ON ELLIPTIC CURVES OF PRIME POWER CONDUCTOR OVER IMAGINARY QUADRATIC FIELDS WITH CLASS NUMBER ONE

JOHN CREMONA AND ARIEL PACETTI

Abstract. The main result of this paper is to generalize from $\mathbb{Q}$ to each of the nine imaginary quadratic fields of class number one a result of Serre and Mestre-Oesterlé of 1989, namely that if E is an elliptic curve of prime conductor then either E or a 2-isogenous curve or a 3-isogenous curve has prime discriminant. The proof is conditional in two ways: first that the curves are modular, so are associated to suitable Bianchi newforms; and secondly that a certain level-lowering conjecture holds for Bianchi newforms. We also classify all elliptic curves of prime power conductor and non-trivial torsion over each of the nine fields: in the case of 2-torsion we find that such curves either have CM or with a small (finite) number of exceptions arise from a family analogous to the Setzer-Neumann family of elliptic curves over $\mathbb{Q}$.

Introduction

The theory of elliptic curves plays a crucial role in modern number theory. An important advance came with the systematic construction of tables, as done by Cremona for elliptic curves defined over $\mathbb{Q}$ ([Cre97]). The purpose of this article is to extend some well known results concerning elliptic curves of prime power conductor over $\mathbb{Q}$ to imaginary quadratic fields K of class number 1, particularly the ones involving discriminant bounds as Szpiro's conjecture or the characterization of curves of prime conductor given by Mestre-Oesterlé ([MO89]). On doing so, we encounter different problems which are interesting on their own, regarding elliptic curves, namely understanding 2-supersingular elliptic curves over K, describing minimal up to twist elliptic curves over K with a 2-torsion point, finding elliptic curves over K of prime power conductor and a point of order ℓ, for ℓ an odd prime, among others. Although our main concern was to solve such problems for the fields K described above, some of the ideas and techniques developed could be easily adapted to more general number fields.

The first section describes for each K all the possible elliptic curves with complex multiplication (by an order in a field L, not necessarily the same as K) of odd prime power discriminant. The same problem over $\mathbb{Q}$ is not very interesting, as they correspond to integers rings of imaginary quadratic fields with class number 1. For imaginary quadratic fields, in many instances, by twisting one can move the primes in the discriminant, so the situation is much more interesting and difficult.

2010 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 14H52.

Key words and phrases. Elliptic Curves, Prime conductor curves, discriminant bounds.

JEC is supported by EPSRC Programme Grant EP/K034383/1 *LMF: L-Functions and Modular Forms*, and the Horizon 2020 European Research Infrastructures project *OpenDreamKit* (#676541).

AP was supported by a Leverhulme Trust Visiting Professorship and by grants BID-PICT-2013-0294, PIP 2014-2016 11220130100073.

The second section studies curves of odd conductor over K with a rational 2-torsion point. An important result is Theorem 2.3, where a description of all such curves (up to twist) is given. This result is very general, and can be applied to different situations. Using this characterization, we describe all curves of prime power conductor $\mathfrak{p}^r$ with a rational 2-torsion point, according to the following cases: a twist of the curve has good reduction at $\mathfrak{p}$, all twists have additive reduction at $\mathfrak{p}$, or the curve has a twist of multiplicative reduction. We prove that in the first case all curves have CM and come in families, described explicitly in Theorem 2.7. For the additive ones, we prove in Theorem 2.9 that there are only some sporadic cases, and for multiplicative ones, we prove that there are infinitely many and belong to a so called *Setzer-Neumann* family (as in [Set75] for curves defined over $\mathbb{Q}$). As in the classical case, all such curves have rank 0.

An important result obtained after a case by case study is that if E is an elliptic curve defined over K of odd prime power conductor with a rational 2-torsion point, then E or a 2-isogenous curve has odd discriminant valuation.

The third section studies elliptic curves over K of odd prime power conductor with a rational point of order ℓ, for ℓ an odd prime. In Theorem 3.3 we prove that if $\ell = 3$ and $K = \mathbb{Q}(\sqrt{-3})$, then any such curve either has discriminant exponent not divisible by 3, or its 3-isogenous curve satisfies this property. For all other choices of ℓ and K, we give a finite list of possibilities (which are contained in Table 3.1). The results of this section rely on the fact that the ring of integers of K contains finitely many units.

The fourth section contains a brief description of Bianchi modular forms, and states a lowering the level Conjecture in the spirit of Ribet's classical result. The difference is that one does not expect forms of minimal level to lift to characteristic zero (this is why the statement involves group cohomology, which contains a lot of torsion).

Finally, the fifth section contains the main result of the article, namely assuming a level-lowering result, any curve over K of prime conductor has an isogenous curve of prime discriminant. As a Corollary we get a version of Szpiro's conjecture valid for curves of prime power conductor over imaginary quadratic fields of class number 1.

Remark 0.1. All curves explicitly mentioned will be labeled with their LMFDB label, see [LMF13].

Notation and terminology. K will denote an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ of class number 1, with ring of integers $\mathcal{O}_K$. As is well known, there are 9 such fields, with $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Many of the results of Section 2 also apply to the case $K = \mathbb{Q}$.

We say that an ideal or element of $\mathcal{O}_K$ is *odd* if it is coprime to 2. Let e_2 be the ramification degree of 2 in $K/\mathbb{Q}$, so that $e_2 = 1$ except for $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-2})$. Note also that 2 splits only in $K = \mathbb{Q}(\sqrt{-7})$. The primes dividing 2 play a crucial role in section 2, where we will denote by $\mathfrak{q}$ a prime dividing 2, and by $\mathfrak{p}$ any prime ideal (which might divide 2 or not). The valuation at $\mathfrak{p}$ is denoted $v_{\mathfrak{p}}()$. We denote by ε a generator of the finite unit group $\mathcal{O}_K^*$ so that $\varepsilon = -1$ except for $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$ when $\varepsilon = \sqrt{-1}$, or ε is a 6th root of unity, respectively.

Acknowledgments: we would like to thank Nicolas Vescovo for participating in some discussions of the present article, to Luis Dieulefait, for explaining us some technicalities used in the proof of Theorem 5.4 and to Samir Siksek for many useful conversations. The second

author would like to thank the University of Warwick for its hospitality during his visit as a Leverhulme visiting Professor.

1. Curves with complex multiplication

Let K denote one of the nine imaginary quadratic fields with class number one. Let E/K be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in K. Since K has class number one, the j-invariant $j(E)$ is rational, in fact in $\mathbb{Z}$, so E is a twist of the base extension of an elliptic curve defined over $\mathbb{Q}$.

For each field K, we fix one such curve E, choosing it to have bad reduction only at the unique ramified prime $\mathfrak{p}$ of K, and to have endomorphism ring isomorphic to the maximal order $\mathcal{O}_K$. Every other elliptic curve with CM by an order in K is then isogenous to a twist of this base curve E. For $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ respectively we take the base curve to be the base-change to K of the elliptic curve over $\mathbb{Q}$ with LMFDB label 64.a4, 256.d1, 27.a3, 49.a1, 121.b1, 361.a1, 1849.a1, 4489.a1, 26569.a1, respectively. Our goal in this section is to determine which twists of these base curves E have odd prime power conductor, recalling that for $d = 1$ and $d = 3$ respectively, we must consider quartic (respectively sextic) twists and not only quadratic twists.

Remark 1.1. For $d > 3$ the base curve listed is uniquely determined (up to isomorphism over K) by the condition that it has CM by $\mathcal{O}_K$ and bad reduction only at the ramified prime $\mathfrak{p} = (\sqrt{-d})$. However for $d = 1, 2, 3$ there are several choices. In the results of this section, we consider elliptic curves with prime power conductor as explicit twists of the base curve, so it is important to fix this choice.

The automorphic form attached to E/K consists of the sum of two conjugate Hecke Grossencharacters $\{\chi, \bar{\chi}\}$ of infinity types $(1, 0)$ and $(0, 1)$, and conductor $\mathfrak{n}$ which is a power of $\mathfrak{p}$. In particular, $\mathrm{cond}(E) = \mathfrak{n}^2$. Note that the Grossencharacters take values in $K^\times$. The character χ is unramified outside $\mathfrak{p}$, so has conductor a power of $\mathfrak{p}$, and the local character $\chi_\mathfrak{p}$ restricted to $\mathcal{O}_\mathfrak{p}^\times$ is a finite character taking values in the roots of unity of K. In particular, it is quadratic except for $d = -1, -3$.

1.1. $K = \mathbb{Q}(\sqrt{-d})$ **with** $d \neq 1, 3$**.** The character χ is quadratic, and unramified outside the prime $\mathfrak{p} = (\sqrt{-d})$, the unique ramified prime of K. If we twist E by a quadratic character whose ramification at $\mathfrak{p}$ matches that of χ, we get a curve with good reduction at $\mathfrak{p}$. Note that there is no global quadratic Grossencharacter unramified outside $\mathfrak{p}$ which locally matches $\chi_\mathfrak{p}$, as the Archimedean part of all such characters is trivial. In particular, although we can move the ramification by twisting, there is no twist with everywhere good reduction.

Remark 1.2. Rational 2-torsion is preserved under twisting, so the quadratic twists of E have rational 2-torsion if and only if E does. The fields K for which the curves E have a K-rational two torsion point are $K = \mathbb{Q}(\sqrt{-d})$ for $d = 2, 7$.

Theorem 1.3. *Let $K = \mathbb{Q}(\sqrt{-d})$, with $d \neq 1, 3$, and let E/K be the base elliptic curve with CM by $\mathcal{O}_K$ defined above. Then all elliptic curves with complex multiplication over K of odd prime power conductor are isogenous to E or to the quadratic twist of E by $\pi\sqrt{-d}$, where π is a prime such that $\pi \equiv u^2\sqrt{-d} \pmod 4$ for $d \neq 2$, respectively $\pi \equiv u^2(1 + \sqrt{-d}) \pmod 4$ for $d = 2$, with u odd. In particular, for $d = 7$, the condition reads $\pi \equiv \sqrt{-7} \pmod 4$, for $d = 2$ the condition reads $\pi \equiv \pm 1 + \sqrt{-2} \pmod 4$ and for $d \geq 11$, the condition reads $\pi \equiv w^{2k}\sqrt{-d} \pmod 4$, for $0 \leq k \leq 2$, where $w = \frac{1+\sqrt{-d}}{2}$.*

Before giving the proof, we need an auxiliary result.

Lemma 1.4. *Let K be a 2-adic field, and $\alpha \in \mathcal{O}_K$ be a 2-adic integer which is a unit. Then the extension $K(\sqrt{\alpha})$ is unramified if and only if there exist a unit $u \in \mathcal{O}_K$ such that $u^2 \equiv \alpha \pmod 4$.*

Proof. Let $L = K(\sqrt{a})$ be the quadratic extension. The ring $\mathcal{O}_K[\sqrt{a}] \subset \mathcal{O}_L$ has discriminant $4a$ over $\mathcal{O}_K$. Then the extension $\mathcal{O}_L$ is unramified if and only if $[\mathcal{O}_L : \mathcal{O}_K[\sqrt{a}]] = 2$, if and only if $\frac{u+v\sqrt{a}}{2} \in \mathcal{O}_L$ for some $u, v \in \mathcal{O}_K$ units. The minimal polynomial of any such element is $x^2 + ux + \frac{u^2-av^2}{4}$, hence the index is 2 if and only if there exist units u, v in $\mathcal{O}_K$ such that $u^2 \equiv av^2 \pmod 4$. Multiplying by the inverse of v we get the result. □

Proof of Theorem1.3. Since all curves with complex multiplication over K are isogenous to a quadratic twist of E, we are led to determine which quadratic twists have bad reduction at exactly one odd prime. Any global character corresponds to a quadratic extension $K(\sqrt{\alpha})$. If the twist has good reduction at $\mathfrak{p}$, then $\mathfrak{p} \mid \alpha$ (and the twist attains good reduction at $\mathfrak{p}$), and the curve will have bad reduction at all other primes dividing α. Thus $(\alpha) = \mathfrak{p}\mathfrak{q}$, for $\mathfrak{q}$ an odd prime. Finally, we need to check whether the character is unramified at 2, which follows from Lemma 1.4, and a description in each case of the squares modulo 4.

