}(\mathbb{F}_q)|$ can only be an integer in the interval $[22, 44]$ of the form $33 + a$ with either a odd, or $a = 0, \pm 8$. Thus the order of the group cannot equal 23 (and for later use, we note that it cannot be equal to 37 or 43 either, but it might equal 17 or 19). When $d = 6$, the order of $|\mathcal{E}_{\mathbb{F}_q}(\mathbb{F}_q)|$ can only be an integer in the interval $[49, 81]$ of the form $65 + a$ with either a odd, or $a = 0, \pm 8, \pm 16$. Thus the order of the group cannot equal 69 and N cannot equal 23. Note that N could a priori equal $29, 31, 37$, and 73, and as we show in Remark 7.3, $N = 37$ does occur when $d = 6$.

Finally, assume that $d = 5$. It might be possible in this case to have $N = 31$ when (2) is prime in $\mathcal{O}_K$ and the reduction is split multiplicative at (2). When the reduction at (2) is good, we already showed that $N = 23$ is not possible and noted at the same time that the same argument also shows that $N \neq 37, 43$. □

Remark 3.2 Let E/K be an elliptic curve with a K-rational point of order N. When $[K : \mathbb{Q}] = 3$, Parent proved that the possible prime values of N are $2, 3, 5, 7, 11$, and 13 ([56], [57]). The same statement follows directly from Proposition 3.1 under the additional hypothesis that E/K be N-special. When $[K : \mathbb{Q}] = 4$, it is expected that a K-rational torsion point of order N can exist only if $N \leq 17$, even when the curve is not N-special.

Theorem 3.3. *Let $N \geq 7$ be prime. Let K be a quadratic number field, and let E/K be an N-special elliptic curve. Then $N = 7$, and there exist only four N-special elliptic curves, two conjugated curves over $K = \mathbb{Q}(\sqrt{5})$, and two conjugated curves with potentially good reduction over $K = \mathbb{Q}(\sqrt{-3})$.*

Proof. That $N \leq 7$ follows immediately from Proposition 3.1. The determination of the N-special curves follows immediately from [40], 2.10 (b) and (c), after listing all exceptions over the two quadratic fields with exceptional units. Example 3.4 gives the complete list of N-special curves over quadratic fields. □

Example 3.4 Let $N = 7$. We list in this example the four N-special elliptic curves E/K when K is a quadratic field. Let $K = \mathbb{Q}(\sqrt{5})$ and let $u := (1 + \sqrt{5})/2$. Consider the elliptic curve E/K given by

$$y^2 - uy = x^3 - ux^2.$$

Then $(0, 0)$ is a K-rational point of order 7. The curve E/K has prime conductor $\mathfrak{P}$, one of the two primes of norm 41, and non-split multiplicative reduction of type I_1 at $\mathfrak{P}$. The conjugated elliptic curve has the same properties. Since these curves have different conductors, they cannot be isomorphic.

Let $K = \mathbb{Q}(\sqrt{-3})$ and let $g := (1 + \sqrt{-3})/2$. Consider the elliptic curve E/K with $j = 0$ given by

$$y^2 + gy = x^3 + (g + 1)x^2 + gx.$$

Then $(0, 0)$ is a K-rational point of order 7. The curve E/K has additive reduction of type II at one of the primes above 7. The conjugated elliptic curve has the same properties.

Remark 3.5 It follows from Theorem 3.3 that if E/K is an elliptic curve over a quadratic field with integral j-invariant, then it cannot have a K-rational torsion point of prime order $N \geq 7$ except when $K = \mathbb{Q}(\zeta_3)$ and $N = 7$. This statement was proved already in [48], Theorem 4 and Table 10. The same authors show that there are only finitely many quadratic fields K each with finitely many elliptic curves E/K with integral j-invariant and a K-rational point of order 5 ([48], Corollaries 1 and 2, and Table 8). When 'integral j-invariant' is replaced by 'E/K is 5-special', the corresponding result is likely to not hold for real quadratic fields (see [40], Remark 2.8).

4. Exceptional Units

Let $F_N(r,s) \in \mathbb{Z}[r,s]$ denote the *raw form equation*[1] of $X_1(N)/\mathbb{Q}$, as in [63], section 2. A list of explicit formulas for $F_N(r,s)$ is given in [64] for $N \leq 101$.

Example 4.1 It may be worth noting that the 'size' of the polynomial $F_N(r,s)$ grows rapidly with N. For instance, in the case of $N = 101$, the file in [64] for $F_N(r,s)$ opens in Notepad with 34516 lines. We list below some small examples of $F_N(r,s)$ which fit on one line.

$$\begin{array}{rcl}
F_3 & = & r,\ F_4 = s,\ F_5 = r-1,\ F_6 = s-1,\ F_7 = r-s \\
F_8 & = & rs - 2r + 1 \\
F_9 & = & r - s^2 + s - 1 \\
F_{10} & = & rs^2 - 3rs + r + s^2 \\
F_{11} & = & r^2 - rs^3 + 3rs^2 - 4rs + s \\
F_{12} & = & r^2 s - 3r^2 + rs + 3r - s^2 - 1 \\
F_{13} & = & r^3 - r^2 s^4 + 5r^2 s^3 - 9r^2 s^2 + 4r^2 s - 2r^2 - rs^3 + 6rs^2 - 3rs + r - s^3
\end{array}$$

Let us consider again the $E(b,c)$-normal form (2.1) and set $b := rs(r-1)$ and $c := s(r-1)$, to obtain a Weierstrass equation with coefficients in the polynomial ring $\mathbb{Z}[r,s]$:

$$E(r,s): \quad y^2 + (1 - s(r-1))xy - rs(r-1)by = x^3 - rs(r-1)x^2.$$

This equation defines an elliptic curve over the field of fractions of $\mathbb{Z}[r,s]$, with the obvious point $P := (0,0)$. We can compute $[n](P) := (X_n(r,s), Y_n(r,s))$, where $[n]$ is the multiplication-by-n map on the elliptic curve. The rational function

$$x_n = x_n(r,s) := X_n(r,s)/b$$

is listed below for $n = 1, \ldots, 11$.

4.2 In our next table, the entry corresponding to $\mathbf{x_i}$ and $\mathbf{x_j}$, when $i \geq 3$ and $j \geq 1$, is the factorization in $\mathbb{Q}(r,s)$ of the rational fraction $x_i - x_j$ in terms of the polynomials $F_3, F_4, \ldots, F_{i+j}$, up to sign. More precisely, we have $x_i - x_j = (-1)^{j-1}(\mathbf{x_i}, \mathbf{x_j})$-entry. The first column thus gives $x_i = x_i - x_1$.

[1]The terminology *raw form* was introduced in [60]. The terminology *exceptional unit* was coined in 1969 by Nagell in [54], section 1. He might be the first author to relate the existence of K-rational torsion points on some elliptic curve E/K to the existence of exceptional units in K (see, e.g., [51], Théorème I and II). Nagell's interest in exceptional units dates back to at least 1928 (see, e.g., [49], Hilfsatz IV, page 17).

	$\mathbf{x_1 = 0}$	$\mathbf{x_2 = 1}$	$\mathbf{x_3}$	$\mathbf{x_4}$	$\mathbf{x_5}$	$\mathbf{x_6}$	$\mathbf{x_7}$	$\mathbf{x_8}$	$\mathbf{x_9}$	$\mathbf{x_{10}}$
$\mathbf{x_3}$	$\frac{1}{F_3} = \frac{1}{r}$	$\frac{F_5}{F_3}$	0							
$\mathbf{x_4}$	$\frac{1}{F_4} = \frac{1}{s}$	$\frac{F_6}{F_4}$	$\frac{F_7}{F_3F_4}$	0						
$\mathbf{x_5}$	$\frac{F_6}{F_5}$	$\frac{F_7}{F_5}$	$\frac{F_8}{F_3F_5}$	$\frac{F_9}{F_4F_5}$	0					
$\mathbf{x_6}$	$\frac{F_7}{F_3F_6^2}$	$\frac{F_4F_8}{F_3F_6^2}$	$\frac{F_9}{F_3F_6^2}$	$\frac{F_{10}}{F_3F_4F_6^2}$	$\frac{F_{11}}{F_3F_5F_6^2}$	0				
$\mathbf{x_7}$	$\frac{F_6F_8}{F_7^2}$	$\frac{F_5F_9}{F_7^2}$	$\frac{F_5F_{10}}{F_3F_7^2}$	$\frac{F_{11}}{F_4F_7^2}$	$\frac{F_6F_{12}}{F_5F_7^2}$	$\frac{F_{13}}{F_3F_6^2F_7^2}$	0			
$\mathbf{x_8}$	$\frac{F_7F_9}{F_4F_8^2}$	$\frac{F_5F_6F_{10}}{F_4F_8^2}$	$\frac{F_5F_{11}}{F_3F_4F_8^2}$	$\frac{F_6F_{12}}{F_4F_8^2}$	$\frac{F_{13}}{F_4F_5F_8^2}$	$\frac{F_7F_{14}}{F_3F_4F_6^2F_8^2}$	$\frac{F_5F_{15}}{F_4F_7^2F_8^2}$	0		
$\mathbf{x_9}$	$\frac{F_8F_{10}}{F_3F_9^2}$	$\frac{F_7F_{11}}{F_3F_9^2}$	$\frac{F_6^2F_{12}}{F_3F_9^2}$	$\frac{F_{13}}{F_3F_4F_9^2}$	$\frac{F_7F_{14}}{F_3F_5F_9^2}$	$\frac{F_{15}}{F_3F_6^2F_9^2}$	$\frac{F_8F_{16}}{F_3F_7^2F_9^2}$	$\frac{F_{17}}{F_3F_4F_8^2F_9^2}$	0	
$\mathbf{x_{10}}$	$\frac{F_9F_{11}}{F_5F_{10}^2}$	$\frac{F_4F_6F_8F_{12}}{F_5F_{10}^2}$	$\frac{F_7F_{13}}{F_3F_5F_{10}^2}$	$\frac{F_6F_7F_{14}}{F_4F_5F_{10}^2}$	$\frac{F_{15}}{F_5F_{10}^2}$	$\frac{F_4F_8F_{16}}{F_3F_5F_6^2F_{10}^2}$	$\frac{F_{17}}{F_5F_7^2F_{10}^2}$	$\frac{F_6F_9F_{18}}{F_4F_5F_8^2F_{10}^2}$	$\frac{F_{19}}{F_3F_5F_9^2F_{10}^2}$	0
$\mathbf{x_{11}}$	$\frac{F_6F_{10}F_{12}}{F_{11}^2}$	$\frac{F_9F_{13}}{F_{11}^2}$	$\frac{F_7F_8F_{14}}{F_3F_{11}^2}$	$\frac{F_7F_{15}}{F_4F_{11}^2}$	$\frac{F_6F_8F_{16}}{F_5F_{11}^2}$	$\frac{F_{17}}{F_3F_6^2F_{11}^2}$	$\frac{F_6F_9F_{18}}{F_7^2F_{11}^2}$	$\frac{F_{19}}{F_4F_8^2F_{11}^2}$	$\frac{F_{10}F_{20}}{F_3F_9^2F_{11}^2}$	$\frac{F_7F_{21}}{F_5F_{10}^2F_{11}^2}$

We can now state the main theorem of this section. The definitions of an *exceptional sequence* and of the *Lenstra constant* $M(K)$ were recalled in the Introduction. Note that if $0, 1, u_3, \ldots, u_n$ is an exceptional sequence, then so is $0, 1, u_3^{-1}, \ldots, u_n^{-1}$.

Theorem 4.3. *Let K be a number field. Let $N \geq 7$ be a prime. Let E/K be an N-special elliptic curve, with a K-rational point P of order N. Let $(r_0, s_0) \in K^2$ be the point with $F_N(r_0, s_0) = 0$ corresponding to the pair $(E/K, P)$. Then*

(i) *If $N = 7$, then r_0 is an exceptional unit.*
(ii) *If $N = 11$, then $0, 1, r_0^{-1}, s_0^{-1}, \frac{s_0-1}{r_0-1}, \frac{r_0-1}{r_0(s_0-1)}$, is an exceptional sequence in $\mathcal{O}_K^*$. In particular, $M(K) \geq 6$.*
(iii) *If $13 \leq N \leq 23$, then $0, 1, r_0^{-1}, s_0^{-1}, \frac{s_0-1}{r_0-1}, x_6(r_0, s_0), \ldots, x_{\frac{N-1}{2}}(r_0, s_0)$, is an exceptional sequence in $\mathcal{O}_K^*$. In particular, $M(K) \geq \frac{N-1}{2}$.*
(iv) *If $23 \leq N \leq 101$, then $M(K) \geq 11$.*

4.4 We conjecture that Part (iii) of Theorem 4.3 holds for any prime $N \geq 13$. The proof of Theorem 4.3 is based on the following conjectural properties of the polynomials $F_N(r, s)$ and of the rational functions $x_3(r, s), \ldots, x_{\frac{N-1}{2}}(r, s)$.