Explicitly, for odd d we require $\alpha = \pi\sqrt{-d}$, where $\mathfrak{q} = (\pi)$, such that $\alpha \equiv u^2 \pmod 4$. For $d = 7$ the only odd square modulo 4 is 1. For $d \geq 11$, since 2 is inert in K the odd squares modulo 4 are the squares of the odd residues modulo 2, which are $1, w, w^2$. For $d = 2$, the twist of the base curve by $(1+\sqrt{-2})\sqrt{-2}$ has odd conductor $(1+\sqrt{-2})^2$, so we must twist by $\pi\sqrt{-2}$ where $\pi \equiv (1+\sqrt{-2})u^2 \pmod 4$; since the odd squares modulo 4 are 1 and $-1+2\sqrt{-2}$ we obtain the condition stated. □

Remark 1.5. In each case in Theorem 1.3, the condition on π is satisfied by one quarter of the odd residue classes modulo 4. Since $\mathfrak{q} = (\pi)$ has two generators $\pm\pi$, our construction gives curves of conductor $\mathfrak{q}^2$ for half the odd primes of K.

1.2. **$K = \mathbb{Q}(\sqrt{-1})$.** The elliptic curve with complex multiplication by $\mathbb{Z}[\sqrt{-1}]$ is

$$E : y^2 = x^3 + x \qquad \text{with label 64.a4.}$$

Its conductor over K equals $\mathfrak{p}^8$, where $\mathfrak{p} = (1+\sqrt{-1})$. In particular, $\chi_{\mathfrak{p}}$ has conductor $\mathfrak{p}^4$ and order 4. Note that since the automorphism group of E is cyclic of order 4 we must consider *quartic twists*. For $\alpha \in K$, the quartic twist of E by α equals

$$E_\alpha : y^2 = x^3 + \alpha x. \tag{1}$$

Note that this operation does not coincide with the twist of the L-series by a quartic character (as such L-series do not satisfy a functional equation). Indeed, if E corresponds to the automorphic form $\chi \oplus \bar{\chi}$ (where χ is a Grossencharacter), then E_α corresponds to the automorphic form $\chi\psi \oplus \bar{\chi}\bar{\psi}$, where $\psi = \left(\frac{}{\alpha}\right)_4$ (the quartic Legendre symbol). It is still true that the curve E_α is isomorphic to E over the extension $K(\sqrt[4]{\alpha})$.

Remark 1.6. All the quartic twists of E have a non-trivial K-rational 2-torsion point.

We first need a local result about when a pure quartic extension is unramified above 2.

Lemma 1.7. *Let $K = \mathbb{Q}_2(\sqrt{-1})$, and let $\alpha \in \mathcal{O}_K$ be a unit. Then the extension $K(\sqrt[4]{\alpha})$ is unramified over K if and only if $\alpha \equiv 1, 1 + 4\sqrt{-1} \pmod 8$.*

Proof. The extension $K(\sqrt[4]{\alpha})$ depends on α up to 4-th powers, i.e. two elements give the same extension if and only if they differ by a 4-th power. By Hensel's Lemma, an odd element of $\mathbb{Q}_2(\sqrt{-1})$ is a fourth power if and only if it is congruent to 1 modulo $(1+\sqrt{-1})^7$, hence the extension is characterized by α modulo $(1+\sqrt{-1})^7$. Also, $K(\sqrt[4]{\alpha})$ is unramified if and only if it is contained in the unique unramified extension of K of degree 4, which is $K(\zeta_5) = K(\sqrt[4]{1+4\sqrt{-1}})$, as can be easily checked. Thus, for $K(\sqrt[4]{\alpha})$ to be unramified, α must be congruent to a power of $1+4\sqrt{-1}$, i.e. $\alpha \equiv 1, 1+4\sqrt{-1}, 9,$ or $9+4\sqrt{-1} \pmod{(1+\sqrt{-1})^7}$; this simplifies to $\alpha \equiv 1, 1+4\sqrt{-1} \pmod 8$ as stated. □

Theorem 1.8. *Let $K = \mathbb{Q}(\sqrt{-1})$ and let E/K be the elliptic curve* 64.a4*. Then all elliptic curves with complex multiplication over K of odd prime power conductor are isogenous to the quartic twist of E by π, where π is a prime power such that $\pi \equiv -1 \pm 2\sqrt{-1} \pmod 8$.*

Proof of Theorem 1.8. Let $\pi = -1+2\sqrt{-1}$. One may check that the quartic twist of E by π has good reduction at 2 and bad additive reduction at $(-1+2\sqrt{-1})$. Then any quartic twist of E of odd conductor is a twist of $E_{-1+2\sqrt{-1}}$ by a quartic character of odd conductor, which by Lemma 1.7 correspond to elements which are congruent to 1 or $1+4\sqrt{-1} \pmod 8$. Multiplying by $-1+2\sqrt{-1}$ gives the classes $-1 \pm 2\sqrt{-1} \pmod 8$ as stated. □

Remark 1.9. Of all odd primes $\mathfrak{q}$ of K, one quarter have a generator π satisfying the condition in Theorem 1.8. Hence our construction gives elliptic curves of conductor $\mathfrak{q}^2$ for one quarter of all primes $\mathfrak{q}$ of K.

1.3. $K = \mathbb{Q}(\sqrt{-3})$**.** The elliptic curve with complex multiplication by $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is the curve 27.a3, with (non-minimal) equation

$$E : y^2 = x^3 + 16.$$

Its conductor over K is $\mathfrak{p}^4$, where $\mathfrak{p} = (\sqrt{-3})$. In particular, $\chi_{\mathfrak{p}}$ has conductor $\mathfrak{p}^2 = (3)$ and order 6 (note that $(\mathcal{O}_K/3)^\times \simeq \mathbb{Z}/6\mathbb{Z}$). Since E has automorphism group of order 6, we must consider sextic twists, where the sextic twist by $\alpha \in K$ of the previous model is

$$E_\alpha : y^2 = x^3 + 16\alpha. \tag{2}$$

The same considerations as the quartic twists apply. In particular, the curve E_α is isomorphic to E over the extension $K(\sqrt[6]{\alpha})$; such twists are needed to cancel the CM character $\chi_{\mathfrak{p}}$.

As before, we need local results, now at both 2 and 3:

Lemma 1.10. *Let $K = \mathbb{Q}(\sqrt{-3})$, let $w = (1+\sqrt{-3})/2 \in K$ be a 6th root of unity, and let $\alpha \in \mathcal{O}_K$ be a 2-adic and 3-adic unit. Then the extension $K(\sqrt[6]{\alpha})/K$ is unramified over both 2 and 3 if and only if*

- *$\alpha \equiv 1, w^2,$ or $w^4 \pmod 4$ (equivalently, α is congruent to a square modulo 4); and*
- *$\alpha \equiv \pm 1 \pmod{\sqrt{-3}^3}$ (equivalently, α is congruent to a cube modulo $\sqrt{-3}^3$).*

Proof. Since $K(\sqrt[6]{\alpha}) = K(\sqrt{\alpha}, \sqrt[3]{\alpha})$ we require both $K(\sqrt{\alpha})/K$ and $K(\sqrt[3]{\alpha})/K$ to be unramified. The first is certainly unramified over 3, and over 2 we may apply Lemma 1.4 to obtain the first condition stated.

Similarly, $K(\sqrt[3]{\alpha})/K$ is always unramified over 2, so we need the condition for it to be unramified also over 3. By Hensel's Lemma, a unit of $\mathbb{Q}_3(\sqrt{-3})$ is a cube if and only if it is congruent to ± 1 modulo 9, hence the extension is characterized by α modulo 9. We may check that $K(\sqrt[3]{\alpha_1})$ is unramified, for $\alpha_1 = 2+3w$. Hence $K(\sqrt[3]{\alpha})/K$ is unramified at 3 if and only if $\alpha \equiv \pm 1, \pm\alpha_1, \pm\alpha_1^2 \pmod 9$, which is if and only if $\alpha \equiv \pm 1 \pmod{\sqrt{-3}^3}$. □

Theorem 1.11. *Let $K = \mathbb{Q}(\sqrt{-3})$ let E/K be the elliptic curve* 27.a3*. Then all elliptic curves with complex multiplication over K of odd prime power conductor are isogenous to E or to the sextic twist E_α of E by $\alpha = \sqrt{-3}^3\pi$, where π is a prime power such that:*

- $\pi \equiv \sqrt{-3}, \sqrt{-3}w^2$, *or* $\sqrt{-3}w^4 \pmod 4$, *and*
- $\pi \equiv \pm 4 \pmod{\sqrt{-3}^3}$,

where $w = (1+\sqrt{-3})/2$ is a 6th root of unity.

Proof. E itself has good reduction except at $\sqrt{-3}$; by Lemma 1.10, the sextic twist E_α will also have good reduction at 2 provided that α is an odd square modulo 4, equivalently $\alpha \equiv 1, w^2, w^4 \pmod 4$. Hence the first condition on π ensures that E_α has good reduction except at π and (possibly) at $\sqrt{-3}$.

The twist E_{α_1} with $\alpha_1 = \sqrt{-3}^3 \cdot 4$ has good reduction at $\sqrt{-3}$. Hence by Lemma 1.10, E_α has good reduction at $\sqrt{-3}$ if α/α_1 is a cube modulo $\sqrt{-3}^3$, or equivalently $\alpha/\alpha_1 \equiv \pm 1 \pmod{\sqrt{-3}^3}$. This is ensured by the second condition, since $\pi/4 = \alpha/\alpha_1$. □

Remark 1.12. The curves in the previous family never have a rational 2-torsion point, since 2α is not a cube.

Remark 1.13. Of all primes of K other than (2) and $(\sqrt{-3})$, half have a generator π satisfying the 2-adic condition in Theorem 1.11, and one third have a generator satisfying the 3-adic condition. Hence our construction gives elliptic curves of conductor $\mathfrak{p}^2$ for about one sixth of all primes $\mathfrak{p}$ of K.

1.3.1. *Curves with complex multiplication by K over an imaginary quadratic field L.* A natural question is what happens if we consider a curve E with complex multiplication by an order in K, over an imaginary quadratic field L: are there twists of E with good reduction at primes dividing $\mathrm{cond}(E)$?

The proofs of the previous results are of a local nature, hence if L has the same completion at a prime dividing $\mathrm{cond}(E)$ as K we are in exactly the same situation.