(1) Let $N \geq 7$ be prime. Consider $F_N(r, s)$ as a polynomial in r with coefficients in $\mathbb{Z}[s]$ and let $d_r = d_r(N)$ denote its degree in r. Write this polynomial as

$$F_N(r, s) = g_{d_r}(s)r^{d_r} + g_{d_r-1}(s)r^{d_r-1} + \cdots + g_1(s)r + g_0(s).$$

Then $g_{d_r}(s) = 1$, and $g_0(s) = \pm s^a$ for some integer $a = a(N) > 0$.

(2) Let $N \geq 11$ be prime. Consider $F_N(r,s)$ as a polynomial in s with coefficients in $\mathbb{Z}[r]$, and let $d_s = d_s(N)$ denote its degree in s. Write this polynomial as

$$F_N(r,s) = f_{d_s}(r)s^{d_s} + f_{d_s-1}(r)s^{d_s-1} + \cdots + f_0(r).$$

Then $f_{d_s}(r) = \pm r^b$ for some integer $b = b(N) > 0$.

(3) For each $i \geq 3$ and $1 \leq j < i$, the rational function $x_i - x_j$ can be expressed in terms of the polynomials $F_3, \ldots, F_{i+j}$ only. In other words, the only irreducible polynomials in $\mathbb{Z}[r,s]$ that can divide either the numerator or the denominator of $x_i - x_j$ written in reduced form are, up to sign, the polynomials $F_3, \ldots, F_{i+j}$. Table 4.2 verifies this claim up to $i = 11$.

We conjecture that these properties always hold when N is prime. Properties (1) and (2) can be checked for $N \leq 101$ by inspection of the formulas given in [64]. Conjectural formulas for $d_r(N)$, $d_s(N)$, $a(N)$, and $b(N)$, are given in 4.10 when N is prime. We further discuss these conjectures and possible proof in 4.10, after we give the proof of Theorem 4.3.

4.5 *Proof of Theorem 4.3.* Let $(r_0, s_0) \in K^2$ with $F_N(r_0, s_0) = 0$ corresponding to the given elliptic curve E/K with a K-rational point P of order N. In particular, $(r_0, s_0) \neq (0,0), (1,1)$ and $(1,0)$. Then E/K is isomorphic to the elliptic curve $E(b,c)$ given in Weierstrass equation by

$$y^2 + (1-c)xy - by = x^3 - bx^2$$

where $b = r_0 s_0(r_0 - 1)$ and $c = s_0(r_0 - 1)$. The above isomorphism sends the point P to the point $P_0 := (0,0)$ in $E(b,c)$.

For N prime with $7 \leq N \leq 101$ as in the theorem, we start by proving the following four claims:

(a) Let $\mathfrak{P}$ denote a prime ideal of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(s_0) > 0$. Then $\mathrm{ord}_{\mathfrak{P}}(r_0) \geq 0$, and E/K has reduction modulo $\mathfrak{P}$ of split multiplicative type I_m with m divisible by N.

(b) Let $\mathfrak{P}$ denote a prime ideal of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(s_0) < 0$. Then $\mathrm{ord}_{\mathfrak{P}}(r_0) \neq 0$ and E/K has reduction modulo $\mathfrak{P}$ of split multiplicative type I_m with m divisible by N.

(c) If s_0 is a unit in $\mathcal{O}_K$, then so is r_0.

(d) Assume that r_0 and s_0 are both units in $\mathcal{O}_K$. Let $\mathfrak{P}$ denote a prime ideal of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(r_0 - 1) > 0$. Then E/K has reduction modulo $\mathfrak{P}$ of split multiplicative type I_m with m divisible by N.

Assuming that (a) and (b) hold and that N does not divide $c(E/K)$, we find that s_0 is a unit. From (c), it follows that r_0 is also a unit. Claim (d) then shows that r_0 is an exceptional unit.

Proof of (a): Let $\mathfrak{P}$ denote a maximal ideal of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(s_0) > 0$. As usual, $\mathcal{O}_{K,\mathfrak{P}}$ denotes the localization of $\mathcal{O}_K$ at $\mathfrak{P}$, so that $s_0 \in \mathcal{O}_{K,\mathfrak{P}}$. When $F_N(r,s)$ is written as a polynomial in r with coefficients in $\mathbb{Z}[s]$, it is monic in r (4.4 (1)). Therefore, if $s_0 \in \mathcal{O}_{K,\mathfrak{P}}$, then so does r_0. It follows that the equation $E(b,c)$ has coefficients in $\mathcal{O}_{K,\mathfrak{P}}$. Reducing this equation modulo $\mathfrak{P}$, we find the equation $y^2 + xy = x^3$, which shows that the reduction is split multiplicative since the singular point $(0,0)$ has distinct tangent lines over $\mathcal{O}_K/\mathfrak{P}$. Moreover, the point P_0 reduces to the singular point in reduction. This implies when N is prime that the point P_0 reduces to a point of order N in the group of components of the

special fiber of the Néron model of $E(b,c)$ at $\mathfrak{P}$. Hence, the reduction is of type I_m for some m divisible by N.

Proof of (b): Assume that there exists a maximal ideal $\mathfrak{P}$ of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(s_0) < 0$. When $N = 7$, we have $r_0 = s_0$, and so $\mathrm{ord}_{\mathfrak{P}}(r_0) < 0$. When $N \geq 11$, the highest power of s in $F_N(r,s)$ as a polynomial in s appears in exactly one monomial $r^i s^j$ (4.4 (2)). This shows that when $\mathrm{ord}_{\mathfrak{P}}(s_0) < 0$, then $\mathrm{ord}_{\mathfrak{P}}(r_0) \neq 0$. Let π denote a uniformizer of $\mathcal{O}_{K,\mathfrak{P}}$. Let $v := -\mathrm{ord}_{\mathfrak{P}}(s_0)$. We consider now two separate cases.

Assume first that $-u := \mathrm{ord}_{\mathfrak{P}}(r_0) < 0$. The Weierstrass equation for E/K given by the coefficients $[1-c,-b,-b,0,0]$ is not integral since $b = r_0 s_0(r_0-1)$ and $c = s_0(r_0-1)$, but the following coefficients define an integral equation for E/K:

$$[\pi^{u+v}(1-c), -\pi^{2u+2v}b, -\pi^{3u+3v}b, 0, 0].$$

Moreover, it is easy to check that $\mathrm{ord}_{\mathfrak{P}}(\pi^{2u+2v}b) > 0$, while $\mathrm{ord}_{\mathfrak{P}}(\pi^{u+v}(1-c)) = 0$. The latter fact uses explicitly that $u > 0$, and is the key to the reduction then being is of type I_m for some m divisible by N.

Assume now that $\mathrm{ord}_{\mathfrak{P}}(r_0) > 0$. The equation for E/K given by $[1-c,-b,-b,0,0]$ is not integral, but the following equation is an integral equation for E/K:

$$[\pi^{v}(1-c), -\pi^{2v}b, -\pi^{3v}b, 0, 0].$$

Moreover, it is easy to check that $\mathrm{ord}_{\mathfrak{P}}(\pi^{2v}b) > 0$, while $\mathrm{ord}_{\mathfrak{P}}(\pi^{v}(1-c)) = 0$. Again, the latter fact uses explicitly that $\mathrm{ord}_{\mathfrak{P}}(r_0) > 0$, and is the key to the reduction then being split multiplicative of type I_m for some m divisible by N.

Proof of (c): For N as in the theorem, when $F_N(r,s)$ is written as a polynomial in r with coefficients in $\mathbb{Z}[s]$, its constant term is a power of s (4.4 (1)). It follows immediately that when s_0 is a unit in $\mathcal{O}_K$, then so is r_0.

Proof of (d): When both r_0 and s_0 are units and there exists a maximal ideal $\mathfrak{P}$ of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{P}}(r_0 - 1) > 0$, then the equation $E(b,c)$ is integral at $\mathfrak{P}$ and reduces to $y^2 + xy = x^3$ modulo $\mathfrak{P}$. Again, the reduction is of split multiplicative type I_m with N dividing m.

We have now proved that if N does not divide $c(E/K)$, then $0, 1, r_0$ is an exceptional sequence, and s_0 is a unit. In particular, Part (i) where $N = 7$ is proved. We now assume that $N \geq 11$, and proceed with the proof that the sequence $0, 1, x_3(r_0,s_0), \ldots, x_{\frac{N-1}{2}}(r_0,s_0)$ is exceptional when $N \leq 23$, and that the sequence $0, 1, x_3(r_0,s_0), \ldots, x_{11}(r_0,s_0)$ is exceptional when $23 \leq N \leq 101$. These two statements completely prove Parts (ii), (iii), and (iv), of the theorem, except when $N = 11$ in Part (ii), since the statements prove only that $M(K) \geq 5$ in this case. The proof of Part (ii) is completed by applying Proposition 5.5.

Claim: *When r_0 is an exceptional unit and s_0 is a unit, then $F_m(r_0,s_0) \in \mathcal{O}_K^*$ for all $m = 3, \ldots, N-1$.*

Proof of the claim. Let $\mathfrak{P}$ be any maximal ideal of $\mathcal{O}_K$. Consider the projective scheme $\mathcal{X} \to \mathrm{Spec}\, \mathcal{O}_{K,\mathfrak{P}}$ defined as the projective closure in $\mathbb{P}^2_{\mathcal{O}_{K,\mathfrak{P}}}$ of the plane curve $E(b,c) \subset \mathbb{P}^2_K$. Since r and s are in $\mathcal{O}_K$, so are b and c. The scheme $\mathcal{X}$ is obtained as the closed subscheme of $\mathbb{P}^2_{\mathcal{O}_{K,\mathfrak{P}}}$ defined by the homogenization

$$y^2z + (1-c)xyz - byz^2 - (x^3 - bxz^2) \in \mathcal{O}_{K,\mathfrak{P}}[x,y,z]$$

of the equation of $E(b,c)$. The generic fiber of $\mathcal{X}/\mathcal{O}_{K,\mathfrak{P}}$ is the curve $E(b,c)/K$. The scheme $\mathcal{X}/\mathcal{O}_{K,\mathfrak{P}}$ is either smooth, or $\mathcal{X}$ has a single singular point Q, located on its special fiber. The torsion point $P=(0,0)\in E(b,c)(K)$ reduces to the point $P_0=(0,0)$ on the special fiber, and the key to our argument is that when r is an exceptional unit and s is a unit, b is a unit, and thus $P_0=(0,0)$ is a regular point of the special fiber.

Let $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$ denote either the scheme $\mathcal{X}/\mathcal{O}_{K,\mathfrak{P}}$ if the latter is smooth, or the scheme $\mathcal{X}'/\mathcal{O}_{K,\mathfrak{P}}$ with $\mathcal{X}':=\mathcal{X}\setminus\{Q\}$, if $\mathcal{X}$ has a singular point. Then $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$ is always smooth. It is well-known that when the Weierstrass equation $y^2+(1-c)xy-by=x^3-bx^2$ is minimal (with respect to the discrete valuation ring $\mathcal{O}_{K,\mathfrak{P}}$), then the scheme $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$ is a group scheme, isomorphic to "the connected component of the identity" subgroup scheme $\mathcal{A}^0/\mathcal{O}_{K,\mathfrak{P}}$ of the Néron model $\mathcal{A}/\mathcal{O}_{K,\mathfrak{P}}$ of the elliptic curve $E(b,c)/K$. The group law on $E(b,c)$ can be succinctly summarized by 'three points on a line add to the identity'. This geometric feature allows one to prove that the scheme $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$ is a group scheme even when the defining equation is not minimal.

The following conditions are then satisfied: The point P is of prime order N, and reduces to the point P_0, which is not the identity on the special fiber of the group scheme $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$. Hence, the point P_0 has order N in the special fiber. By virtue of the construction of the group scheme $\mathcal{X}^{sm}/\mathcal{O}_{K,\mathfrak{P}}$, and of the definition of the polynomials $F_m(r,s)$, we find that since P_0 has order N in the special fiber, we must have $F_m(r_0,s_0)\notin\mathfrak{P}$ for all $m=3,\dots,N-1$. Since this statement is true for all maximal ideals $\mathfrak{P}$, the claim is true.

Suppose now that $11\le N\le 101$ and let us complete the proof of the theorem. We know that r_0 is an exceptional unit and s_0 is a unit. We can therefore use the claim, and Part (3) of 4.4 to conclude that $0,1,x_3(r_0,s_0),\dots,x_m(r_0,s_0)$ is an exceptional sequence in $\mathcal{O}_K$ for any $m\le\min(11,(N-1)/2)$. □

Remark 4.6 Given a number field K and a prime $N\ge 11$, Theorem 4.3 suggests an algorithm for finding all N-special elliptic curves E/K. First produce the finite list of all exceptional units in $\mathcal{O}_K^*$ (the current implementation for this in Magma requires that the unit rank be at most 10). Then find all the points (r_0,s_0) on the curve $F_N(r_0,s_0)=0$ where both r_0 and s_0 are exceptional units. Finally, check that the elliptic curve $E(r_0,s_0)/K$ is such that N does not divide $c(E(r_0,s_0)/K)$.

We do not know if this final step is necessary. A priori, even though when both r_0 and s_0 are exceptional units, the torsion point $(0,0)$ in $E(r_0,s_0)(K)$ reduces to a smooth point of the connected component of the identity in the special fiber of the Néron model, it is not immediate that the group of components cannot have order divisible by N. Examples where the group of components has order 2 or 3 when $N=19$ are found in Remark 7.13.

Example 4.7 Let p be prime. The number of exceptional units of $\mathbb{Q}(\zeta_p)^+$ grows rapidly with the degree. For instance, when $p=13,17,19$ and 23, the fields $\mathbb{Q}(\zeta_p)^+$ have respectively 1830, 11700, 28398, and 130812 exceptional units. These values were obtained using the command *ExceptionalUnits*() in Magma [5].

The fields $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_p)^+$ are both totally ramified over (p) and so have a prime of norm p. In particular, both $M(\mathbb{Q}(\zeta_p)^+)$ and $M(\mathbb{Q}(\zeta_p))$ are bounded by p. Lenstra [28] determined that $M(\mathbb{Q}(\zeta_p))=p$. Leutbecher and Nicklash showed that $M(\mathbb{Q}(\zeta_p)^+)\ge p-1$ ([32], Theorem 3), with strict inequality for instance when $p=7,11,13$. Tables of fields along with lower

bounds on their Lenstra constant can be found in Lenstra's original paper [28], and in [29], [30], [31], [32], and [42].

Example 4.8 Theorem 4.3 implies that if $N = 11$ or $N = 13$ and there exists an N-special elliptic curve E/K, then $M(K) \geq 6$. We note here that this bound $M(K) \geq 6$ cannot be improved in general. For instance, the quartic field of discriminant 117 in the table in 1.5 has $M(K) = 6$, and there are two N-special elliptic curves over K with $N = 11$ and one N-special elliptic curve over K with $N = 13$. See also Remark 7.7 for the case $N = 19$.

Example 4.9 We did not consider in this article the case where N is not prime. We only note in this example that when $N = 7^2$, there exist examples of fields K with an elliptic curve E/K having a K-rational point of order N and $c(E/K)$ not divisible by 7, and such that $M(K) \leq 7$.

For instance, when $N = 49$, the first point of $X_1(49)$ listed in [69] is over a totally complex field K of degree 14 with discriminant $3^7 7^{12}$ having one prime $\mathfrak{P}$ over (7) which has ramification index 7 and residual index 1. It follows that $M(K) \leq 7$. This first point corresponds to an elliptic curve with $j = 0$ and complex multiplication which has a K-rational point of order N, and with bad reduction only above $\mathfrak{P}$, of reduction type II.

The fourth example in [69] is over a field of degree 22, having one prime over (7) which has ramification index 6 and residual index 1, so that again $M(K) \leq 7$. There exists over K an elliptic curve with everywhere good reduction (and no CM) and a K-rational point of order N.

4.10 We end this section with some conjectural properties of the polynomial $F_N(r, s)$ when $N \geq 11$ is prime. Recall the degrees d_r and d_s defined in 4.4, as well as the associated integers a and b. When N is prime, we conjecture that

$$\begin{aligned} d_r(N) &= \begin{cases} \frac{N^2-1}{60} & \text{if } N \equiv \pm 1 \pmod{10} \\ \frac{N^2-1}{60} + \frac{1}{5} & \text{if } N \equiv \pm 3 \pmod{10}, \end{cases} \\ d_s(N) &= \tfrac{N^2-1}{24} - d_r(N), \\ a(N) &= \textstyle\sum_{\frac{N}{4} \leq t \leq \frac{N}{3}, t \in \mathbb{N}} (4t - N), \\ b(N) &= \textstyle\sum_{\frac{N}{3} \leq t \leq \frac{2N}{5}, t \in \mathbb{N}} (3t - N). \end{aligned}$$

Moreover, let

$$\begin{aligned} c = c(N) &:= \textstyle\sum_{\frac{N}{5} \leq t \leq \frac{N}{4}, t \in \mathbb{N}} (N - 4t), \\ d = d(N) &:= \textstyle\sum_{\frac{N}{4} \leq t \leq \frac{N}{3}, t \in \mathbb{N}} (N - 3t). \end{aligned}$$

We conjecture that the polynomial $F_N(r, s) \in \mathbb{Z}[r, s]$ satisfies the following properties:

(1) $F_N(r, 1) = (r - 1)^{d_r}$,
(2) $F_N(1, s) = \pm s^c (s - 1)^{d_s - c}$,
(3) $F_N(r, 0) = r^d (r - 1)^{d_r - d}$,

In particular, the points $(0, 0)$ and $(1, 1)$ are on the curve $F_N(r, s) = 0$ if $N \geq 11$, and $(1, 1)$ is singular. When $N \geq 13$, the point $(1, 0)$ is also on the curve, and these three points are

the only points on the affine plane curve $F_N(r,s)=0$ with either $r\in\{0,1\}$ or $s\in\{0,1\}$. All three are singular as soon as $N\geq 23$.

For $N\leq 101$, the conjectures can be proved by inspection of the equations for $F_N(r,s)$ listed in [64]. To check whether a given point is singular on the curve $F_N(r,s)=0$, we simply look at the Taylor expansion of the curve at the point. Recall that we also conjecture that $F(0,s)=\pm s^a$. We find that

(i) $(0,0)$ is singular if $a>1$ and $d>1$.
(ii) $(1,0)$ is singular if $d_r-d>1$ and $c>1$.
(iii) $(1,1)$ is singular if $d_s-c>1$, and $d_r>1$.

It is possible that the above conjectures could be fully proved as follows. The function field of $X_1(N)/\mathbb{C}$, when $N\geq 11$, is isomorphic to $\mathbb{C}(W_3,W_4)$ ([20], Theorem 1), where W_3 and W_4 are explicit Weierstrass units (see [20], (1) on page 305 for the definition. See also [25], Theorem 1, and [26], Chapter 2, Theorem 6.4. A related definition is found in [47], top of page 125).

One might wonder whether

$$F_N(W_3,W_4)=0,$$

in view of the proof of Theorem 3 in [47], bottom of page 130, where a similar statement is asserted but the computations needed to verify it are left to the reader. Assuming that $F_N(W_3,W_4)=0$, the techniques of proof developed in [20] to describe the equation relating the functions W_3 and W_5 ([20], Theorems 2 and 3) could possibly be used to establish the conjectural properties of $F_N(r,s)$ discussed here.

Remark 4.11 In [20] and [27], the fact that the function field of $X_1(N)/\mathbb{C}$ is isomorphic to $\mathbb{C}(W_3,W_5)$ when $N\geq 11$ is used to produce explicit equations for $X_1(N)$. The equation given for $X_1(13)$ in [20], Example, page 316, has a sign error, giving a curve of genus 3. The correct equation can be found in [27], middle of page 56. On page 317, just before section 5, the authors of [20] state that *our equations seem to correspond to the "raw form" of Reichert*. As discussed above, it is more likely that the raw form equation corresponds to the polynomial associated with the pair (W_3,W_4).

Remark 4.12 In [2], one finds for each N a description of three different equations for $X_1(N)$. In Table 1, page 2383, the middle polynomial denoted by $\Phi_N(T,S)$ is related to $F_N(r,s)$ by the formula $F_N(r,s)=\pm\Phi_N(r,-s)$, at least when $N\leq 15$. This fact does not seem to be pointed out in [2].

Remark 4.13 Let N be prime. The formulas for $d_r(N)$ and $d_s(N)$ grow quadratically in N and are upper bounds for the $\mathbb{Q}$-gonality of $X_1(N)$. For comparison, we recall here that the the genus of $X_1(N)$ is given by the formula $g(X_1(N))=\frac{(N-6)^2-1}{24}$ ([18], p. 161).

5. The curve $X_1(11)$

In this section, we finish the proof of Theorem 4.3 (ii) in the case of $N=11$ in Proposition 5.5. We also introduce in 5.1 a natural involution on $X_1(11)/\mathbb{Q}$ which acts on the set of points (r,s) on $F_{11}(r,s)=0$ where r,s are both exceptional units in $\mathcal{O}_K$ (see 5.3). This involution is used to prove Proposition 5.8.

Let $F_N(r,s)$ denote the raw form equation for $X_1(N)$. Consider the change of variables

$$x = x(r,s) := \frac{(s-r)}{(rs-2r+1)} = -\frac{F_7}{F_8},$$

and

$$y = y(r,s) := \frac{(rs-2r+1)}{(s^2-s-r+1)} = -\frac{F_8}{F_9}.$$

This change of variable provides a birational isomorphism from the plane curve $F_N(r,s)=0$ to a plane curve $f_N(x,y)=0$. The equation $f_N(x,y)=0$ is called the *alternative defining equation of* $X_1(N)$ in [64].

Example 5.1 The raw form equation of $X_1(11)$ is given by

$$F_{11}(r,s) = r^2 - rs^3 + 3rs^2 - 4rs + s,$$

while $f_{11}(x,y) := x^2y - xy^2 + y - 1$. We find that

$$f_{11}(x(r,s), y(r,s)) = \frac{(s-1)(r-s)F_{11}(r,s)}{(s^2-s-r+1)^2(rs-2r+1)}.$$

The function $y(r,s)$ is not defined on $F_{11}(r,s)=0$ when $r = s^2-s+1$, which only happens when $s=1$. It turns out that the singular point $(1,1)$ is the only point where the map $(r,s)\mapsto(x,y)$ is undefined on the curve $F_{11}(r,s)=0$.

After homogenizing f_{11} to $x^2y - xy^2 + yu^2 - u^3$, we obtain a minimal Weierstrass equation over $\mathbb{Z}$ for the elliptic curve $X_1(11)/\mathbb{Q}$, given by

$$v^2 - v = u^3 - u^2,$$

by setting $u = 1/y$ and $v = x/y$. Note that an equation for $X_1(11)/\mathbb{Q}$ appears already in the literature as early as 1908 ([33], page 160, Section 5., (7)), given as $y^2x - y^2z - x^2z + yz^2 = 0$.

Since the equation $F_{11}(r,s)$ is quadratic in r, we have an involution σ of the plane curve $F_{11}(r,s)=0$ given by $r \mapsto -r + (s^3 - 3s^2 + 4s)$. For a point $(r,s) \neq (0,0)$ with $F_{11}(r,s)=0$, we have $(s^3-3s^2+4s) = r + s/r$. Hence this involution reduces in this case to $r \mapsto s/r$. The involution fixes both points $(0,0)$ and $(1,1)$.