Theorem 1.14. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor p^r with complex multiplication by an order in K. Let $L = \mathbb{Q}(\sqrt{-t})$ be an imaginary quadratic field different from K and $\mathfrak{p}$ a prime ideal of L dividing p. If the completion of L at $\mathfrak{p}$ is isomorphic to the completion of K at the prime dividing p, then there exists $\alpha \in L$ such that:*

- *if $K = \mathbb{Q}(\sqrt{-d})$, $d \neq 1, 3$, then the quadratic twist of E/L by $\sqrt{-t}\,\alpha$ has good reduction at $\mathfrak{p}$.*
- *if $K = \mathbb{Q}(\sqrt{-1})$, let $\sqrt{-1}$ denote an element of L whose square root equals -1 modulo 8. Then then the quartic twist of the curve* 64.a4 *by α has good reduction at 2 for $\alpha \equiv -1 \pm 2\sqrt{-1} \pmod 8$.*
- *if $K = \mathbb{Q}(\sqrt{-3})$, let $\sqrt{-3}$ denote an element of L whose square is congruent to -3 modulo 9. Then the sextic twist of the curve* 27.a3 *by α has good reduction at 3 for $\alpha \equiv \pm 4\sqrt{-3}^3 \pmod{\sqrt{-3}^3}$.*

On the other hand, if the completions are not isomorphic, no such twist exists.

Proof. The proof of the first facts mimics that of Theorems 1.3, 1.8 and 1.11, as the completions being isomorphic implies that the local reduction types are the same. If the local completions are not isomorphic, consider the Weil representation attached to our elliptic curve (recall that CM elliptic curves have no monodromy, hence we do not need to consider the whole Weil-Deligne representation). Then the image of inertia at $\mathfrak{p}$ equals:

- a cyclic group of order 4 if $d \neq -1, -3$,
- the dihedral group of order 8 if $d = -1$,
- the dihedral group of order 12 if $d = -3$.

In the first case, we cannot take a quartic twist, so we cannot cancel the ramification, and the other two ones are not abelian, hence the statement follows. □

Corollary 1.15. *If $E/\mathbb{Q}$ is an elliptic curve with complex multiplication by a suborder of K and L is an imaginary quadratic field of class number 1 different from K, then E is the unique curve in the family of its appropriate twists (quadratic, quartic or sextic) of prime power conductor.*

Proof. Let $D = \{1, 2, 3, , 7, 11, 19, 43, 67, 163\}$. The field $\mathbb{Q}(\sqrt{-d})$ for each odd $d \in D$ has a different ramification set, hence we cannot get good reduction at d by Theorem 1.14. For $d \in D$ even, the completions for $d = 1$ and $d = 2$ are also different, hence we cannot get odd conductor while looking at the curve with CM by an order of $\mathbb{Q}(\sqrt{-1})$ over $\mathbb{Q}(\sqrt{-2})$ and vice versa. □

2. Curves with rational 2-torsion

Our goal in this section is to classify all elliptic curves E defined over K with odd prime power conductor which have a K-rational point of order 2. As a result we will see (Corollary 2.13 below) that each isogeny class of such curves contains a curve whose discriminant has odd valuation, which will be important in the last section of the paper.

2.1. Preliminaries on curves with odd conductor and rational 2-torsion.

In this subsection and the next we assume that E is an elliptic curve defined over K, with odd conductor, and with a rational 2-torsion point; later we will specialize to the case where the conductor is an odd prime power. Such an elliptic curve E has an equation of the form

$$E_{a,b} : y^2 = x(x^2 + ax + b), \tag{3}$$

where $a, b \in \mathcal{O}_K$ and the given 2-torsion point is $(0, 0)$. However, while it is easy to see that this model can be taken to be minimal at all odd primes, we need to be more precise concerning the primes dividing 2 where such a model cannot have good reduction. To this end, we need to consider carefully the transformation from a global minimal model for E (which exists since K has class number 1) to this form. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4}$$

be a global minimal model for E; its discriminant $\mathcal{D}_{\min}(E)$ is odd since E has odd conductor. To transform this model into $E_{a,b}$ we first complete the square, then scale to make the equation integral, and finally translate the x-coordinate so that the 2-torsion point has $x = 0$.

After completing the square the right-hand side of the equation is

$$x^3 + (a_2 + (a_1/2)^2)x^2 + (a_4 + (a_1/2)a_3)x + (a_6 + (a_3/2)^2) \tag{5}$$

which is still integral, and minimal, at all odd primes. Let $\mathfrak{q} = (\tau)$ be a prime of K dividing 2. Then a_1 and a_3 are not both divisible by $\mathfrak{q}$, as otherwise $\mathfrak{q}$ would divide the discriminant, so (5) is not already integral at $\mathfrak{q}$. To make the equation integral we scale x by τ^{2r} for some $r \geq 1$ chosen to be minimal. The minimal r depends on whether E is ordinary or supersingular at $\mathfrak{q}$, or equivalently whether $v_{\mathfrak{q}}(a_1) = 0$ or $v_{\mathfrak{q}}(a_1) > 0$.

Proposition 2.1. *Let E be an elliptic curve of odd conductor over K with a K-rational point of order 2 with minimal equation (4). Let $\mathfrak{q} = (\tau)$ be a prime of K dividing 2.*

1. *If E has ordinary reduction at $\mathfrak{q}$ (that is, if $v_{\mathfrak{q}}(a_1) = 0$), then the minimal scaling to make (5) integral is $x \mapsto 2^2 x$ with scaling exponent $r = 2e_2$.*
2. *If E has supersingular reduction at $\mathfrak{q}$ (that is, if $v_{\mathfrak{q}}(a_1) > 0$), then K is ramified at 2 and $v_{\mathfrak{q}}(a_1) = 1$. The minimal scaling is $x \mapsto \tau^2 x$ with $r = 2$.*

In both cases, after scaling, (5) reduces to $x^2(x+u)$ modulo $\mathfrak{q}$ with u odd. In the supersingular case, there is only one K-rational point of order 2, whose x-coordinate (after scaling) is odd.

Proof. After scaling x by τ^{2r}, the coefficient of x^{3-j} is multiplied by τ^{2rj}.

First suppose that $v_{\mathfrak{q}}(a_1) = 0$ (the ordinary case). From the coefficient of x^2 in (5) it is immediate that $x \mapsto 4x$ is the minimal scaling which gives integral coefficients. After scaling, the coefficient of x^2 is $u = a_1^2 + 4a_2$, with $\mathfrak{q}$-valuation 0, and the others are divisible by 8 and 16 respectively.

Now suppose that $v_{\mathfrak{q}}(a_1) > 0$ (the supersingular case), which implies $v_{\mathfrak{q}}(a_3) = 0$. If $v_{\mathfrak{q}}(a_1) \geq e_2$, then all coefficients in (5) are $\mathfrak{q}$-integral except the last one, which has $\mathfrak{q}$-valuation $-2e_2$. But then all roots have valuation $-2e_2/3$, which is not an integer, contradicting the fact that the polynomial has a root in K. It follows that this supersingular case can only occur if $e_2 = 2$ and $v_{\mathfrak{q}}(a_1) = 1$. The coefficients in (5) now have valuations -2, -1, -4, from which it follows that the roots (whether in K or an extension) have valuations -2, -1, -1; since the x-coordinates of non-integral K-rational points must have even valuation, there can be only one K-rational point of order 2, with x-coordinate of valuation -2. To achieve integrality we must scale x by τ^2, after which the cubic reduces to $x^2(x+1)$ modulo $\mathfrak{q}$ and the x-coordinate of the K-rational point of order 2 is odd. □

We will refer to the two cases of this proposition as "the ordinary case" and "the supersingular case" respectively.

The model $E_{a,b}$ has invariants

$$\Delta = 2^4 b^2(a^2 - 4b), \qquad c_4 = 2^4(a^2 - 3b), \qquad c_6 = 2^5 a(9b - 2a^2). \tag{6}$$

We set $\mathcal{D}(E) = b^2(a^2 - 4b)$, and compare this with $\mathcal{D}_{\min}(E)$. In the ordinary case, $\Delta = 2^{12}\mathcal{D}_{\min}(E)$ so $\mathcal{D}(E) = 2^8\mathcal{D}_{\min}(E)$; in the supersingular case, $\Delta = \tau^{12}\mathcal{D}_{\min}(E)$ and $\mathcal{D}(E) = \pm 2^2\mathcal{D}_{\min}(E)$, with sign -1 for $\mathbb{Q}(\sqrt{-1})$ when $\tau = 1+\sqrt{-1}$ and $+1$ for $\mathbb{Q}(\sqrt{-2})$ when $\tau = \sqrt{-2}$.

Corollary 2.2. *Let $(x_0, 0)$ be the coordinates of the given 2-torsion point on the scaled model, so $x_0 \in \mathcal{O}_K$. We obtain a model of the form $E_{a,b}$ by shifting the x-coordinate by x_0.*

1. *In the ordinary case, if $v_{\mathfrak{q}}(x_0) > 0$ then we obtain (a, b) with $(v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(b)) = (0, 4e_2)$, while if $v_{\mathfrak{q}}(x_0) = 0$ then $(v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(b)) = (e_2, 0)$.*
2. *In the supersingular case we always have $v_{\mathfrak{q}}(x_0) = 0$, and $(v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(b)) = (k, 0)$ with $k \geq 3$. (We include the possibility that $a = 0$ here.)*

Proof. After the shift by x_0 we have $\mathfrak{q} \mid b$ if x_0 reduces to the double root modulo $\mathfrak{q}$ and $\mathfrak{q} \mid a$ otherwise; $\mathfrak{q}$ does not divide both since there is no triple root modulo $\mathfrak{q}$. In the supersingular case, $\mathfrak{q}$ must divide a.

Suppose that $\mathfrak{q} \mid b$. Then we are in the ordinary case, and $8e_2 = v_{\mathfrak{q}}(\mathcal{D}(E)) = 2v_{\mathfrak{q}}(b)$ so $v_{\mathfrak{q}}(b) = 4e_2$.

Alternatively, suppose that $\mathfrak{q} \mid a$. Then in the ordinary case, $v_{\mathfrak{q}}(a^2 - 4b) = v_{\mathfrak{q}}(\mathcal{D}(E)) = 8e_2 > 2e_2 = v_{\mathfrak{q}}(4b)$, so $v_{\mathfrak{q}}(a^2) = 2e_2$ and $v_{\mathfrak{q}}(a) = e_2$. In the supersingular case, $v_{\mathfrak{q}}(a^2 - 4b) =$

$4 = v_{\mathfrak{q}}(4b)$ so $v_{\mathfrak{q}}(a) \geq 2$; however it is easy to see that $v_{\mathfrak{q}}(a) = 2$ leads to a contradiction since the residue field at $\mathfrak{q}$ has only size 2. □

Note that $a = 0$ can only happen in the supersingular case. Such curves have CM by $\mathbb{Z}[\sqrt{-1}]$ and were considered in the previous section.

In what follows it would be enough to determine curves up to quadratic twist, since given one elliptic curve it is straightforward (see [CL07]) to find all of its twists with good reduction outside a fixed set of primes. The quadratic twists of $E_{a,b}$ have the form $E_{\lambda a,\lambda^2 b}$ for $\lambda \in K^*$. Taking $\lambda = \mu^{-1}$ with $\mu \in \mathcal{O}_K$, where $\mu \mid a$ and $\mu^2 \mid b$, we obtain a curve with a smaller discriminant, by a factor μ^6. In our situation of curves with odd conductor, such a factor μ must be odd, supported on primes of bad reduction, and also square-free (by minimality of the equation at all odd primes). However, if $\mathfrak{p} = (\pi)$ is an odd prime factor of the conductor such that $\pi \mid a$ and $\pi^2 \mid b$, it can happen[1] that the twist E^π acquires bad reduction at a prime $\mathfrak{q}$ dividing 2: this is the case if $\mathfrak{q}$ ramifies in $K(\sqrt{\pi})$.