Lemma 5.2. *Let $r, s \in \mathcal{O}_K^*$ be non-trivial units. Suppose that $0, 1, r, s, (r-1)/(s-1)$ is an exceptional sequence in $\mathcal{O}_K^*$. Then*

(a) *$x(r,s)$ and $y(r,s)$ are exceptional units.*
(b) *If $N \geq 11$ is prime and $F_N(r,s)=0$, then $0, 1, x(r,s), y(r,s)$ is an exceptional sequence.*

Proof. (a) We need to show that $x, y, 1-x$, and $1-y$, are units. We have

$$1 - x = \frac{(r-1)(s-1)}{(rs-2r+1)},$$

and

$$1 - y = \frac{(s-1)(s-r)}{(s^2-s-r+1)}.$$

By hypothesis, we know that $s-1, r-1$, and $s-r$, are all units. Thus to conclude the proof of the lemma, it suffices to show that both $(rs-2r+1)$ and $(s^2-s-r+1)$ are

units. For this, we use the last relations implied by the exceptional sequence, namely that $s-(r-1)/(s-1)$ and $r-(r-1)/(s-1)$ are also units. We find that

$$s-\frac{(r-1)}{(s-1)}=\frac{s^2-s-r+1}{s-1}$$

and

$$r-\frac{(r-1)}{(s-1)}=\frac{rs-2r+1}{s-1},$$

and (a) follows

To prove (b), it suffices to show that $x-y$ is a unit. We find that

$$x-y=\frac{(s-1)(r^2s-3r^2+rs+3r-s^2-1)}{(rs-2r+1)(s^2-s-r+1)}=\frac{F_6F_{12}}{F_8F_9}.$$

In view of the proof of (a), *$x-y$ is a unit if and only if F_{12} is a unit*, where

$$F_{12}=F_{12}(r,s):=r^2s-3r^2+rs+3r-s^2-1.$$

Assume that $F_{11}(r,s)=0$. Recall that $F_{11}(r,s)=r^2-rs^3+3rs^2-4rs+s$, and note that $sF_{12}+F_{11}=(s-r)(rs^2-3rs+r+s^2)$. If the expression $rs^2-3rs+r+s^2$ is not a unit, it must be in a maximal ideal $\mathfrak{P}$. Thus modulo $\mathfrak{P}$, we have $r=-s^2/(s^2-3s+1)$. Substituting this expression for r in F_{11}, we obtain

$$F_{11}(s)=\frac{s(s-1)^6}{(s^2-3s+1)^2},$$

leading to a contradiction since by hypothesis, both s and $s-1$ cannot belong to $\mathfrak{P}$. So F_{12} is a unit.

Assume now that $F_N(r,s)=0$ for some prime $N>12$. By hypothesis, r and s are exceptional units, so we can use the Claim in the proof of Theorem 4.3 to deduce that $F_{12}(r,s)$ is a unit in $\mathcal{O}_K$. □

Lemma 5.3. *Let (r,s) be a point on the plane curve $F_{11}(r,s)=0$ such that r and s are exceptional units in $\mathcal{O}_K^*$. Then $0,1,r,s,(r-1)/(s-1)$ is an exceptional sequence, and*

(a) *The image of (r,s) under the map $(r,s)\mapsto(u,v)$ is a point where $0,1,u,v$ is an exceptional sequence.*

(b) *The image of (r,s) under the involution $(r,s)\mapsto(s/r,s)$ is such that $0,1,s/r,s$ is an exceptional sequence.*

Conversely, if $(u,v)\in K^2$ is a point on the curve $v^2-v=u^3-u^2$ and u is an exceptional unit, then $0,1,u,v$ is an exceptional sequence and the image (r,s) under the inverse map $(u,v)\mapsto(r,s)$ is such that $0,1,r,s$ is an exceptional sequence.

Proof. We can rewrite the equation F_{11} as $F_{11}=(r-s)(r-1)-r(s-1)^3$. Since r, $r-1$, and $s-1$ are units by hypothesis, it follows that $r-s\in\mathcal{O}_K^*$. This shows that $0,1,r,s$ is an exceptional sequence. To prove that $0,1,r,s,(r-1)/(s-1)$ is an exceptional sequence, we use the Claim in the proof of Theorem 4.3, and conclude as in the proof of this theorem.

(a) Consider the maps $(r,s)\to(x,y)\to(u,v)$ introduced in Example 5.1. Any point (r,s) with $F_{11}(r,s)=0$ where both r and s are exceptional units is sent to a point (u,v) with $v^2-v=u^3-u^2$ where both u and v are exceptional units. Indeed, we have x

and y exceptional units by 5.2, and thus $u = 1/y$ is also an exceptional unit. Moreover, $v(v-1) = u^2(u-1)$, so $v(v-1)$ is a unit and, hence, v is an exceptional unit. By definition, $u - v = 1/y - x/y = (1-x)/y$ is a unit.

(b) When r, s, and $r-s$ are units, then s/r is a unit, and so is $1 - s/r = (r-s)/r$. Hence, s/r is an exceptional unit. When r is an exceptional unit, then so is $1 - 1/r$. It follows that the difference $s/r - s$ is a unit, and so $0, 1, s/r, s$ is an exceptional sequence.

Suppose now that (u, v) is a point on $v^2 - v = u^3 - u^2$ and u is an exceptional unit. From $v(v-1) = u^2(u-1)$, we find that v is an exceptional unit. In K, the equation $z^2 - z - (u^3 - u^2) = 0$ has two roots v and $\overline{v}$, and we find that $(u-v)(u-\overline{v}) = u^2 - u - (u^3 - u^2) = -u(u-1)^2$. Since u is an exceptional unit, $u - v$ is a unit. From this we find that $y = 1/u$ is an exceptional unit. Since $x = v/u$, we find that x is a unit, and since $1 - x = (u-v)/u$, $1-x$ is a unit and so x is an exceptional unit. The equation $f_{11}(x, y) := x^2y - xy^2 + y - 1 = 0$ shows that $x - y = (1-y)/(xy)$ is a unit. Consider the change of coordinates

$$r = (x^2y - xy + y - 1)/(x^2y - x) \text{ and } s = (xy - y + 1)/(xy).$$

We leave it to the reader to check that r and s are exceptional units. It follows then from the beginning of the proof that $r - s$ is a unit. □

Lemma 5.4. *Let $r, s \in \mathcal{O}_K^*$ be non-trivial units. Suppose that $0, 1, r, s$ is an exceptional sequence in $\mathcal{O}_K^*$. Let $F_8 := rs - 2r + 1$ and $F_9 := -(s^2 - s - r + 1)$. Then*

(a) *$0, 1, r, s, \frac{r(s-1)}{r-1}$ is an exceptional sequence in $\mathcal{O}_K^*$ if and only if $F_8 \in \mathcal{O}_K^*$.*
(b) *$0, 1, r, s, \frac{r-1}{s-1}$ is an exceptional sequence in $\mathcal{O}_K^*$ if and only if $F_8, F_9 \in \mathcal{O}_K^*$.*

Proof. For (a), the extended sequence is immediately exceptional as soon as $\frac{r(s-1)}{r-1}$ is an exceptional unit, and this latter condition is equivalent to $F_8 \in \mathcal{O}_K^*$. For (b), $\frac{r-1}{s-1}$ is automatically an exceptional unit, and the extended sequence is exceptional if and only if $F_8, F_9 \in \mathcal{O}_K^*$. We leave the details to the reader. □

Proposition 5.5. *Suppose that $r, s \in \mathcal{O}_K^*$ are non-trivial units such that $0, 1, r, s, \frac{r-1}{s-1}$ is an exceptional sequence in $\mathcal{O}_K^*$. If $F_{11}(r, s) = 0$, then*

$$0, 1, r, s, \frac{r-1}{s-1}, \frac{r(s-1)}{r-1}$$

is also an exceptional sequence in $\mathcal{O}_K^*$. In particular, $M(K) \geq 6$.

Proof. In view of Lemma 5.4, we only need to show that the difference $\frac{r-1}{s-1} - \frac{r(s-1)}{r-1}$ is a unit. We have

$$\frac{r-1}{s-1} - \frac{r(s-1)}{r-1} = \frac{r^2 - 3r - rs^2 + 2rs + 1}{(r-1)(s-1)}.$$

Let us set $u := r^2 - 3r - rs^2 + 2rs + 1$, and note that it suffices to show that su is a unit. Recall that $F_{11}(r, s) = r^2 - rs^3 + 3rs^2 - 4rs + s$. Then

$$su - F_{11} = r(s-1)(r-s)$$

and the proposition is proved. □

Let K be a number field and let $(r,s) \in K^2$. Let $c := s(r-1)$ and $b := cr$. Consider the plane curve $E_{(r,s)}$ given by the equation

$$y^2 + (1-c)xy - by = x^3 - bx^2.$$

Let $N = 11$ and set

$$\Delta_N := s^4r^3(r-1)^5(r^2s^3 - 8r^2s^2 + 16r^2s - 2rs^3 + 5rs^2 - 20rs + s^3 + 3s^2 + 3s + 1).$$

Assume that $(r,s) \in K^2$ with $F_N(r,s) = 0$. If $\Delta_N \neq 0$, then $E_{(r,s)}/K$ is an elliptic curve with a K-rational point $(0,0)$ of order N. If $\Delta_N = 0$, we will call (r,s) a K-rational *cusp* of the plane curve $F_N(r,s) = 0$.

Lemma 5.6. *The cusps of the plane curve $F_{11}(r,s) = 0$ consists of $(1,1)$ and five conjugated points whose coordinates are exceptional units in $\mathcal{O}_{\mathbb{Q}(\zeta_{11})^+}$.*

Proof. Magma computes the primary decomposition of the ideal I of $\mathbb{Q}[r,s]$ generated by Δ_N and F_N using the command *PrimaryDecomposition*(). We find that I is contained in exactly two prime ideals, $(r-1, s-1)$, and $(s^5 - 4s^4 - 9s^3 + 27s^2 - 13s - 1, r - (-2s^4 + 2s^3 + 13s^2 - 26s + 3)/11)$. The field $\mathbb{Q}[s]/(s^5 - 4s^4 - 9s^3 + 27s^2 - 13s - 1)$ is isomorphic to $\mathbb{Q}(\zeta_{11})^+$ and the class s_0 of s is an exceptional unit. The element $r_0 = (-2s_0^4 + 2s_0^3 + 13s_0^2 - 26s_0 + 3)/11)$ is also an exceptional unit. □

Let $N \geq 11$ be prime. It is well-known that the complement of $Y_1(N)(\overline{\mathbb{Q}})$ in $X_1(N)(\overline{\mathbb{Q}})$ consists of $(N-1)/2$ rational points, and $(N-1)/2$ conjugated points over $\mathbb{Q}(\zeta_N)^+$ (see, e.g., [72], page 7). We conjecture that the latter points correspond to $(N-1)/2$ points (r_0, s_0) on the plane curve $F_N(r,s) = 0$ where both r_0 and s_0 are exceptional units in $\mathcal{O}_{\mathbb{Q}(\zeta_N)^+}$. Moreover, $0, 1, r_0^{-1}, s_0^{-1}, \frac{s_0-1}{r_0-1}, x_6(r_0,s_0), \ldots, x_{\frac{N-1}{2}}(r_0,s_0)$, is an exceptional sequence in $\mathcal{O}_{\mathbb{Q}(\zeta_N)^+}$, as in Theorem 4.3.

Let S_K denote the set of all points (r,s) such that $F_N(r,s) = 0$ and both r and s are exceptional units in $\mathcal{O}_K^*$. Let $\mathcal{E}_K$ denote the set of all elliptic curves $E_{(r,s)}/K$ corresponding to points in S_K, up to isomorphism. When $N = 11$ and $K = \mathbb{Q}(\zeta_{11})^+$, our next example shows that $|\mathcal{E}_K| = 3$. Proposition 5.8 shows that when $N = 11$, $|\mathcal{E}_K|$ is even in general.

Example 5.7 Let $K = \mathbb{Q}(\zeta_{11})^+$. A computation with Magma finds that $|S_K| = 20$. Five of these twenty elements are cusps. The remaining 15 elements of S_K give rise to only three distinct elliptic curves $E_{(r,s)}/K$, which have integral j-invariants $j = -11^2$, $-11 \cdot 131^3$, and -2^{15}, and have additive reduction at the unique prime above (11). In particular, $|\mathcal{E}_K| = 3$.

Let $A/\mathbb{Q}$ denote the elliptic curve given in Weierstrass form by $v^2 - v = u^3 - u^2$. This curve is commonly denoted by $X_1(11)/\mathbb{Q}$. We described in 5.1 a birational $\mathbb{Q}$-map from the plane curve $F_{11}(r,s) = 0$ to the curve A which produces a bijection between the points where both coordinates are exceptional units (Lemma 5.3). A computer search for points (u,v) in $A(K)$ where $v^2 - v = u^3 - u^2$ and both u and v are exceptional units produces exactly 20 such points, as expected. These points are all of order 25 in $A(K)$. It is a classical result, dating back at least to [4], Lemma 2, that $A(\mathbb{Q})$ is finite of order 5, and is generated by $P := (0:0:1)$, with $2P = (1:1:1)$, $3P := (1:0:1)$, and $4P := (0:1:1)$. We have thus found 25 explicit torsion points in $A(K)$ of order dividing 25. It is known that the algebraic rank of A_K/K is 0, and that the torsion subgroup over K is isomorphic to $\mathbb{Z}/25\mathbb{Z}$ (see [15], Theorem 1). It follows that the torsion points of $A(K)$ are completely determined.