For a prime $\mathfrak{p} = (\pi)$ we say that the pair (a, b) is *minimal* at $\mathfrak{p}$ (or π) if either $\pi \nmid a$ or $\pi^2 \nmid b$. When (a, b) are the parameters obtained from a curve of odd conductor, we have already seen that (a, b) is minimal at $\mathfrak{q}$ for all $\mathfrak{q} \mid 2$ since either a or b is not divisible by $\mathfrak{q}$, while for the primes $\mathfrak{p}$ dividing the conductor, (a, b) may not be $\mathfrak{p}$-minimal. However, as already observed, we can always assume that either $\pi^2 \nmid a$ or $\pi^4 \nmid b$.

Since we cannot assume that a minimal twist of a curve with odd conductor still has odd conductor, we will need to consider curves with non-minimal (a, b). In the prime power conductor case, this means that we will consider curves in sets of four twists, a base curve $E = E_{a,b}$ which is $\mathfrak{p}$-minimal, may have bad reduction at primes dividing 2, and may even have good reduction at $\mathfrak{p}$; and the twists E^s of E by $s \in \{\varepsilon, \pi, \varepsilon\pi\}$, where $\mathfrak{p} = (\pi)$.

For example, over $K = \mathbb{Q}(\sqrt{-2})$ we have seen in the previous section that the elliptic curve 256.d1, which has conductor $(\sqrt{-2})^{10}$, has infinitely many quadratic twists of odd prime square conductor.

2.2. **Classification of curves with odd conductor and 2-torsion.** We continue with the notation of the previous subsection: E is an elliptic curve with odd conductor and a K-rational point of order 2, and (a, b) are parameters for the model $E_{a,b}$ for E constructed above. Write $(2) = \mathfrak{q}_a\mathfrak{q}_b$ where $\mathfrak{q}_a$, with generator τ_a, (respectively $\mathfrak{q}_b$, with generator τ_b), is divisible only by primes dividing a (respectively b), and $2 = \tau_a\tau_b$. For $K \neq \mathbb{Q}(\sqrt{-7})$ we have $(\tau_a, \tau_b) = (1, 2)$ or $(2, 1)$ according to whether $(v_{\mathfrak{q}}(a), v_{\mathfrak{q}}(b)) = (0, 4e_2)$ or $(e_2, 0)$ for the unique prime $\mathfrak{q}$ dividing 2 in the ordinary case, and also $(\tau_a, \tau_b) = (2, 1)$ in the supersingular case.

The following result completely classifies curves with odd conductor and a point of order 2 in terms of the solutions to a certain equation (7).

Theorem 2.3. *Let E be an elliptic curve defined over K, with a K-rational 2-torsion point and odd conductor. Let $D = \mathcal{D}_{min}(E)$. Set*

- $P = \gcd(D, b, a^2 - 4b) = As^2$ *with A square-free;*
- $B = (a^2 - 4b)/(\tau_a^2 P)$*;*
- $C = 4b/(\tau_a^2 P)$*;*
- $\tilde{a} = as/(\tau_a P)$.

[1]This does not happen over $\mathbb{Q}$ since for every odd prime ideal (p) either $\pm p \equiv 1 \pmod 4$ so that $\mathbb{Q}(\sqrt{\pm p})$ is unramified at 2.

Then

$$\tilde{a}^2 A = B + C \tag{7}$$

and $\tilde{a}, A, B, C \in \mathcal{O}_K$ *satisfy the following conditions:*

(1) $\gcd(B, C) = 1$ *and* A *is square-free;*

(2) A, B, C *are only divisible by primes dividing* $2D$*.*

Furthermore,

- *For each prime* $\mathfrak{p} \mid D$ *with* $k = v_{\mathfrak{p}}(D)$ *and* $k' = k - 6$*:*

$$(v_{\mathfrak{p}}(A), v_{\mathfrak{p}}(B), v_{\mathfrak{p}}(C)) = (0, k, 0), (0, k', 0), (0, 0, \frac{1}{2}k), (0, 0, \frac{1}{2}k') \quad \text{or} \quad (1, 0, 0);$$

- *In the ordinary case, for each prime* $\mathfrak{q} \mid 2$*,*

$$(v_{\mathfrak{q}}(A), v_{\mathfrak{q}}(B), v_{\mathfrak{q}}(C)) = (0, 6e_2, 0) \quad \text{or} \quad (0, 0, 6e_2).$$

- *In the supersingular case, for* $\mathfrak{q} \mid 2$*,* $(v_{\mathfrak{q}}(A), v_{\mathfrak{q}}(B), v_{\mathfrak{q}}(C)) = (0, 0, 0)$*.*

Conversely, given integral $A, B, C, \tilde{a}$ *satisfying* $\tilde{a}^2 A = B + C$ *and the above conditions, if we set* $a = 2A\tilde{a}/\gcd(2, C)$ *and* $b = AC/\gcd(2, C)^2$ *then* $E_{a,b}$ *and its twists* E_{sa,s^2b} *for all square-free* $s \in \mathcal{O}_K$ *dividing* D*, all have good reduction outside* $2D$*.*

Proof. We have $a^2 = (a^2 - 4b) + 4b = B_0 + C_0$ where $B_0 = a^2 - 4b = \mathcal{D}(E)/b^2$ and $C_0 = 4b$, and consider $\gcd(B_0, C_0)$ one prime at a time, these primes all being divisors of $2D$.

First consider odd primes $\mathfrak{p} = (\pi)$. These contribute to P if $\mathfrak{p} \mid B_0$ and $\mathfrak{p} \mid C_0$, so that $\mathfrak{p} \mid b$ and $\mathfrak{p} \mid a$. In general, the contribution to P from $\mathfrak{p}$ is π^j where $j = \min\{v_{\mathfrak{p}}(b), v_{\mathfrak{p}}(a^2 - 4b)\}$, with $0 \le j \le 3$ as in table 2.1, where $k = v_{\mathfrak{p}}(D)$. The entries above the line correspond to (a, b) being $\mathfrak{p}$-minimal while those below are non-minimal. We include $a = 0$ as a possibility in each row with ' $\ge$ ' in the first column. Let P be the product of π^j over all these odd

$v_{\mathfrak{p}}(a)$	$v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(C_0)$	$v_{\mathfrak{p}}(a^2 - 4b) = v_{\mathfrak{p}}(B_0)$	j	k	$v_{\mathfrak{p}}(A)$	$v_{\mathfrak{p}}(B)$	$v_{\mathfrak{p}}(C)$
0	0	≥ 0	0	≥ 0	0	k	0
≥ 1	0	0	0	0	0	0	0
0	≥ 1	0	0	≥ 2, even	0	0	$\frac{1}{2}k$
≥ 1	1	1	1	3	1	0	0
1	2	≥ 2	2	≥ 6	0	$k-6$	0
≥ 2	2	2	2	6	0	0	0
1	≥ 3	2	2	≥ 8, even	0	0	$\frac{1}{2}(k-6)$
≥ 2	3	3	3	9	1	0	0

TABLE 2.1. Possible parameter valuations at an odd prime

prime ideals. We can write $P = As^2$ with A and s square-free (since $j \le 3$ in all cases); P is the odd part of $\gcd(a^2 - 4b, 4b)$ which is $\gcd(D, b, a^2 - 4b)$.

Now consider the prime (or primes) $\mathfrak{q} \mid 2$, which divide a or b but not both by Corollary 2.2. The possible valuations are given in table 2.2. Since $e_2 = 2$ in the supersingular case, this prime(s) contributes τ_a^2 to $\gcd(B_0, C_0)$.

Hence $\gcd(B_0, C_0) = \tau_a^2 P$; dividing through gives $\tilde{a}^2 A = B + C$ with $B, C, \tilde{a}$ as given. In the factorization $P = As^2$, A is the product of those odd π for which j is odd while s is the product of those for which $j \ge 2$; both are square-free divisors of D.

For all primes $\mathfrak{p}$ dividing $2D$, the values of $v_{\mathfrak{p}}(A)$, $v_{\mathfrak{p}}(B)$, $v_{\mathfrak{p}}(C)$ in the tables may easily be deduced from the previous columns.

Case	$v_\mathfrak{p}(a)$	$v_\mathfrak{p}(b)$	$v_\mathfrak{p}(B_0) = v_\mathfrak{p}(a^2-4b)$	$v_\mathfrak{p}(C_0) = v_\mathfrak{p}(4b)$	$v_\mathfrak{p}(A)$	$v_\mathfrak{p}(B)$	$v_\mathfrak{p}(C)$
Ordinary	0	$4e_2$	0	$6e_2$	0	0	$6e_2$
	e_2	0	$8e_2$	$2e_2$	0	$6e_2$	0
Supersingular	≥ 3	0	4	4	0	0	0

TABLE 2.2. Possible parameter valuations at a prime dividing 2

For the converse, it suffices to observe that with a, b as defined we have $b^2(a^2-4b) = 4A^3BC^2/\gcd(2,C)^6$, whose support lies in $2D$, and hence determines a base curve $E_{a,b}$, which has good reduction away from $2D$. The same is true of twists by square-free s dividing D. □

Remark 2.4. We can scale solutions (A, B, C) to (7) by units without affecting the conditions, and scaling by squares of units gives isomorphic curves. Since K has finitely many units, for each odd $D \in \mathcal{O}_K$, we can use Theorem 2.3 to compute all curves of discriminant D with a K-rational two-torsion point. This will be our strategy in the following subsections, where we restrict to the case where there is only one odd prime factor.

Recall that each curve $E_{a,b}$ has a 2-isogenous curve E_{-2a,a^2-4b}, via the 2-isogeny with kernel $(0,0)$, which has the same conductor as E. At odd primes $\mathfrak{p}$ it is immediate that (a,b) is minimal at $\mathfrak{p}$ if and only if $(a',b') = (-2a, a^2-4b)$ is minimal. When $E_{a,b}$ has odd conductor with (a,b) given by our construction, at primes $\mathfrak{q}$ dividing 2 we see that in the ordinary case, $(v_\mathfrak{q}(a), v_\mathfrak{q}(b)) = (0, 4e_2)$ implies $(v_\mathfrak{q}(-2a), v_\mathfrak{q}(a^2-4b)) = (e_2, 0)$, while conversely if $(v_\mathfrak{q}(a), v_\mathfrak{q}(b)) = (e_2, 0)$ then $(v_\mathfrak{q}(a'), v_\mathfrak{q}(b')) = (2e_2, 8e_2)$ and the associated minimal pair is $(a'/\tau^{2e_2}, b'/\tau^{4e_2})$ with valuations $(0, 4e_2)$. In the supersingular case with valuations $(\geq 3, 0)$, a minimal pair for the isogenous curve is $(a'/(-2), b'/4) = (a, (a/2)^2 - b)$ with the same valuations as (a,b).

Proposition 2.5. *Following the notation of Theorem 2.3, if $E_{a,b}$ is a curve with odd conductor associated to a triple (A,B,C) satisfying (7), then the 2-isogenous curve E_{-2a,a^2-4b} has associated triple (A,C,B).*

Proof. It is clear that the parameter A is the same for both curves, and then a straightforward computation gives the result, using the remarks about minimality stated above. □

Given an odd prime ideal $\mathfrak{p} = (\pi)$ of bad reduction, we have two different situations depending on whether $v_\mathfrak{p}(A) = 0$ or $v_\mathfrak{p}(A) = 1$. In the first case, one curve in each isogenous pair has double the discriminant valuation of the other, and one of the two isogenous pairs, which are π-twists of each other, has good or multiplicative reduction at $\mathfrak{p}$ (when the parameter s of Theorem 2.3 is not divisible by π), while the other has additive reduction (when s is divisible by π). In the second case, all curves have additive reduction at $\mathfrak{p}$, one isogenous pair (with $\pi \nmid s$) has discriminant valuation 3 and the other (with $\pi \mid s$) has valuation 9.

Each solution to (7) falls into one of these cases, according to whether $B+C$ has even or odd valuation at $\mathfrak{p}$, unless $B+C=0$, corresponding to $a=0$, which we have treated separately. When seeking curves with conductor a power of the odd prime $\mathfrak{p}$ in subsequent subsections, we will also treat separately solutions to (7) where all of A, B and C are units at $\mathfrak{p}$, since in such cases we cannot recover $\mathfrak{p}$ from the solution. Such cases occur when an elliptic curve E has conductor $\mathfrak{p}^2$, so has additive reduction at $\mathfrak{p}$, but is a quadratic twist of a curve E_0 with good reduction at $\mathfrak{p}$. Here we must consider twists of E_0 by *all* odd primes to see which have good reduction above 2.

In the next three subsections we will determine all elliptic curves with odd prime power conductor $\mathfrak{p}^r$, treating first this "good twist" case where E has a twist with good reduction at $\mathfrak{p}$ (this includes the case $a = 0$), then the "additive twist" cases where all twists have additive reduction at $\mathfrak{p}$ (here $A = \pi$) and lastly the "multiplicative twist" case where E has a twist with multiplicative reduction at $\mathfrak{p}$ (here $A = 1$).

In each case we determine which (B, C) pairs give an appropriate solution to (7), thus obtaining a "base curve" $E_{a,b}$, and then determine which of its twists have good reduction at primes dividing 2. For the last part we will make essential use of the local criterion of Kraus from [Kra89, Théorème 2], which we state here for the reader's convenience.

Proposition 2.6 (Kraus)**.** *Let K be a finite extension of $\mathbb{Q}_2$ with valuation ring $\mathcal{O}_K$, normalized valuation v and ramification degree $e = v(2)$. Let c_4, c_6, Δ in $\mathcal{O}_K$ satisfy $c_4^3 - c_6^2 = 1728\Delta \neq 0$. Then there exists an integral Weierstrass model of an elliptic curve over K with invariants c_4 and c_6 if and only if one of the following holds:*

(1) $v(c_4) = 0$ and there exists $a_1 \in \mathcal{O}_K$ such that $a_1^2 \equiv -c_6 \pmod 4$.

(2) $0 < v(c_4) < 4e$ and there exist $a_1, a_3 \in \mathcal{O}_K$ such that

$$\begin{aligned} d = -a_1^6 + 3a_1^2c_4 + 2c_6 &\equiv 0 \pmod{16};\\ a_3^2 &\equiv d/16 \pmod 4;\\ 4a_1^2 d &\equiv (a_1^4 - c_4)^2 \pmod{256}. \end{aligned}$$

(3) $v(c_4) \geq 4e$ and there exists $a_3 \in \mathcal{O}_K$ such that $a_3^2 \equiv c_6/8 \pmod 4$.

2.3. **Curves with odd prime power conductor: the good twist case.** In this subsection we determine all elliptic curves defined over one of the fields K with K-rational 2-torsion and conductor a power of an odd prime $\mathfrak{p}$, such that a quadratic twist of E by a generator π of $\mathfrak{p}$ has good reduction at $\mathfrak{p}$. In fact all such curves have CM by an order in K and have been fully described in the previous section.

Theorem 2.7. *Let K be an imaginary quadratic field with class number 1, and let $\mathfrak{p}$ be an odd prime of K. Let E be an elliptic curve defined over K, with a K-rational point of order 2 of conductor a power of $\mathfrak{p}$. If E has a quadratic twist with good reduction at $\mathfrak{p}$ then E belongs to one of the following complex multiplication families as studied in Section 1:*

- *$K = \mathbb{Q}(\sqrt{-7})$ and E is a twist of the base-change to K of one of the curves in the isogeny class 49.a over $\mathbb{Q}$, with conductor $\mathfrak{p}^2 = (\pi)^2$ where $\pi \equiv 1 \pmod 4$; or*
- *$K = \mathbb{Q}(\sqrt{-1})$ and E is a twist of the base-change to K of one of the curves in the isogeny class 64.a over $\mathbb{Q}$. E has equation $y^2 = x(x^2 + b)$ and conductor $\mathfrak{p}^2 = (\pi)^2$, where $b \equiv -1 \pm 2i \pmod 8$ with $b = \pi$ or $b = \pi^3$; or*
- *$K = \mathbb{Q}(\sqrt{-2})$ and E is a twist of the base-change to K of one of the curves in the isogeny class 256.a over $\mathbb{Q}$, with conductor $\mathfrak{p}^2 = (\pi)^2$ where $\pi \equiv \pm 1 + \sqrt{-2} \pmod 4$, for $(a, b) = (2\pi\sqrt{-2}, -\pi^2)$.*

In each case, the elliptic curves have CM by an order in the field of definition K: their j-invariants are either -15^3 or 255^3 in the first case, either 12^3 or 66^3 in the second, and in the third they have $j = 20^3$ and CM by $\mathbb{Z}[\sqrt{-2}]$.

Remark 2.8. There are four curves in the isogeny class 49.a over $\mathbb{Q}$, linked by 2- and 7-isogenies and in two pairs of -7-twists, so that over $\mathbb{Q}(\sqrt{-7})$ they become isomorphic in pairs. The first two are 49.a1, which has parameters $(a, b) = (21, 112)$, and 49.a2, with $(a, b) = (-42, -7)$; the other two are their -7-twists and are 7-isogenous to these.

Proof. By Theorems 1.3 and 1.8 we know that the three families of curves do have good reduction away from $\mathfrak{p}$, hence we are led to prove that these are the unique ones.

In the notation of Table 2.1 such curves have discriminant valuation $k = 6$ so come from solutions with $\mathfrak{p}$-valuations given in the first two lines of the second half of the table. Hence B and C are not divisible by π, and from Table 2.2 they have valuation $6e_2$ or 0 at the prime(s) above 2 in the ordinary case, while in the supersingular case they are units. Up to scaling by units, and interchanging B and C (corresponding to applying a 2-isogeny), we reduce to considering the following finite number of possibilities for (B, C):

(1) over all fields, $(B, C) = (64\eta, 1)$ with $\eta \in \mathcal{O}_K^*$;
(2) over $\mathbb{Q}(\sqrt{-7})$ where $2 = \tau\overline{\tau}$ with $\tau = \frac{1+\sqrt{-7}}{2}$, $(B, C) = (\pm\tau^6, \overline{\tau}^6)$;
(3) over $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$, $(B, C) = (\pm 1, 1)$ (the supersingular case).

For a solution we require $B + C$ to be either 0 or a non-zero square times a unit.

Case (1) yields no solutions with $\eta = 1$ since $B+C = 65 = 5\cdot 13$ is not a square since neither 5 nor 13 ramifies in any of the fields. Taking $\eta = -1$ in (1) gives $B + C = -63 = 3^2 \cdot 7$, which is valid when 7 is ramified, and leads to the base curves $E = E_{a,b}$ with $(a, b) = (6\sqrt{-7}, 1)$ (and its Galois conjugate). Such curves lie in the first family.

A simple check shows that none of the additional units in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ gives a value of $B + C$ of the required form.

In case (2) we have $B + C = \pm\tau^6 \pm \overline{\tau}^6 \in \{\pm 9, \pm 5\sqrt{-7}\}$, giving a potential solution with $A = \pm 6$ and $b = \overline{\tau}^6$ (or its Galois conjugate). Taking $(a, b) = (6, \tau^6)$ we find a twist of 49.a1 and hence no curves not already encountered.

In case (3) with $B + C = 0$ we obtain curves with $a = 0$. All such curves have CM by $\mathbb{Z}[\sqrt{-1}]$, hence we get curves in the second family from Theorem 1.8.

In case (3) with $B+C = 2$ we obtain a solution when 2 is ramified, with base curve $E = E_{a,b}$ where $(a, b) = (2(1+i), i)$ or $(2\sqrt{-2}, -1)$. Both cases are isomorphic to the curve 256.a1 with CM by $\mathbb{Z}[\sqrt{-2}]$. Then we get the third family from Theorem 1.11 and Corollary 1.15. □

2.4. **Curves with odd prime power conductor: the additive twist case.** We continue to consider elliptic curves E whose conductor is a power of the odd prime $\mathfrak{p} = (\pi)$, using Theorem 2.3 to find all such curves by considering solutions to the parametrizing equation (7).

In this subsection, we consider the "additive twist" case in which the parameter A is divisible by π so that the curves and their twists by π and by units all have additive reduction at $\mathfrak{p}$. The discriminant valuations are 3 or 9. We find that the only such curves are again the base changes of CM elliptic curves over $\mathbb{Q}$ with conductor 49, but unlike the previous subsection, K must be one of the six fields in which 7 is inert. This corresponds to looking at elliptic curves with CM by an order in K over a field $L \neq K$, which furthermore have a 2-torsion point and odd prime power conductor. By the results of Section 1 (specifically Corollary 1.15), we have to restrict to odd values of d, and the unique curve with a 2-torsion point corresponds to $d = 7$.

Theorem 2.9. *Let K be an imaginary quadratic field with class number 1, and let $\mathfrak{p}$ be an odd prime of K. Let E be an elliptic curve defined over K, with a K-rational point of order 2 and conductor a power of $\mathfrak{p}$, such that no quadratic twist of E has good or multiplicative reduction at $\mathfrak{p}$. Then*

- *$K = \mathbb{Q}(\sqrt{-d})$ for $d = 1, 2, 11, 43, 67, 163$, E has conductor $\mathfrak{p}^2$ where $\mathfrak{p} = (7)$, and E is a base-change to K of one of the curves in the isogeny class 49.a over $\mathbb{Q}$.*

Proof. Inspecting Table 2.1, we are led to the same set of pairs (B, C) as considered in the proof of Theorem 2.7, except that now we require $B + C$ to be nonzero, with odd valuation at exactly one odd prime $\mathfrak{p}$. We use the same numbering of cases as before and recall that these are all possibilities, up to scaling by units and switching B and C.

Case (1), where $B + C \in \{\pm 63, \pm 65\}$ again yields no solutions with $B + C = 65 = 5 \cdot 13$ since neither 5 nor 13 ramifies in any of the fields. However, $B + C = -63 = 3^2 \cdot 7$ is valid when 7 is inert in K. This gives the base curve with $(a, b) = (-42, -7)$, which is the elliptic curve defined over $\mathbb{Q}$ with label 49.a2. Note that this curve also appeared in the good twist case over $\mathbb{Q}(\sqrt{-7})$, but here we require 7 to be inert. The quadratic twist by -7 (with label 49.a4) also has good reduction away from 7, so all four curves in the isogeny class 49.a have conductor $(7)^2$ over the fields listed.

A simple check shows that none of the additional units in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ gives a value of $B + C$ of the required form.