Proposition 5.8. *Let K be a field that does not contain $\mathbb{Q}(\zeta_{11})^+$. Then $|\mathcal{E}_K|$ is even.*

Proof. Recall the involution σ of the plane curve $F_{11}(r,s)=0$ introduced in 5.1. We showed in Lemma 5.3 (b) that σ induces an action on the set S_K. Since we assume that K does not contain $\mathbb{Q}(\zeta_{11})^+$, Lemma 5.6 shows that the set S_K does not contain any cusp. Thus in this case the proposition is proved if we can show that for any $(r,s)\in S_K$, the j-invariant of $E_{(r,s)}$ is not equal to the j-invariant of $E_{(r/s,s)}$, where as we noted in 5.1, $\sigma(r,s)=(r/s,s)$.

Working in the field of fractions of the polynomial ring $\mathbb{Q}[r,s]$, we can write down explicit expressions for $j(E_{(r,s)})$ and $j(E_{(r/s,s)})$. Let w denote the numerator of $j(E_{(r,s)})-j(E_{(r/s,s)})$ divided by its factor r^2-s. Magma can compute the primary decomposition of the ideal $I:=(w,F_{11})$ in the ring $\mathbb{Q}[r,s]$. It turns out that this primary decomposition has seven prime ideals, consisting in (r,s), $(r-1,s-1)$ and M,M_1,M_2,M_3,M_4 that we now describe. In the end, none of these ideals correspond to points in S_K. The ideal M corresponds to a point on $F_{11}(r,s)=0$ defined over an extension of degree 25, and it can be checked that this extension contains $\mathbb{Q}(\zeta_{11})^+$. The other four ideals M_1,M_2,M_3,M_4 have a more intrinsic description.

Indeed, let $A/\mathbb{Q}$ denote the elliptic curve given in Weierstrass form by $v^2-v=u^3-u^2$, as in Example 5.7. The automorphisms of the curve A of genus 1 are well understood, and each corresponds to the composition of an automorphism μ of the elliptic curve A with a translation t_P on A by a point P in $A(\mathbb{Q})$. Since σ is an involution, the automorphism μ has to be the inverse *inv* in the group law on A. Letting $P:=(0:0:1)$, the reader can verify that the involution σ corresponds to the composition $t_P\circ inv$. The smooth point $(0,0)$ on the plane curve $F_{11}(r,s)=0$ is fixed by σ, and is sent to the point $3P$ in $A(\mathbb{Q})$ under the map $(r,s)\mapsto(u,v)$. The set of points corresponding to the ideals M_1,M_2,M_3,M_4, when mapped to the curve A, is of the form $R,R+P,R+2P,R+4P$, where R is a point of order 2 in $A(\overline{\mathbb{Q}})$. It can be checked that none of these points corresponds to points in S_K. Note that $\{R,R+P\}$ and $\{R+2P,R+4P\}$ are two orbits under the involution $t_P\circ inv$. □

Remark 5.9 We record below another explicit involution of the plane curve $F_{11}(r,s)=0$:

$$\tau:(r,s)\longmapsto(1-r,(s^2-s+1-r)/(s-1)^2).$$

The composition $\sigma\circ\tau$ is a birational automorphism of the plane curve $F_{11}(r,s)=0$ of order 5, corresponding to an automorphism of $X_1(11)$ of the form $Q\mapsto Q+S$, with S a rational point of order 5.

6. The Lenstra constant

Let $N\geq 11$ be prime. We use in this section results or conjectures on the Lenstra constant of fields of small degrees, along with Theorem 4.3, to obtain applications to N-special elliptic curves.

Theorem 6.1. *Let $N\geq 11$ be prime. Let K be a cubic number field, and let E/K be an N-special elliptic curve. Then $N=13$, the field K is $\mathbb{Q}(\zeta_7)^+$, and there exits a unique such curve E/K.*

The curve E/K has j-invariant $-28672/3$ and Cremona label 147b1. It has prime conductor (3), and its reduction at (3) is split multiplicative of type I_1.

Proof. Assume that E/K is N-special. Then Proposition 3.1 implies that $N \leq 13$. That no N-special elliptic curve exists when $N = 11$ was proved by Krumm in [23], 5.4.2. When $N = 13$, the unique curve in the statement of Theorem 6.1 was found by Krumm in [23], 5.4.4. We now show the uniqueness of this 13-special elliptic curve, and also give a new proof for the case $N = 11$.

Leutbecher and Martinet show in [30, Theorem 4.1.1] that for a cubic field K, either $M(K) \leq 3$, or $K = \mathbb{Q}(\zeta_7)^+$ and $M(K) = 7$, or $M(K) = 5$ and $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha - 1 = 0$. The end of the proof is then machine-assisted: for both fields $\mathbb{Q}(\zeta_7)^+$ and $\mathbb{Q}(\alpha)$, make a list of all the exceptional units in the field, and check whether the raw form equations $F_{11}(r, s) = 0$ and $F_{13}(r, s) = 0$ have any solutions with both r, s exceptional units. Such computation can be done with Magma [5] and produces only six solutions, all of $F_{13}(r, s) = 0$ over the field $K = \mathbb{Q}(\zeta_7)^+$. This leads to a single N-special elliptic curve E/K with $N = 13$, since the six solutions corresponds to the orbit of (E, P) under the Galois group of $X_1(13)/X_0(13)$. □

Corollary 6.2. *Let $N \geq 11$ be prime. Let K be a cubic number field, and let E/K be an elliptic curve with a K-rational torsion point of order N and everywhere semi-stable reduction. Then E/K has a place of split multiplicative reduction.*

Proof. The corollary follows immediately from Theorem 6.1, since Lemma 1.2 shows that the statement is true once it is proved for N-special curves. □

The corollary partially generalizes Theorem 1.1 to cubic fields. The statement cannot be modified to include the case $N = 7$. Indeed, over the smallest cubic field $K = \mathbb{Q}(\alpha)$, with α a root of $x^3 - x^2 + 1$, of discriminant -23, the elliptic curve E/K labeled 167.1-$A1$ in [35] has prime conductor over $p = 167$ and does not have a place of split multiplicative reduction.

Remark 6.3 It follows from Theorem 3.3 that if E/K is an elliptic curve over a cubic field with integral j-invariant, then it cannot have a K-rational torsion point of prime order $N \geq 11$. This statement was proved already in [58] (see [73], Theorem 6). When $N = 5$, it is shown in [73], Corollary, page 212, that there are infinitely many cubic fields K with infinitely many elliptic curves E/K having integral j-invariant and such that E/K has a K-rational torsion point of order $N = 5$.

We now turn to the case of quartic fields, and prove Theorem 1.4. The exceptional units in fields of unit rank 1 were completely determined by Nagell ([50], [51], [52], [53], [54]). In the case of quartic fields of unit rank 1 the Lenstra constant was determined by Lenstra in [28], 3.11. In particular, he shows that for such quartic field, $M(K) \leq 4$ *except when* $K = \mathbb{Q}(\zeta_5)$ *with* $M(K) = 5$*, and when K is the quadratic extension of* $\mathbb{Q}(\zeta_3)$ *of discriminant* 117 *with* $M(K) = 6$. (We have used here that the tables [21] are complete and that there is a unique quartic field of rank 1 and discriminant 117. It appears in the table in Conjecture 6.4).

Leutbecher and Martinet make a conjecture on the Lenstra constant of number fields of unit rank at most 2 in [30], 6.1.7. Since the Leutbecher–Martinet conjecture does not cover the case of unit rank 3 when $[K : \mathbb{Q}] = 4$, we complement it below in 6.4 (b) so that all cases are covered for quartic fields. The form of this conjecture was anticipated by Martinet (see [42], Remarque on page 17-12).

Conjecture 6.4. *Let $K/\mathbb{Q}$ be a number field of degree 4. Then $M(K) \leq 4$ except for finitely many explicit exceptions. More precisely:*

(a) *Assume that the unit rank of K is 2. If K contains $\mathbb{Q}(\zeta_5)^+$, then $M(K) = 4$. Except for the fields of discriminants $-275, -283, -331$, and -475 in the table below, all the other fields have $M(K) \leq 4$.*

(b) *Assume that the unit rank of K is 3. Then $M(K) \geq 10$ if K is the field of discriminant 725 in the table below, $M(K) = 5$ if $K = \mathbb{Q}(\zeta_{15})^+$, and for all other fields, $M(K) \leq 4$.*

N	field K (degree 4)	rk	#exu	$M(K)$	disc(K)
$11(2), 13(j=0)$	$x^4 - x^3 - x^2 + x + 1$	1	20	6	117
None	$x^4 - x^3 + x^2 - x + 1$, $\mathbb{Q}(\zeta_5)$	1	18	5	125
$11(4)^*$	$x^4 - x^3 + 2x - 1$	2	54	9	-275
$11(2)$	$x^4 - x - 1$	2	54	7	-283
None	$x^4 - x^3 + x^2 + x - 1$	2	42	5	-331
None	$x^4 - 2x^3 + 2x^2 - x - 1$	2	30	5	-475
$11(2), 13, \mathbf{17}$	$x^4 - x^3 - 3x^2 + x + 1$	3	162	10 or 11	725
None	$x^4 - x^3 - 4x^2 + 4x + 1$, $\mathbb{Q}(\zeta_{15})^+$	3	90	5	1125

The notation in the above table is described in 1.5. The reader will note that all fields appearing in Theorem 1.4 also appear in the above table.

6.5 *Proof of Theorem 1.4.* Let $N \geq 11$ be prime. Let $K/\mathbb{Q}$ be a quartic field, and let E/K be an N-special elliptic curve. Then Proposition 3.1 shows that $N \leq 17$. Theorem 4.3 implies that $M(K) \geq 6$.

Conjecture 6.4 implies that there is only one quartic field of unit rank 3 with $M(K) \geq 6$. Thus the proof of Theorem 1.4 (b) reduces to finitely many computations: it suffices to make a list of all the exceptional units in the field, and check whether the raw form equations $F_N(r, s) = 0$ for $N = 11, 13$, and 17, have any solutions with both r, s exceptional units. Such computation can be done with Magma [5] and produces the solutions in Theorem 1.4 (b) (and recalled in the above table).

To prove Theorem 1.4 (a), where the unit rank is at most 2, we note that the quartic fields of rank at most 2 which have $M(K) > 5$ have been completely described by Nagell and Lenstra (in rank 1, see [28], 3.11) and by Leutbecher and Martinet (in rank 2, see [30], 5.1.1). The above discussion then can be applied and the proof of Theorem 1.4 (a) also reduces to finitely many computations.

Let us now turn to the case of quintic fields.

Theorem 6.6. *Let $K/\mathbb{Q}$ be a quintic field of unit rank 2. Let $N \geq 11$ be prime. Let E/K be an N-special elliptic curve. Then K is one of only three fields $K/\mathbb{Q}$, listed below (notation as in 1.5). The possible N's are listed in the first column next to the defining polynomial of the field.*

N	field K (degree 5)	rk	#exu	$M(K)$	discr(K)
$13, \mathbf{17}$	$x^5 - x^3 - x^2 + x + 1$	2	78	≥ 9	1609
$11(2), 13$	$x^5 - x^4 + x^2 - x + 1$	2	78	≥ 8	1649
$11(2)$	$x^5 - x^4 + x^3 - 2x^2 + x - 1$	2	72	7	1777

The information on $M(K)$ in the table is found in [30], 5.3.

Conjecture 6.7. *Let $K/\mathbb{Q}$ be a quintic field of unit rank greater than 2. Let $N \geq 11$ be prime. Let E/K be an N-special elliptic curve. Then K is one of only six fields $K/\mathbb{Q}$, listed below (notation as in 1.5). The possible N's are listed in the first column next to the defining polynomial of the field.*

N	field K (degree 5)	rk	#exu	$M(K)$	discr(K)
$13(2)^*, \mathbf{19}$	$x^5 - x^3 - 2x^2 + 1$	3	228	≥ 11	-4511
$11(2)$	$x^5 - x^4 - x^3 + 2x^2 - x - 1$	3	198	9	-4903
$11(2), 13$	$x^5 - x^4 - x^3 + 3x^2 - 1$	3	180	7	-5519
$11(2)$	$x^5 - 2x^4 + x^3 + 2x^2 - 2x - 1$	3	168	7	-5783
$11(2)$	$x^5 - 2x^4 + 3x^2 - 2x - 1$	3	132	7	-7367
None	$x^5 - x^4 - x^2 - x + 1$	3	108	6	-8519
$11(3)^*$	$\mathbb{Q}(\zeta_{11})^+$	4	570	11	11^4
None	$x^5 - 5x^3 + 4x - 1$	4	240	7	38569

6.8 As in the case of quartic fields, we state below a conjecture on the Lenstra constant of quintic fields which will imply Conjecture 6.7. Lenstra showed that one should expect infinitely many quintic fields with $M(K) \geq 5$ and, more generally, for any fixed degree $d \geq 5$, infinitely many fields K of degree d with $M(K) \geq 5$. Indeed, it is shown in [28], 2.4, (c), that if $K = \mathbb{Q}(\alpha)$ is such that the minimal polynomial $f(x)$ of α over $\mathbb{Q}$ has the form

$$f(x) = g(x)(x^2 - x + 1)(x - 1)x \pm 1$$

for some monic $g(x) \in \mathbb{Z}[x]$, then $M(K) \geq 5$. As soon as $\deg(g) \geq 1$, we should expect to find infinitely many pairwise not isomorphic such fields.

We propose the following conjecture for quintic fields, extending a theorem of Leutbecher and Martinet for the fields of unit rank 2 ([30], 5.2.1).

Conjecture 6.9. *Let $K/\mathbb{Q}$ be a quintic field. Then $M(K) \leq 5$ unless K is one of the fields listed in the tables in Theorem 6.6 and Conjecture 6.7.*

6.10 *Proof of Theorem 6.6.* We note here that Conjecture 6.9 implies Conjecture 6.7, and we prove Theorem 6.6. Indeed, let $N \geq 11$ be prime, and assume that E/K is N-special. Then Proposition 3.1 shows that $N \leq 19$ or $N = 31$ or 41. Theorem 4.3 implies that $M(K) \geq 6$. Conjecture 6.9 reduces the verification of Theorem 6.6 to finitely many computations, since

there are only finitely many explicit quintic fields with $M(K) \geq 6$. For each such field, it suffices to make a list of all the exceptional units in the field, and check whether the raw form equations $F_N(r,s) = 0$ for $N = 11, 13, 17, 19, 31, 41$, have any solutions with both r, s exceptional units. Such computation can be done with Magma [5] and produces the solutions listed in Conjecture 6.7.

To prove Theorem 6.6, where the unit rank is 2, we note that the quintic fields of rank 2 which have $M(K) > 5$ have been completely described by Leutbecher and Martinet ([30], 5.2.1). The above discussion then can be applied.

Remark 6.11 When $[K : \mathbb{Q}] = 4$ and $N = 17$, and when $[K : \mathbb{Q}] = 5$ and $N = 19$, Theorem 1.4 (b) and Conjecture 6.7 imply that there exists only a single N-special elliptic curve E/K. These curves were found by Krumm already in [23], 5.5.2 and 5.6.2, by a different method using an algorithm developed in [13]. We used the more targeted search suggested by Theorem 4.3 in 4.6 and found examples of N-special curves with the following pairs $(N, [K : \mathbb{Q}])$:

N	$[K:\mathbb{Q}]$	N	$[K:\mathbb{Q}]$	N	$[K:\mathbb{Q}]$
19	6,7,8,9,10,11,12	29	9,10,11	37	6,10,12
23	7,8,9,10,11,12	31	9,10	43	12

Explicit examples with $N = 31$ are also known with $[K : \mathbb{Q}] = 11$ and unit rank 6 or 7: they were found in [68] using a different method. The list of examples up to degree 13 where the elliptic curves have in addition complex multiplication was found earlier in [7]. In particular, when $(N-1)/3$ is an integer, then there exists an N-special curve with $j = 0$ over a field of degree $(N-1)/3$ ([6], Theorem 1 a)).

Let $d_{min}(N)$ denote the smallest integer d such that the modular curve $X_1(N)/\mathbb{Q}$ has *infinitely many* closed points of degree d. The following are known values of $d_{min}(N)$ (see [10], Table 1, and Theorem 3), along with bounds coming from $d_{min}(N) \leq \mathrm{gon}_{\mathbb{Q}}(X_1(N))$.

N	11	13	17	19	23	29	31	37
$d_{min}(N)$	2	2	4	5	7	≤ 11	≤ 12	≤ 18

Remark 6.12 Let $K/\mathbb{Q}$ be a number field of degree $d > 1$. We return here to a question raised in the introduction: is it possible to find a non-trivial $g(d)$ such that if E/K is a semi-stable elliptic curve with a K-rational torsion point of order $N \geq g(d)$, then there exists a place of K where E/K has *split* multiplicative reduction? Lemma 1.2 shows that if such an elliptic curve E/K is not N-special, then it always has a place of split multiplicative reduction. On the other hand, an N-special elliptic curve need not always have a place of split multiplicative reduction.

Let $f(d)$ denote the largest prime N such that there exist a field $K/\mathbb{Q}$ of degree d and an elliptic curve E/K with everywhere good reduction and a K-rational point of order N. It is clear that such an elliptic curve has no places of multiplicative reduction. Let $h(d)$ denote the largest prime N such that there exist a field $K/\mathbb{Q}$ of degree d and an elliptic curve E/K with a K-rational point of order N. That $h(d)$ is well-defined follows from a famous theorem of L. Merel [46]. In fact, $h(d) < d^{3d^2}$ [46], refined to $h(d) < (3^{d/2}+1)^2$ by J. Oesterlé [59],

Remark 1. For our question to have a non-trivial positive answer, we need to impose that $f(d) < g(d) \leq h(d)$. We do not know whether $f(d) < h(d)$ in general.

Let $d = 4$, where it is expected that $h(4) = 17$. The 17-special elliptic curve over the quartic field of discriminant 725 in Theorem 1.4 has prime conductor (2) and does not have a place of split multiplicative reduction. Thus conjecturally, our question cannot have a non-trivial positive answer for any value $g(4)$.

Let $d = 5$, where it is expected that $h(5) = 19$. The 19-special elliptic curve over the quintic field of discriminant -4511 in Conjecture 6.7 has prime conductor (above $p = 37$) and does not have split multiplicative reduction at this place.

7. Sextic and septic fields

For sextic number fields, we propose the following conjecture.

Conjecture 7.1. *Let $N \geq 17$ be prime. Then there exist only finitely many sextic fields $K/\mathbb{Q}$ with an N-special elliptic curve E/K.*

7.2 In the following table, we include all sextic fields K found to have at least one N-special elliptic curve E/K with $N \geq 17$. We keep the notation introduced in 1.5. In addition, the notation $19(2)^{**}$ indicates that both curves found have everywhere good reduction (the two curves in the table over $\mathbb{Q}(\zeta_{13})^+$ are discussed for instance in [9], Example 6.8, page 168. They are linked by an isogeny of degree 3 [35]). As before, the notation $19(2)^*$ indicates that at least one of the curves has integral j-invariant. In the instance below, only one curve has integral j-invariant, with $j = 0$.

N	field K (degree 6)	rk	#exu	$M(K)$	discr(K)
$13(4), \mathbf{19}(2)^*$	$x^6 - x^5 + x^4 - 2x^3 + 4x^2 - 3x + 1$	2	110	9	-9747
$11(2), \mathbf{17}^*, \mathbf{19}$	$x^6 - 2x^5 + x^4 + x^3 - 2x^2 + x + 1$	3	282	≥ 10	29189
$11(2), 13, \mathbf{17}$	$x^6 - x^5 + 2x^3 - 2x^2 + 1$	3	252	≥ 10	31709
$11(6), 13(2), \mathbf{37}^{**}$	$\mathbb{Q}(\sqrt{5})\mathbb{Q}(\zeta_7)^+$	5	2700	≥ 18	300125
$11(6)^{\mathrm{b}}, \mathbf{19}(2)^{**}$	$\mathbb{Q}(\zeta_{13})^+$	5	1830	13	$13^5 = 371293$

Remark 7.3 The field $K = \mathbb{Q}(\sqrt{5})\mathbb{Q}(\zeta_7)^+$ supports an N-special elliptic curve E/K with $N = 37$. The technique of proof of Theorem 4.3 shows that K contains an exceptional sequence of length $(N-1)/2$, so that $M(K) \geq 18$. This fact was noted by Mestre already in [47], page 127. It is suggested in [36], page 577, that $M(K)$ might in fact equal 18. We do not know if there exists a sextic field F with $M(F) > 18$.

Remark 7.4 Recall that over $K_0 = \mathbb{Q}(\zeta_7)^+$ there exists an N-special elliptic curve E/K_0 with $N = 13$. Thus over any quadratic extension K of K_0, the base change E_K/K has the same property. It is natural to wonder whether the statement of Conjecture 7.1 still holds when $N = 11$, and still holds when $N = 13$ when one considers only the sextic fields that do not contain $\mathbb{Q}(\zeta_7)^+$.

[b] The analytic rank of $X_1(11)$ over $\mathbb{Q}(\zeta_{13})^+$ is 3, with torsion subgroup reduced to $\mathbb{Z}/5\mathbb{Z}$. Over $\mathbb{Q}(\sqrt{5})\mathbb{Q}(\zeta_7)^+$, the analytic rank is 2.

The data that we computed does not support conjecturing an answer to these questions when the unit rank is 4 or 5. In fact, when $N = 11$, Nicholas Triantafillou informed us [67] that he can parameterize the sextic fields K and the points $(r_0, s_0) \in K^2$ on the Weierstrass equation $y^2 - y = x^3 - x^2$ of $X_1(11)$ where both r_0 and s_0 are exceptional units in $\mathcal{O}_K^*$. He found 80 families of polynomials $f(x, k) \in \mathbb{Z}[x, k]$ such that when k is an integer, a root r_0 of $f(x, k)$ is an exceptional unit in the number field $L_k = \mathbb{Q}(r_0)$, and there exists an explicit exceptional unit s_0 such that (r_0, s_0) is a point on $y^2-y = x^3-x^2$. The first such polynomial on his list is

$$f(x, k) = x^6 + (2k - 18)x^5 + (k^2 - 4k + 33)x^4 + (-2k^2 + 2k - 20)x^3 + k^2x^2 + 4x - 1$$

with the corresponding coordinate

$$y := \frac{-x^3 + (-k + 1)x^2 + (k + 2)x - 1}{4x - 2}.$$

The number fields L_k defined by a root of $f(x, k)$ are likely to have unit rank 4 or 5. In view of these examples and Lemma 5.3, the extended statement of Conjecture 7.1 that includes $N = 11$ is unlikely to hold.

Remark 7.5 Consider the natural morphism $X_1(13) \to X_0(13)$ of degree 6. Since the curve $X_0(13)$ is rational, Hilbert's Irreducibility Theorem shows that the curve $X_1(13)$ has infinitely many points P defined over a cyclic Galois extension $K(P)$ of degree 6. It would be interesting to determine whether infinitely many such points P correspond to N-special elliptic curves $E/K(P)$ with $N = 13$.

We present below two totally real (non-Galois) sextic fields $K/\mathbb{Q}$ where we found an N-special elliptic curve E/K with $N = 13$, and where the discriminant of K is several orders of magnitude larger than the largest ones currently found in the available tables of sextic fields. We do not know if the construction described below could be used to generate infinitely many such examples.

Start with a curve $A/\mathbb{Q}$ with an isogeny of degree 13 defined over $\mathbb{Q}$. For instance, consider the curve $9025.a1$ in [35], with the j-invariant $j = 2045023375454208$. This curve has a point of order 13 over a degree 12 extension. This degree 12 extension contains a totally real sextic subextension K given by adjoining a root of the polynomial

$$f(x) := x^6 - 435x^5 + 61557x^4 - 3899227x^3 + 116234341x^2 - 1451842437x + 4630649791.$$

The field K has discriminant $6048409381625 = 5^3 13^5 19^4$ and 126 exceptional units, with class number 6. It has $M(K) = 6$. The search for a solution to $F_{13}(r, s) = 0$ with r, s exceptional units in $\mathcal{O}_K^*$ is successful, and there exists an N-special elliptic curve E/K with $N = 13$, and same j-invariant. A similar example can be obtained starting with $j = -738044630625096380416/3$ and the elliptic curve $31827b1$, giving a point over the field of discriminant $41789354259133 = 13^5 103^4$.

It is possible that Conjecture 7.1 might be proved by first giving a positive answer to the following question on the Lenstra constant of sextic fields.

Question 7.6 Let $K/\mathbb{Q}$ be a sextic field. Is it true that $M(K) \leq 7$ except for finitely many explicit exceptions?

Remark 7.7 Leutbecher and Martinet prove in [30], 6.1.1, that a sextic field with unit rank 2 has $M(K) \leq 9$ except for two explicit fields. In particular, the field K of discriminant -9747 in 7.2 is not one these two fields, showing that Theorem 4.3 is sharp when $N = 19$: the field K must have $M(K) = 9$.

As we mentioned in 6.8, there are infinitely many sextic fields $K/\mathbb{Q}$ with $M(K) \geq 5$. It is straightforward to prove that there are in fact infinitely many sextic fields with $M(K) \geq 7$. Indeed, the cubic field $K_0 := \mathbb{Q}(\zeta_7)^+$ has $M(K_0) = 7$, and thus any quadratic extension K of K_0 has $M(K) \geq M(K_0)$. There is in addition at least one other infinite family of sextic fields with $M(K) \geq 7$ discovered by Leutbecher ([42], top of page 17-15, or [30], 3.2, A).