In case (2) we have $B + C = \pm\tau^6 \pm \overline{\tau}^6 \in \{\pm 9, \pm 5\sqrt{-7}\}$. Since 5 is inert this gives no solutions.

Case (3), with $B + C \in \{0, \pm 2\}$, also provides no solutions. □

2.5. **Curves with odd prime power conductor: the multiplicative twist case.** We now consider curves of odd prime power conductor $\mathfrak{p}^r$ which in our parametrization have $A = 1$, such that the base curve $E_{a,b}$ (with $\mathfrak{p}$-minimal (a, b)) has multiplicative reduction at $\mathfrak{p}$.

The main result of this subsection is that these elliptic curves are of two types, up to quadratic twist by a generator of $\mathfrak{p}$:

- one of a finite number of "sporadic" curves, with conductor either a prime dividing 17 (over all fields where 17 does not split), or a prime of norm 257 over $\mathbb{Q}(\sqrt{-1})$ only, or a prime of norm 241 over $\mathbb{Q}(\sqrt{-3})$ only;
- one of a family analogous to the Setzer-Neumann family over $\mathbb{Q}$.

The sporadic curves are all given by a more general construction which we discuss first. Over any number field K let $u \in K \setminus \{0, -16\}$ and define $E_u = E_{-(u+32)/4, u+16}$, an elliptic curve with invariants $c_4 = u^2 + 16u + 256$, $c_6 = (u - 16)(u + 8)(u + 32)$ and discriminant $\Delta_u = u^2(u + 16)^2$.

Lemma 2.10. *E_u has full 2-torsion over K; the three curves 2-isogenous to E are isomorphic to $E_{a,b}$ for $(a, b) = (2(u-16), u^2+32u+256)$, $(2(u+32), u^2)$ and $(u+8, 16)$, with discriminants $-u(u + 16)^4$, $u^4(u + 16)$, and $u(u + 16)$ respectively.*

Proof. Elementary: note that Δ_u is a square. □

In fact the family of curves E_u is the universal family of elliptic curves with full 2-torsion over K, as it is easy to check that E_u has Legendre parameter $\lambda = (u + 16)/u$. Our reason for writing the family this way is that if we specialize the parameter u to a unit with certain properties, then we obtain elliptic curves with square-free odd conductor.

Proposition 2.11. *Let K be any number field and $u \in \mathcal{O}_K^*$. The quadratic twist $E_u^{(-u)}$ of E_u by $-u$, together with its three 2-isogenous curves, is semistable with bad reduction only at primes dividing $u+16$. The same is true of E_u itself if $-u$ is congruent to a square modulo 4.*

Proof. From the invariants given above we see that Δ_u is only divisible by primes dividing $u + 16$ which is odd, and that Δ_u is coprime to c_4 so the reduction is multiplicative at all bad primes. Also since c_4 and c_6 are odd the condition that c_4 and c_6 are the invariants

of an integral model, which then has good reduction at primes dividing 2, is that $-c_6$ is a square modulo 4, which is the case when $-u$ is a square modulo 4 since $c_6 \equiv u^3 \pmod 4$. Twisting by $-u$ gives a curve whose $c_6 \equiv -u^6 \pmod 4$ which satisfies Kraus' condition unconditionally. □

For example, over $\mathbb{Q}$ we take $u = 1$ and find that $E_1^{(-1)}$ is the elliptic curve 17.a2 of conductor 17, with 2-isogenous curves 17.a1, 17.a3 and 17.a4. Since $17 \equiv 1 \pmod 4$, its quadratic twists by 17 also have good reduction at 2. Taking $u = -1$ gives curves of conductor 15, which are not relevant for us.

More generally we consider the curves given by this proposition over imaginary quadratic fields, for units u such that $u + 16$ is a prime power, so that we obtain curves of prime conductor. When ± 1 are the only units, the only case is the one just considered with $u = 1$, leading to curves whose conductors are divisible only by the primes above 17, which are primes except when 17 splits in K. Since $17 \equiv 1 \pmod 4$, the quadratic twists of such curves also have good reduction at 2.

Over $K = \mathbb{Q}(\sqrt{-1})$ we can also take $u = \pm\sqrt{-1}$ since $16 \pm \sqrt{-1}$ have prime norm 257. This gives 8 elliptic curves, 4 in one isogeny class 2.0.4.1-257.1-a with conductor $\mathfrak{p} = (16 + \sqrt{-1})$, linked by 2-isogenies, and their Galois conjugates in isogeny class 2.0.4.1-257.2-a. The quadratic twists by $1 \pm 16\sqrt{-1}$ have good reduction at 2 and give curves of conductor $\mathfrak{p}^2$ in isogeny classes 2.0.4.1-66049.1-a and 2.0.4.1-66049.3-a.

Over $K = \mathbb{Q}(\sqrt{-3})$ let ε be a 6th root of unity generating the unit group. Taking $u = \varepsilon^2$ or its Galois conjugate, we obtain elliptic curves with prime conductors $\mathfrak{p}$ of norm 241. Again there are two Galois conjugate isogeny classes 2.0.3.1-241.1-a and 2.0.3.1-241.3-a, each containing 4 elliptic curves linked by 2-isogenies. The quadratic twists by $16 \pm u$ have good reduction at 2, conductor $\mathfrak{p}^2$, in isogeny classes 2.0.3.1-58081.1-a and 2.0.3.1-58081.3-a.

The next result shows that, apart from these sporadic cases, all elliptic curves with odd prime conductor and rational 2-torsion come from an analogue of the Setzer-Neumann family over $\mathbb{Q}$.

Theorem 2.12. *Let K be an imaginary quadratic field with class number 1, and ε a generator of its unit group. Let E be an elliptic curve defined over K with conductor an odd prime power $\mathfrak{p}^r$ and a K-rational 2-torsion point. Assume that E has a quadratic twist with multiplicative reduction at $\mathfrak{p}$. Then E is either*

- *one of the sporadic curves listed above, where $\mathfrak{p}$ has norm 17 (over all fields), or 257 (over $K = \mathbb{Q}(\sqrt{-1})$ only) or 241 (over $K = \mathbb{Q}(\sqrt{-3})$ only); or*
- *isomorphic or 2-isogenous to $E_{a,b}$ where $b = 16\varepsilon$ and a satisfies an equation of the form*
$$a^2 = u\pi^r + 64\varepsilon,$$
with r odd, u a unit and $u\pi^r \equiv 1 \pmod{\frac{8}{e_2}}$; or
- *the quadratic twist by $u\pi$ of the previous case, without any congruence condition.*

Proof. We start with the observation that in each case ε is not congruent to a square modulo 4, which may be checked easily and which will be used repeatedly.

As before we use Theorem 2.3 to first find the curves with minimal parameters, arising from solutions to (7) with $A = s = 1$. Up to 2-isogeny, we may assume that $a = \tilde{a}$ is odd, that B is odd and C divisible by 64 with $C/64$ odd, except in the case $K = \mathbb{Q}(\sqrt{-7})$ where B and C are each divisible by the 6th power of one of the two primes dividing 2, or the supersingular case over $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. We will leave these last cases to the end.

Scaling by squares of units, we must solve each of the following equations:

$$a^2 = P + 64 \tag{8}$$
$$a^2 = 1 + 64P \tag{9}$$
$$a^2 = P + 64\varepsilon \tag{10}$$
$$a^2 = \varepsilon + 64P \tag{11}$$

where P is an odd prime power, i.e. an element of $\mathcal{O}_K$ with precisely one prime factor. We immediately see that (11) has no solution modulo 4.

(8) factors as $(a-8)(a+8) = P$. Without loss of generality (changing a for $-a$ if necessary) we have $P \mid (a-8)$; writing $a = 8+Pt$ leads to $t(16+Pt) = 1$, so t is a unit, and $16-t^{-1} = -Pt$. Setting $u = -t^{-1}$ leads to one of the sporadic cases (we have one of the curves 2-isogenous to $E_{-t^{-1}}$) and its quadratic twists.

(9) factors as $(a-1)(a+1) = 64P$. Now P divides one factor, and also one factor is divisible exactly by 2, the other by 32. By symmetry this gives two cases to consider: if $a = 1 + 32Pt$ with t odd then $t(1+16Pt) = 1$ so t is a unit and $16Pt = t^{-1} - 1$ which is impossible. Otherwise $a = 1 + 2Pt$ with t odd, and $t(1+Pt) = 16$ so again t is a unit and we have a sporadic case (a twist of E_{-t}).

In (10) we divide according to whether the valuation r of P is even or odd. If even then we must have $P = Q^2$ with Q a prime power, since $P = \varepsilon Q^2$ gives a contradiction modulo 4. Now $(a-Q)(a+Q) = 64\varepsilon$; by symmetry $a = Q + 32t$ with t odd, so $t(Q+16t) = \varepsilon$, leading to the third sporadic case (a twist of $E_{-\varepsilon t^2}$).

Otherwise in (10) we have $P = u\pi^r$ with u a unit and r odd, leading to the Setzer-Neumann family. Recall that c_4 is odd and $2c_6 = a(9b-2a^2)$, hence Proposition 2.6 implies that $a \equiv \square \pmod 4$ so $a^2 \equiv 1 \pmod 8$ if 2 is unramified in K and $a^2 \equiv 1 \pmod 4$ otherwise. In any case, the same criterion implies that the quadratic twist by $u\pi$ has good reduction at 2.

Over $K = \mathbb{Q}(\sqrt{-7})$ we must also consider the equation

$$a^2 = \pm T + UP \tag{12}$$

(up to Galois conjugation and 2-isogeny) where $T = \alpha^6$ with $\alpha = (1+\sqrt{-7})/2$ and $U = \overline{T}$ so that $TU = 64$; here P again denotes a prime power. The minus sign is impossible modulo $\overline{\alpha}^2$, and with the plus sign we can factor as $(a-\alpha^3)(a+\alpha^3) = UP$. Arguing as in earlier cases one finds that this equation has no solutions.

Lastly we consider curves which are supersingular at $\mathfrak{q} \mid 2$, which by Theorem 2.3 and Corollary 2.2 arise from solutions to the following equations:

$$\tilde{a}^2 = P + 1 \tag{13}$$
$$\tilde{a}^2 = P + \epsilon \tag{14}$$

with $a = 2\tilde{a}$.

(13) factors as $(\tilde{a}-1)(\tilde{a}+1)$, and one of the factors is a unit. This gives solutions $P = 3$ and $P = -1 \pm 2i$ over $\mathbb{Q}(i)$ but the associated curves with $(a,b) = (4,1)$ and $(2 \pm 2i, 1)$ have bad reduction at $1+i$ as do all their quadratic twists.

In (14) the base curve has $(a,b) = (2\tilde{a}, \varepsilon)$ with $(c_4, c_6) = (2^4(4P+\varepsilon), 2^6\tilde{a}(-8P+\varepsilon))$. We scale by $\tau = 1+i$ (respectively $\sqrt{-2}$) to get $(c_4, c_6) = (\tau^4(4P+i), \tau^6\tilde{a}(8P-i))$ over $\mathbb{Q}(i)$ or $(c_4, c_6) = (\tau^4(4P-1), \tau^6\tilde{a}(-8P-1))$ over $\mathbb{Q}(\sqrt{-2})$ respectively. We must test whether these, or their twists by $s \in \{1, \varepsilon, \pi, \varepsilon\pi\}$ have good reduction at τ. Note that $v_{\mathfrak{q}}(c_4) = 4$ and

$v_{\mathfrak{q}}(c_6) \geq 7$, and that we are in the second case of Proposition 2.6, with $a_1 = \tau$ (since we are in the supersingular case).

Over $\mathbb{Q}(i)$ the first congruence in Proposition 2.6 reduces to $1 + is^2 \equiv 0 \pmod 2$ which is impossible.

Over $\mathbb{Q}(\sqrt{-2})$, in the notation of Proposition 2.6 the first condition on d is always satisfied (since s is odd), while the second is that either $(1 - s^2)/2$ or $(1 - s^2)/2 + 2\tau$ is a square modulo 4, depending on whether $v_{\mathfrak{q}}(\tilde{a}) \geq 2$ or $v_{\mathfrak{q}}(\tilde{a}) = 1$. At least one of these is satisfied provided that $s \equiv \pm 1 \pmod{\tau^3}$, and in either case $d/16 \equiv 0 \pmod 4$. But now the final condition implies $s^2 \equiv -1 \pmod 4$, contradiction. □

The above classification implies the following crucial fact, which will be used in the final section of the paper, and which was an important motivation for this section.

Corollary 2.13. *Every isogeny class of elliptic curves defined over K with prime conductor and a K-rational 2-torsion point contains a curve whose discriminant has odd valuation.*

Proof. If E is a curve over K of prime conductor $\mathfrak{p}$ and a K-rational 2-torsion point, we are in the multiplicative case. By Theorem 2.12 E is either a sporadic curve of conductor norm 17, 241 over $\mathbb{Q}(\sqrt{-1})$ or 257 over $\mathbb{Q}(\sqrt{-3})$ (all of these have a curve with prime discriminant in their isogeny class) or is isogenous to $E_{a,b}$ with $b = 16\varepsilon$ and $a^2 = u\pi^r + 64\varepsilon$ with r odd. Such curves have discriminant $2^8 u\varepsilon^2\pi^r$, so odd valuation. □

Remark 2.14. All the computations done in this section could be generalized to other number fields of class number one, as the number of units modulo squares is always finite. The case of real quadratic fields is of particular interest, requiring almost no modification except to allow for $\mathcal{O}_K^*/(\mathcal{O}_K^*)^2$ having order 4. In this case, Proposition 2.11 gives an infinite family of elliptic curves of prime power conductor. For example, over $\mathbb{Q}(\sqrt{5})$, we get curves of prime conductor with norms $1009, 35569, 1659169, \ldots$.

We end this section with an interesting phenomenon concerning curves of prime conductor and rational 2-torsion.

Theorem 2.15. *Let K be an imaginary quadratic field with class number 1, and E/K be an elliptic curve of prime power conductor with a K-rational 2-torsion point. Then E has rank 0.*

Proof. A simple 2-descent computation shows that this is the case for curves in the Setzer-Neumann family (this phenomenon also occurs for rational elliptic curves, and the proof is the same). The remaining sporadic cases can be handled by looking at tables [LMF13] or computing the rank of the curve 27.a1 over the different fields K directly, for example using SageMath [S$^+$17]. □

3. Curves with a torsion point of odd order

Recall the following result of [KM88] and [Kam92]:

Theorem 3.1. *Let K be a quadratic field, and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

- $\mathbb{Z}/N$, *with* $1 \leq N \leq 18$ *but* $N \neq 17$.
- $\mathbb{Z}/2N \times \mathbb{Z}/2$ *with* $1 \leq N \leq 6$.
- $\mathbb{Z}/4 \times \mathbb{Z}/4$.

Label	Weierstrass Coefficients	ℓ	$\mathcal{D}(E)$	Field
19.a2	$[0,1,1,-9,-15]$	3	-19^3	$1,7,11,19,43,163$
19.a3	$[0,1,1,1,0]$	3	-19	$1,7,11,19,43,163$
27.a2	$[0,0,1,-30,63]$	3	-3^5	$1,7,19,43,67,163$
27.a4	$[0,0,1,0,0]$	3	-3^3	$1,7,19,43,67,163$
37.b2	$[0,1,1,-23,-50]$	3	37^3	$2,19,43,163$
37.b3	$[0,1,1,-3,1]$	3	37	$2,19,43,163$
2.0.4.1-757.1-a1	$[1+i,-1+i,1,-15+5i,-17+6i]$	3	$(-26+9i)^3$	1
2.0.4.1-757.1-a2	$[1+i,1+i,1,2i,i]$	3	$-26+9i$	1
2.0.8.1-9.1-CMa1	$[\sqrt{-2},1-\sqrt{-2},1,-1,0]$	3	$(-1-\sqrt{-2})^6$	2
2.0.11.1-9.3-CMa1	$[0,\frac{1-\sqrt{-11}}{2},1,\frac{-5-\sqrt{-11}}{2},-2]$	3	$(\frac{-1+\sqrt{-11}}{2})^6$	11
11.a2	$[0,-1,1,-10,-20]$	5	-11^5	$1,3,11,67,163$
11.a3	$[0,-1,1,0,0]$	5	-11	$1,3,11,67,163$
2.0.4.1-25.3-CMa1	$[1+i,i,i,0,0]$	5	$(2i+1)^3$	1
2.0.3.1-49.3-CMa1	$[0,\frac{-3+\sqrt{-3}}{2},\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},0]$	7	$(\frac{-1-3\sqrt{-3}}{2})^2$	3

TABLE 3.1. Prime power conductor curves with an ℓ-torsion point

- $\mathbb{Z}/3\times\mathbb{Z}/3N$ *with* $N=1,2$.

In particular the primes dividing the order of the torsion subgroup are $2,3,5,7,11$ and 13. Let $\mathfrak{q}\mid 2$ be a prime and E be an elliptic curve of odd conductor. By Hasse's bound

$$\#E(\mathbb{F}_{\mathfrak{q}})=|\mathcal{N}\mathfrak{q}+1-a_E(\mathfrak{q})|\leq \mathcal{N}\mathfrak{q}+1+2\sqrt{\mathcal{N}\mathfrak{q}}<11.$$

In particular a curve of odd prime power conductor over K can only have a torsion point of odd prime order ℓ for $\ell\in\{3,5,7\}$.

While studying the possible torsion of an elliptic curve over K, the case $\ell=3$ and $K=\mathbb{Q}(\sqrt{-3})$ is quite different from the others. The reason is that since K contains the sixth roots of unity, the determinant of the Galois representation acting on 3-torsion points is trivial. The main results of the present section are Theorem 3.3, where a similar statement to that of Corollary 2.13 is proven for curves over $\mathbb{Q}(\sqrt{-3})$ with a rational 3-torsion point, and a complete list of elliptic curves of prime power conductor with a point of order $\ell\in\{3,5,7\}$ is given in all other cases. The complete list (omitting Galois conjugates) is given in Table 3.1, whose completeness will be proved in this section, in Theorems 3.5 3.7 3.8.

Remark 3.2. Besides curves over $\mathbb{Q}(\sqrt{-3})$ with a rational 3-torsion point, the only curves of prime conductor over imaginary quadratic fields with a rational ℓ-torsion point are those over $\mathbb{Q}(\sqrt{-1})$ with a 3-torsion point.

Let p be an odd prime, $K/\mathbb{Q}$ be a quadratic extension and E/K be an elliptic curve with a global minimal model. If $P\in E(K)$ has order p, then by [Sil09, Theorem 3.4] P has algebraic integer coordinates in the minimal model, except when $p=3$ and $K/\mathbb{Q}$ is ramified at 3 where, if $\mathfrak{p}_3$ denotes the prime dividing 3, the case $v_{\mathfrak{p}_3}(x(P),y(P))=(-2,-3)$ might occur.

Theorem 3.3. *Let $K=\mathbb{Q}(\sqrt{-3})$, and let E/K be a curve with a point of order* 3 *and prime power conductor $\mathfrak{p}^r$ and let $\tilde{E}$ be its* 3*-isogenous curve. Then the valuations at $\mathfrak{p}$ of $\mathcal{D}(E)$ and $\mathcal{D}(\tilde{E})$ are not both divisible by* 3*, unless E is one of the CM curves* 2.0.3.1-81.1-CMa1*,* 2.0.3.1-729.1-CMa1 *or* 2.0.3.1-729.1-CMb1*.*

Proof. Suppose that $(\mathcal{D}(E)) = \mathfrak{p}^{3r}$. Let P denote the point of order 3 in $E(K)$. If P has integral coordinates, we use the parametrization of elliptic curves with a rational point of order 3 given by Kubert in [Kub76, Table 1]: such curves have a minimal model of the form

$$E : y^2 + a_1xy + a_3y = x^3, \tag{15}$$

where a_i are algebraic integers, $P = (0, 0)$ has order 3, with discriminant

$$\mathcal{D}(E) = a_3^3(a_1^3 - 27a_3). \tag{16}$$

If P does not have integral coordinates, when we take the minimal equation to one of the form (15), $v_\mathfrak{p}(a_1) \geq 0$ and $v_\mathfrak{p}(a_3) = -3$.

Note that over a field with the 3-rd roots of unity the cyclotomic character modulo 3 is trivial so the representation of the Galois group acting on $E[3]$ has image in $\mathrm{SL}(2, 3)$. Then if it is reducible, with upper triangular matrices, the diagonal entries are both $+1$ or both -1. So if the curve E has a rational point of order 3, so does the isogenous curve $\tilde{E}$. We find that $\tilde{E}$ has equation $y^2 + a_1xy + a_3y = x^3 - 5a_1a_3x - a_1^3a_3 - 7a_3^2$, and discriminant

$$\mathcal{D}(\tilde{E}) = a_3(a_1^3 - 27a_3)^3. \tag{17}$$

Suppose that both $\mathcal{D}(E)$ and $\mathcal{D}(\tilde{E})$ generate ideals which are cubes. Then

$$a_1^3 - 27a_3 = u\alpha^3$$
$$a_3 = v\beta^3,$$

for u, v units and $\alpha, \beta \in K^\times$; in fact, $\alpha, \sqrt{-3}\beta \in \mathcal{O}_K$. In particular, $(a_1 : -\alpha : -3\beta)$ is a K-rational point on the cubic curve

$$x^3 + uy^3 + vz^3 = 0, \tag{18}$$

a twist of the Fermat cubic. By Lemma 3.4 below, all K-rational points $(x : y : z)$ on all curves of the form (18) either satisfy $xyz = 0$, or (after scaling so that $x, y, z \in \mathcal{O}_K$ are coprime) that x, y, z are all units.

Since $\alpha\beta \neq 0$ the first case is possible only when $a_1 = 0$. Then a_3 is a unit times a cube, so by minimality is a unit: this leads to the three isomorphism classes of curves with conductor (9) or (27) as stated.