Having noted in the data a number of sextic fields with large discriminants and 126 exceptional units, we wonder whether there exist infinitely many such fields. Initial computations with the Leutbecher family indicate that there may be infinitely many sextic fields with at least 96 exceptional units.

For septic number fields, we propose the following conjecture.

Conjecture 7.8. *Let $N \geq 17$ be prime. There there exist only finitely many septic fields $K/\mathbb{Q}$ with an N-special elliptic curve E/K.*

7.9 In the following table, we include all septic fields K found where there exists at least one N-special elliptic curve E/K with $N \geq 17$. The notation is as in 1.5 and 7.2.

N	field K (degree 7)	rk	#exu	discr(K)
$11(2), 13, \mathbf{19}$	$x^7 - x^6 + x^3 - x + 1$	3	336	-199559
$11(2), 13, \mathbf{17}$	$x^7 - 2x^6 + 4x^5 - 4x^4 + 3x^3 - x^2 - x + 1$	3	270	-250367
$11(6), \mathbf{23}$	$x^7 - 3x^5 - x^4 + 3x^3 + 1$	4	960	612569
$11(6), \mathbf{23}$	$x^7 - x^6 - x^4 + 3x^2 - 1$	4	906	649177
$11(2), \mathbf{17}$	$x^7 - x^6 - x^5 + 2x^3 + x^2 - 2x - 1$	4	882	661033
$11(2), \mathbf{23}$	$x^7 - 3x^6 + 5x^5 - 6x^4 + 3x^3 - x^2 - x + 1$	4	864	674057
$13(3), \mathbf{19}$	$x^7 - x^6 - x^5 + 3x^4 - 2x^3 + 2x - 1$	4	768	788857
$11(6), \mathbf{17}$	$x^7 - x^6 - 4x^3 + 2x^2 + 2x - 1$	5	1908	-2932823
$\mathbf{17}^{**}$	$x^7 - x^6 - 2x^5 + 5x^4 - 6x^2 + x + 1$	5	1464	-3998639

It is possible that Conjecture 7.8 might be proved by first answering positively the following question on the Lenstra constant of septic fields.

Question 7.10 Let $K/\mathbb{Q}$ be a septic field. Is it true that $M(K) \leq 7$ except for finitely many exceptions?

Remark 7.11 A septic field with $M(K) \geq 15$ is given in [29], page 103, Table 3. This field might be the only known septic field with $M(K) \geq 15$. The field K in the table in 7.9 of discriminant -2932823 is mentioned in [29], page 105, as having $M(K) \geq 13$.

The reader will find in [41] the results of our search for N-special elliptic curves E/K when $K/\mathbb{Q}$ has degree 8 through 12. We note below the following two examples in degree 12.

Remark 7.12 Consider the field K of degree 12 with discriminant $42553255797 = 3^6 13^3 163^2$, defined by the polynomial $x^{12} - x^9 + 5x^8 - 2x^7 - x^6 - 7x^5 + 8x^4 - 4x^3 + 5x^2 - 4x + 1$, with 5204 exceptional units. This field contains the subfields $\mathbb{Q}(\zeta_3)$ and the quartic field of discriminant 117 appearing in 1.5. There exists an explicit N-special elliptic curve E/K with $N = 43$, and we find using the technique of proof in Theorem 4.3 that there is in K an exceptional sequence of units of length $(N-1)/2$. In particular, $M(K) \geq 21$. The ideal of $\mathcal{O}_K$ of smallest norm has norm 37, so that $M(K) \leq 37$. To our knowledge, this field K is the field of degree 12 with the largest known lower bound for its Lenstra constant. Some fields F of degree 12 with $M(F) \geq 18$ are given in [19], Table 6.

Remark 7.13 Let K denote the totally complex field K of degree 12 defined by the polynomial $x^{12} - 2x^{11} + 5x^{10} - 10x^9 + 16x^8 - 22x^7 + 30x^6 - 31x^5 + 28x^4 - 27x^3 + 19x^2 - 7x + 1$. This field has discriminant $48737056617 = 3^9 19^5$, and 4622 exceptional units. It contains the sextic field having discriminant $-9747 = -3^3 19^2$ in 7.2. In $\mathcal{O}_K$, the ideal (19) has a factorization in maximal ideals of the form $(19) = M^6 M_1 M_2 M_3$.

There are four N-special elliptic curves E/K with $N = 19$. Three have integral j-invariant. One of them has $j = 0$ and a K-rational point of order 57, and reduction modulo M of type IV. This curve is found in [7], page 531. The other two curves do not have complex multiplication and have a point of order 38, with reduction modulo M of type III. It is shown in [45], Theorem 1.2, that the possible additive reduction types of a curve E/K with a K-rational point of order N modulo a prime above N are quite restricted, and only reduction of type II is allowed in addition to the two examples above with reduction III and IV.

8. Higher dimension

It would be interesting to determine whether some of the results of this article have generalizations to abelian varieties A/K of dimension $g > 1$. It is straighforward to generalize our definitions to higher dimensional abelian varieties: Given a place v of a number field $K/\mathbb{Q}$, we let again K_v denote the completion of K at v, and k_v denote the residue field of $\mathcal{O}_{K_v}$. Given an abelian variety A/K, the *local Tamagawa number* c_v of A/K is the order $|\Phi_v(k_v)|$ of the group of k_v-rational points of the component group Φ_v/k_v of the special fiber $\mathcal{A}_{k_v}/k_v$ of the Néron model $\mathcal{A}/\mathcal{O}_K$ of A_{K_v}/K_v. The *Tamagawa number* $c(A/K)$ is the product $\prod_v c_v$. Let N be prime. We say that A/K is *N-special* if A/K has a K-rational point of order N and N does not divide $c(A/K)$.

Let E/K be an elliptic curve. When $N \geq 5$ and N divides $c(E/K)$, Lemma 1.2 shows that E/K has a place of split multiplicative reduction. This fact is expected to generalize as follows.

Lemma 8.1. *Let A/K be an Jacobian variety of dimension g, and let N be prime. When $N > 2g+1$ and v is a place of K where N divides c_v, then the reduction of A at v has positive toric rank. The same result holds when A/K is a principally polarized abelian variety and $N \neq \mathrm{char}(k_v)$.*

Proof. When the abelian variety A/K is principally polarized, its group of components $\Phi_v(\overline{k_v})$ is expected to contain a subgroup Θ whose order is bounded be a constant depending only on the unipotent rank of the special fiber $\mathcal{A}_{k_v}$, and such that $\Phi_v(\overline{k_v})/\Theta$ has a number

of generators bounded by the toric rank of $\mathcal{A}_{k_v}$. This statement is true for the prime-to-p part of $\Phi_v(\overline{k_v})$, where $p = \text{char}(k_v)$. In this case it is further known that the primes ℓ which divide $|\Theta|$ satisfy $\ell \leq 2g+1$ (use [39], Theorem 3.21, with Θ isomorphic to the product over all primes ℓ of the groups denoted by $\Theta_{K,\ell}(A)$ in Part (ii)). Hence, when $N > 2g+1$ and N divides c_v and $N \neq p$, we find that $\Phi_v(\overline{k_v})/\Theta$ cannot be trivial, and so the toric rank of $\mathcal{A}_{k_v}$ cannot be 0.

When A/K is a Jacobian with toric tank 0 at v, we can use the bound for $|\Phi_v(\overline{k_v})|$ given in [37], Theorem 2.4, to show that only primes ℓ with $\ell \leq 2g+1$ can divide $|\Phi_v(\overline{k_v})|$. □

Let $A/\mathbb{Q}$ be an abelian surface. The full list of primes N that can divide the order of the torsion subgroup of $A(\mathbb{Q})$ is not yet known. In particular, $N = 31$ or 37 are not known to divide $|A(\mathbb{Q})_{tors}|$ for some $A/\mathbb{Q}$. Examples of N-special abelian surfaces $A/\mathbb{Q}$ with $N = 11, 13$, and 19 are given in [40], 3.14 to 3.17. When the base field is not $\mathbb{Q}$, we do not know of any explicit example beyond the following examples of an abelian surface with large prime torsion (not defined already over $\mathbb{Q}$).

Example 8.2 Let $K := \mathbb{Q}(\zeta_7)^+$, the totally real cubic field of smallest discriminant. This field has $M(K) = 7$. We present below a hyperelliptic curve $X/\mathbb{Q}$ of genus 2 whose Jacobian $A/\mathbb{Q}$ is such that A_K/K is N-special with $N = 31$. We also present an N-special abelian surface A'/K with $N = 37$.

Consider the curve $X/\mathbb{Q}$ given by the affine equation $y^2 = 5x^6 - 4x^5 + 20x^4 - 2x^3 + 24x^2 + 20x + 5$. This curve was found by Noam Elkies [14]. He mentions that X has three K-rational points $P_m = (z_m, 7z_m^2)$, where $z_m = \zeta_7^m + \zeta_7^{-m} \in K$, $m = 1, 2, 3$. He states that the Jacobian $A/\mathbb{Q}$ of $X/\mathbb{Q}$ has a $\mathbb{Q}$-rational subgroup of order 31. Magma can work with this Jacobian using the command *Jacobian*() and can check that the point Q of $A(K)$ determined by the divisor $P_1 - P_2$ has exact order $N = 31$. Magma further checks that the point Q' of $A(K)$ determined by the divisor $P_3 - P_2$ has exact order $N = 31$, with $Q' = 26Q$.

Elkies mentions that the curve has good reduction at $p = 2$. Sage computes the reduction of $X/\mathbb{Q}$ at each odd prime p using the command *genus2reduction*(), and finds that the conductor of this curve over $\mathbb{Q}$ is $5^2 7^4 = (245)^2$. It is easy to see directly that the reduction modulo 5 has equation $y^2 = x^2(x+1)(x+2)^2$ and so is stable with two $\mathbb{F}_5$-rational ordinary nodes at $(0, 0)$ and at $(-2, 0)$. The given equation in fact can be used to construct the regular model of $X_{\mathbb{Q}_5}/\mathbb{Q}_5$. The reduction of the equation modulo 7 is $y^2 = (x+5)^6$ and so defines the union of two rational curves meeting at one point. Sage indicates that the reduction of $X/\mathbb{Q}$ modulo 7 is of type [III] page 155, in [55].

We now turn to showing that $N = 31$ does not divide $c(A_K/K)$. For this, we use the information above on the reduction of $X/\mathbb{Q}$ and infer from it information on the reduction of X_K/K. The prime (5) of $\mathbb{Z}$ is inert in $\mathcal{O}_K$. Therefore, the reduction modulo (5) does not change when passing from $\mathbb{Q}$ to K. The component group of the Néron model over $(\mathcal{O}_K)_{(5)}$ is trivial.

Recall that the extension $K/\mathbb{Q}$ is ramified only above (7) with $(7) = (\alpha)^3$ and $\alpha = 2 - \zeta_7 - \zeta_7^{-1}$. We claim that the curve X_K/K has good reduction modulo (α), so that the component group above (α) of the Néron model of A_K/K is again trivial. To verify this claim, it suffices to use that the extension of degree 3 that we are making from $\mathbb{Z}_{(7)}$ to $(\mathcal{O}_K)_{(\alpha)}$ is tame. This allows for an explicit calculation of the reduction type of the special fiber of

the regular model over $(\mathcal{O}_K)_{(\alpha)}$ from the knowledge of the special fiber of the regular model over $\mathbb{Z}_{(7)}$ (see, e.g., [38], 1.8, for more details on this). The new special fiber over $(\mathcal{O}_K)_{(\alpha)}$ is a curve of genus 2 with an automorphism of order 3 inducing a morphism of degree 3 to a projective line ramified over 4 points.

Let $L := \mathbb{Q}(\sqrt{5})K$, and consider the N-special elliptic curve E/L in 7.2 with $N = 37$. Let A'/K denote the Weil restriction of E/L to K. Lemma 8.3 shows that A'/K is an N-special abelian surface.

We can use the following lemma to construct N-special abelian varieties $A/\mathbb{Q}$ using the examples of N-special elliptic curves produced in this article.

Lemma 8.3. *Given a number field $L/\mathbb{Q}$ with a subfield K and an abelian variety B/L, let A/K denote the Weil restriction of B/L from L to K. Then the abelian variety A/K has dimension $[L : K]\dim(B)$, and comes with a natural isomorphism $A(K) = B(L)$. In particular, if B/L has a L-rational torsion point of prime order N, then A/K has a K-rational torsion point of order N. Moreover, A/K is N-special if and only if B/L is N-special.*

Proof. Most of the statements simply recall standard properties of the Weil restriction. For the last statement use [40], 3.19, to obtain that $c(A/K) = c(B/L)$. □

Let $N \geq 7$ be prime. It is natural to ask if there are any constraints on the field K when there exists an N-special abelian variety A/K. In the case of elliptic curves, Theorem 4.3 shows that these hypotheses produce information on the Lenstra constant $M(K)$. Given an N-special elliptic curve E/L with $M(L) \geq (N-1)/2$, it is not always the case that a subfield K of L still has a large Lenstra constant. Lemma 8.3, on the other hand, lets us obtain from E/L an abelian variety A/K which is always N-special. Given an N-special abelian variety A/K of dimension g such that the N-torsion subgroup of $A(K)$ has order at least N^g, one may wonder whether it is true that $M(K) \geq (N-1)/2$.

Example 8.4 Let K denote the cubic field of smallest discriminant -23 (in absolute value), with $K = \mathbb{Q}(\alpha)$ and α a root of $x^3 - x^2 + 1$. We present below an N-special abelian threefold A/K with $N = 23$ and $N = 31$. The field K has $M(K) = 5$ [30, Theorem 4.1.1].

Let L denote the field of degree 9 and unit rank 5 defined by the polynomial $x^9 - 2x^8 + x^6 - x^5 + 14x^4 - 28x^3 + 19x^2 - 2x - 1$. The field L has discriminant $-114479303 = -23^3 97^2$ and contains the field K. It has 3246 exceptional units. There exists a 31-special elliptic curve E/L. We can thus consider the Weil restriction A/K from L to K of the elliptic curve E/L, and use Lemma 8.3 to obtain that A/K is 31-special.

There exists a 23-special elliptic curve E'/L' defined over the field L' of degree 9 and unit rank 4 given by the polynomial $x^9 - 2x^8 + 2x^7 - 2x^5 + 2x^4 - x + 1$. The field L' has discriminant $33860761 = 11^2 23^4$ and contains the field K. As above, we can consider the Weil restriction A'/K from L' to K of the elliptic curve E'/L'.

Example 8.5 Consider the decic field K of discriminant $995628125 = 5^5 318601$ and rank 5 given by the polynomial $x^{10} - 3x^9 + 5x^8 - 6x^7 + 6x^6 - 4x^5 + 3x^4 - 2x^3 + x^2 - x - 1$. The field K has 3270 exceptional units. We present below an N-special abelian threefold A/K with $N = 67$. Note that in this example, $M(K) \geq 9$ by Theorem 4.3, since the field K supports

an N-special elliptic curve E_0/K with $N = 19$. The smallest norm of a prime ideal of K is 19, so that $M(K) \leq 19$.

The field K has a Galois extension L/K of degree 3 such that over L, there exists an elliptic curve E/L with everywhere good reduction and an L-rational point of order $N = 67$. The j-invariant of this curve belongs to K, and the curve does not have complex multiplication. This curve was found by van Hoeij (see [69], second given point on $X_1(67)$, over a field of degree 30). We can thus consider the Weil restriction A/K from L to K of the elliptic curve E/L, and use Lemma 8.3 to obtain that A/K has the desired properties.

References

[1] A. Agashe, *Conjectures concerning the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup*, Exp. Math. **22** (2013), no. 4, 363–366

[2] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Mathematics of Computation **79** (2010), no. 272, 2371–2386.

[3] F. Beukers and H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta Arith. **78** (1996), no. 2, 189–199.

[4] G. Billing and K. Mahler, *On exceptional points on cubic curves*, J. London Math. Soc. **15** (1940), 32–43.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. http://magma.maths.usyd.edu.au/magma/

[6] P. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication* (with an appendix by Alex Rice), Int. J. Number Theory **9** (2013), no. 2, 447–479.

[7] P. Clark, P. Corn, A. Rice, and J. Stankewicz, *Computations on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), no. 1, 509–535

[8] J. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[9] L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, in Elliptic curves, Hilbert modular forms and Galois deformations, 135–198, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013.

[10] M. Derickx and M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71.

[11] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596.

[12] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, With an appendix by Tom Fisher. Proc. London Math. Soc. (3) **91** (2005), no. 2, 300–324.

[13] J. Doyle and D. Krumm, *Computing algebraic numbers of bounded height*, Math. Comp. **84** (2015), no. 296, 2867–2891.

[14] N. Elkies, *Elliptic curves in nature*, `http://math.harvard.edu/~elkies/nature.html`

[15] T. Fisher, *Descent calculations for the elliptic curves of conductor* 11, Proc. London Math. Soc. (3) **86** (2003), no. 3, 583–606.

[16] G. Frey, *Some remarks concerning points of finite order on elliptic curves over global fields*, Ark. Mat. **15** (1977), no. 1, 1–19.

[17] M. Hindry and J. Silverman, *Diophantine geometry. An introduction*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2000.

[18] F. Hirzebruch, T. Berger, and R. Jung, *Manifolds and modular forms*, with appendices by N.-P. Skoruppa and by P. Baum. Aspects of Mathematics, E20, Friedr. Vieweg & Sohn, 1992.

[19] J. Houriet, *Exceptional units and Euclidean number fields*, Arch. Math. **88** (2007), no. 5, 425–433.

[20] N. Ishida and N. Ishii, *Generators and defining equation of the modular function field of the group $\Gamma_1(N)$*, Acta Arith. **101** (2002), no. 4, 303–320.

[21] J. Jones, `http://hobbes.la.asu.edu/NFDB/`

[22] J. Jones and D. Roberts, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618.
[23] D. Krumm, *Quadratic points on modular curves*, Thesis, University of Georgia, 2013.
[24] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.
[25] D. Kubert and S. Lang, *Units in the modular function fields, I*, Math. Ann. **218** (1975), 67-96.
[26] D. Kubert and S. Lang, *Modular Units*, Grundlehren Math. Wiss. (Fundamental Principles of Mathematical Science), vol. 244, Springer-Verlag, New York, 1981.
[27] O. Lecacheux, *Unités d'une famille de corps cycliques réels de degré* 6 *liés à la courbe modulaire* $X_1(13)$, J. Number Theory **31** (1989), no. 1, 54–63.
[28] H. Lenstra, *Euclidean number fields of large degree*, Invent. Math. **38** (1976/77), no. 3, 237–254.
[29] A. Leutbecher, *Euclidean fields having a large Lenstra constant*, Ann. Inst. Fourier **35** (1985), no. 2, 83–106.
[30] A. Leutbecher and J. Martinet, *Lenstra's constant and Euclidean number fields*, Arithmetic Conference (Metz, 1981), 87–131, Astérisque, 94, Soc. Math. France, Paris, 1982.
[31] A. Leutbecher and J. Martinet, *Constante de Lenstra et corps de nombres euclidiens*, Seminar on Number Theory, 1981/1982, Exp. No. 4, 7 pp., Univ. Bordeaux I, Talence, 1982.
[32] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, Number theory (Ulm, 1987), 150–178, Lecture Notes in Math., 1380, Springer, New York, 1989.
[33] B. Levi, *Saggio per una teoria aritmetica delle forme cubiche ternarie, Notta III*, Atti della R. Accademia delle scienze di Torino, **43** (1908) 155–176.
[34] Q. Liu, *Algebraic geometry and arithmetic curves*, Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics, 6. Oxford University Press, Oxford, 2002.
[35] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2021.
[36] D. Long and M. Thistlethwaite, *Lenstra-Hurwitz cliques and the class number one problem*, J. Number Theory **162** (2016), 564–577.
[37] D. Lorenzini, *Groups of components of Néron models of Jacobians*, Compositio Math. **73** (1990), no. 2, 145–160.
[38] D. Lorenzini, *Jacobians with potentially good ℓ-reduction*, J. reine angew. Math. **430** (1992), 151–177.
[39] D. Lorenzini, *On the group of components of a Néron model*, J. reine angew. Math. **445** (1993), 109–160.
[40] D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier **61** no. 5 (2011), 1995–2037.
[41] D. Lorenzini, `http://alpha.math.uga.edu/~lorenz/paper.html`
[42] J. Martinet, *Sur la constante de Lenstra des corps de nombres*, Seminar on Number Theory, 1979–1980 (French), Exp. No. 17, 21 pp., Univ. Bordeaux I, Talence, 1980.
[43] B. Mazur, *Modular curves and the Eisenstein ideal*, With an appendix by Mazur and M. Rapoport. Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), 33–186.
[44] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750.
[45] M. Melistas, *Purely additive reduction of abelian varieties with torsion*, J. Number Th. **239** (2022), 21–39.
[46] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. math. **124** (1996), no. 1-3, 437–449.
[47] J.-F. Mestre, *Corps euclidiens, unités exceptionnelles et courbes élliptiques*, J. Number Theory **13** (1981), no. 2, 123–137.
[48] H. Müller, H. Ströher, H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*, J. reine angew. Math. **397** (1989), 100–161.
[49] T. Nagell, *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante*, Math. Zeit. **28** (1928), 10–29.
[50] T. Nagell, *Les points exceptionnels rationnels sur certaines cubiques du premier genre*, Acta Arith. **5** (1959), 333–357.

[51] T. Nagell, *Les points exceptionnels sur les cubiques* $ax^3 + by^3 + cz^3 = 0$, Acta Sci. Math. Szeged **21** (1960), 173–180.
[52] T. Nagell, *Sur une propriété des unités d'un corps algébrique*, Ark. Mat. **5** (1964), 343–356.
[53] T. Nagell, *Quelques problèmes relatifs aux unités algébriques*, Ark. Mat. **8** (1969), 115–127.
[54] T. Nagell, *Sur un type particulier d'unités algébriques*, Ark. Mat. **8** (1969), 163–184.
[55] Y. Namikawa and K. Ueno, *On fibres in families of curves of genus two. I. Singular fibres of elliptic type*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, pp. 297–371. Kinokuniya, Tokyo, 1973.
[56] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier **50** (2000), no. 3, 723–749.
[57] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux **15** (2003), no. 3, 831–838.
[58] A. Pethö, T. Weis, H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*, Internat. J. Algebra Comput. **7** (1997), no. 3, 353–413.
[59] M. Rebolledo, *Merel's theorem on the boundedness of the torsion of elliptic curves*, Arithmetic geometry, 71–82, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009.
[60] M. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **46** (1986), no. 174, 637–658.
[61] SageMath, *The Sage Mathematics Software System*, The Sage Developers, 2021, `https://www.sagemath.org`.
[62] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378.
[63] A. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147.
[64] A. Sutherland, *Alternative defining equations for* $X_1(N)$, `https://math.mit.edu/~drew/X1_altcurves.html`, *Defining equations for* $X_1(N)$ *in raw form*, `http://math.mit.edu/~drew/X1_rawcurves.html`
[65] H. Swinnerton-Dyer and B. Birch, *Elliptic curves and modular functions*, Modular functions of one variable, IV, Edited by B. J. Birch and W. Kuyk. Lect. Notes in Math. **476**, Springer-Verlag, 1975, 2–32.
[66] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Modular functions of one variable, IV, Edited by B. J. Birch and W. Kuyk. Lect. Notes in Math. **476**, Springer-Verlag, 1975, 33–52.
[67] N. Triantafillou, 80 *one-parameter families of sextic integral points on* $y^2 - y = x^3 - x^2$ *minus its* 5 *integral points*, private communication, January 2022.
[68] M. van Hoeij, *Low Degree Places on the Modular Curve* $X_1(N)$, `https://arxiv.org/abs/1202.4355`.
[69] M. van Hoeij, `https://www.math.fsu.edu/~hoeij/files/X1N`, and `https://www.math.fsu.edu/~hoeij/files/X1N/LowDegreePlaces_61_80`.
[70] W. Waterhouse, *Abelian varieties over finite fields* Ann. Sci. ENS (4) **2** (1969), 521–560.
[71] H. Wiersema and C. Wuthrich, *Integrality of twisted L-values of elliptic curves*, Preprint 2021. `https://arxiv.org/abs/2004.05492`
[72] A. Wiles, *Modular curves and the class group of* $\mathbf{Q}(\zeta_p)$, Invent. Math. **58** (1980), no. 1, 1–35.
[73] H. Zimmer, *Torsion groups of elliptic curves over cubic and certain biquadratic number fields*, Arithmetic geometry (Tempe, AZ, 1993), 203–220, Contemp. Math., 174, AMS, Providence, RI, 1994.

Department of mathematics, University of Georgia, Athens, GA 30602, USA
Email address: `lorenzin@uga.edu`