In case none of the coordinates is zero, we consider separately the finite cases where β is integral or has valuation -1, and find that there are no more solutions. □

Lemma 3.4. *Let $K = \mathbb{Q}(\sqrt{-3})$ and $u, v \in \mathcal{O}_K^*$. The cubic curve (18) has either 3 or 9 rational points, which either lie on one of the lines $x = 0$, $y = 0$ or $z = 0$, or have projective coordinates which are all units.*

Proof. After permuting the coordinates, scaling by units and absorbing cubes, there are only three essentially different equations, those with $(u, v) = (1, 1)$, $(1, \zeta)$, and (ζ, ζ^2) where $\zeta \in K$ is a 6th root of unity. When $u = 1$, it is well-known that all points have one zero coordinate (see [IR82, Proposition 17.8.1]). There are 9 such points (all the flexes) when $v = 1$, and 3 when $u = \zeta$. The curve with $(u, v) = (\zeta, \zeta^2)$ is isomorphic to the one with $(u, v) = (1, 1)$, since the isomorphism class depends only on uv modulo cubes, and hence also has 9 points; these are $(\zeta^{2k} : \zeta^{2l+1} : 1)$ for $k, l \in \{0, 1, 2\}$. □

Theorem 3.5. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field of class number 1, $K \neq \mathbb{Q}(\sqrt{-3})$ and E/K an elliptic curve of odd prime power conductor with a point of order 3. Then E is isomorphic to one of the following:*

- *the curve* 19.a2 *or* 19.a3 *over* $\mathbb{Q}(\sqrt{-d})$ *for* $d = 1, 7, 11, 19, 43, 163$*;*
- *the curve* 27.a2 *or* 27.a3 *or* 27.a4 *over* $\mathbb{Q}(\sqrt{-d})$ *for* $d = 1, 7, 11, 19, 43, 67, 163$*;*
- *the curve* 37.b2 *or* 37.b3 *over* $\mathbb{Q}(\sqrt{-d})$ *for* $d = 2, 19, 43, 163$*;*
- $K = \mathbb{Q}(\sqrt{-1})$ *and* E *is one of the* 3*-isogenous curves*

$$y^2 + (1+i)xy + iy = x^3 + (-1+i)x^2 + (-14-8i)x + (-10-20i), \qquad \text{with label } 2.0.4.1\text{-}757.1\text{-a1},$$
$$y^2 + (1+i)xy + iy = x^3 + (1+i)x^2 + (1-i)x + 2, \qquad \text{with label } 2.0.4.1\text{-}757.1\text{-a2},$$

or their Galois conjugates with labels 2.0.4.1-757.2-a1 *and* 2.0.4.1-757.2-a2.

- $K = \mathbb{Q}(\sqrt{-2})$ *and* E *is the curve*

$$y^2 + \sqrt{-2}xy + y = x^3 + (1-\sqrt{-2})x^2 - x, \qquad \text{with label } 2.0.8.1\text{-}9.1\text{-CMa1},$$

or its Galois conjugate with label 2.0.8.1-9.3-CMa1*;*

- $K = \mathbb{Q}(\sqrt{-11})$ *and* E *is the curve*

$$y^2 + y = x^3 + \frac{1-\sqrt{-11}}{2}x^2 + \frac{-5-\sqrt{-11}}{2}x - 2, \qquad \text{with label } 2.0.11.1\text{-}9.3\text{-CMa1},$$

or its Galois conjugate with label 2.0.11.1-9.1-CMa1*.*

Proof. As in Theorem 3.3, we use the parametrization of elliptic curves with a rational point of order 3 given by Kubert in [Kub76, Table 1]: such curves have a model of the form

$$E : y^2 + a_1xy + a_3y = x^3, \tag{19}$$

where $P = (0,0)$ has order 3, with discriminant

$$\mathcal{D}(E) = a_3^3(a_1^3 - 27a_3). \tag{20}$$

By scaling, we can choose a model of this form such that for all primes $\mathfrak{q}$ either $\mathfrak{q} \nmid a_1$ or $\mathfrak{q}^3 \nmid a_3$. Then the model is minimal at all primes, as we now show. To be non-minimal at a prime $\mathfrak{q}$ implies that $\mathfrak{q}^6 \mid c_6$ and $\mathfrak{q}^{12} \mid \mathcal{D}(E)$, where c_6 is the usual invariant of the model. The ideal generated by c_6 and $\mathcal{D}(E)$ in the ring $\mathbb{Z}[a_1, a_3]$ contains both a_1^{15} and $3^3a_3^5$, so $\mathfrak{q} \mid a_1$ and $\mathfrak{q} \mid a_3$: in case $\mathfrak{q} \mid 3$, we need the fact that 3 is not ramified in K. By minimality, $v_{\mathfrak{q}}(a_3) \in \{1, 2\}$; this implies $v_{\mathfrak{q}}(\mathcal{D}(E)) \leq 11$, contradiction.

Let $\mathfrak{p} = (\pi)$ be the unique prime dividing $\mathcal{D}(E)$. As above, we can assume that either $\mathfrak{p} \nmid a_1$ or $\mathfrak{p}^3 \nmid a_3$. We can also scale by units, replacing (a_1, a_3) by (ua_1, u^3a_3), and we note that for the fields under consideration every unit is a cube. Our strategy is to prove that (a_1, a_3) lies in a small finite set, and then systematically search through all possible values.

- If a_3 is a unit, we may assume by scaling that $a_3 = 1$. Then we can factor (20) as

$$\mathcal{D}(E) = a_1^3 - 27 = (a_1 - 3)(a_1^2 + 3a_1 + 9).$$

We consider the following cases:

(1) If $\mathfrak{p} \nmid 3$ then the factors are coprime, so one is a unit. If $u = a_1 - 3 \in \mathcal{O}_K^*$ we get four solutions $(a_1, a_3) = (4, 1)$, $(2, 1)$, $(3 \pm \sqrt{-1}, 1)$ which give the curves 37.b3, 19.a3, 2.0.4.1-757.1-a2 and 2.0.4.1-757.2-a2. If $a_1^2 + 3a_1 + 9 = u \in \mathcal{O}_K^*$ then $(2a_1 + 3)^2 = 4u - 27 \in \{-23, -31, -27 \pm 4\sqrt{-1}\}$ which has no solution in K.

(2) If $\mathfrak{p} \mid 3$ then $\mathfrak{p} \mid a_1$. If $v_{\mathfrak{p}}(a_1) = 1$, we write $a_1 = \pi b$. In the inert case, $\pi = 3$ and $\mathcal{D}(E) = 27(b^3 - 1) = 27(b - 1)(b^2 + b + 1)$. If either factor is a unit one finds no solutions, otherwise both are divisible by 3, so write $b = 1 + 3c$; now the second factor is $3(1 + 3c + 3c^2)$ so $1 + 3c + 3c^2$ is a unit. Only $u = 1$ gives a solution: $c = -1$, $b = -2$ and $a_1 = -6$. The pair $(a_1, a_3) = (-6, 1)$ yields the curve 27.a4.

In the split case we get $\mathcal{D}(E) = \pi^3(b^3-\overline{\pi}^3) = \pi^3(b-\overline{\pi})(b^2+b\overline{\pi}+\overline{\pi}^2)$. Elementary computations reveal two solutions: $b = \sqrt{-2}$ giving $(a_1, a_3) = (\sqrt{-2}-2, 1)$ and the curve 2.0.8.1-9.1-CMa1; and $b = -2$ giving $(a_1, a_3) = (-1-\sqrt{-11}, 1)$ and the curve 2.0.11.1-9.1-CMa1; together with their Galois conjugates.
If $v_{\mathfrak{p}}(a_1) \geq 2$ then $v_{\mathfrak{p}}(\mathcal{D}(E)) = 3$. This gives the equation $a_1^3 = 27+\pi^3 u$ with u a unit. When 3 is inert we have $\pi = 3$ and $(a_1/3)^3 = 1+u \in \{2, 0, 1\pm\sqrt{-1}\}$, giving just one solution $(a_1, a_3) = (0, 1)$ and the curve 27.a4. When $3 = \pi\overline{\pi}$ we have $(a_1/\pi)^3 = \overline{\pi}^3 \pm 1$ but this is not a cube. (Here, $\pi = 1\pm\sqrt{-2}$ or $\pi = (1\pm\sqrt{-11})/2$.)

- Now suppose that a_3 is not a unit.
  (1) If $\mathfrak{p} \mid a_1$, the minimality of the model implies that $v_{\mathfrak{p}}(a_3) < 3$; scaling by units we can assume that $a_3 = \pi^j$ with $j \in \{1, 2\}$.
  If $\mathfrak{p} \nmid 3$ then $v_{\mathfrak{p}}(a_1^3 - 27a_3) = v_{\mathfrak{p}}(a_3) = j$ so $a_1^3 = \pi^j(27+v)$ for some unit v, but none of these expressions is a cube. Hence $\mathfrak{p} \mid 3$.
  If $v_{\mathfrak{p}}(a_1) = 1$, we have $v_{\mathfrak{p}}(a_1^3 - 27a_3) = 3$ so $a_1^3 = 27a_3 + \pi^3 u$ with u a unit. In the inert cases $(a_1/3)^3 = a_3 + u$, whose only solution is $(a_1, a_3) = (6, 9)$ which yields the curve 27.a3. In the split cases we find no solutions.
  If $v_{\mathfrak{p}}(a_1) \geq 2$, we have $v_{\mathfrak{p}}(a_1^3 - 27a_3) = v_{\mathfrak{p}}(27a_3) = 3 + j$ so $a_1^3 = 27a_3 + \pi^{3+j}u = \pi^j(27 + \pi^3 u)$ with u a unit. This has no solutions.
  (2) If $\mathfrak{p} \nmid a_1$, then $a_1^3 - 27a_3$ is a unit and we can scale so the unit is 1, so $a_1^3 = 1+27a_3$.
  If $\mathfrak{p} \mid 3$ then from $27a_3 = a_1^3 - 1 \equiv (a_1-1)^3 \pmod 3$ we have $\mathfrak{p} \mid a_1 = 1$ and either $a_1 - 1$ or $a_1^2 + a_1 + 1$ has valuation 1, but no solutions arise.
  Hence $\mathfrak{p} \nmid 3$. Now $27a_3 = a_1^3 - 1 = (a_1-1)(a_1^2+a_1+1)$, where the gcd of the factors divides 3. One of the factors is coprime to $\mathfrak{p}$, so divides 27, and both factors are divisible by the prime or primes dividing 3, so $3 \mid (a_1 - 1)$. Suppose that we are in the case that $a_1 - 1 \mid 27$. In case 3 is inert, write $a_1 - 1 = 3^k u$ with u a unit and $k \in \{1, 2, 3\}$. The only cases where $a_1^3 \equiv 1 \pmod{27}$ are $(a_1, a_3) = (10, 37)$ and $(-8, -19)$, giving the curves 37.b2 and 19.a2 respectively. In case 3 splits as $3 = \omega\overline{\omega}$ we have $a_1 = 1 \pm \omega^k\overline{\omega}^l$ with $k, l \in \{1, 2, 3\}$; the only solutions are those with have $k = l = 2$ which have already been seen. Secondly, if $a_1^2 + a_1 + 1 = d \mid 27$ then the quadratic in a_1 has discriminant $4d - 3$ which must be a square; enumeration of cases shows no solutions.

In summary we find that the only solutions (a_1, a_3), up to scaling by units and Galois conjugates, are $(a_1, 1)$ for $a_1 \in \{0, 2, 4, -6, 3+\sqrt{-1}, -2+\sqrt{-2}, -1-\sqrt{-11}\}$, and $(6, 9), (10, 37), (-8, -19)$.

□

Remark 3.6. It is an interesting question to determine whether there are infinitely many curves over $\mathbb{Q}(\sqrt{-3})$ with a point of order 3 and prime conductor. Based on numerical evidence, it seems quite plausible that this is indeed the case, but we did not focus on this particular problem.

Theorem 3.7. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field of class number 1 and E/K an elliptic curve of odd prime power conductor with a point of order 5. Then either E is isomorphic to the curve* 11.a2 *or* 11.a3 *for $d = 1, 3, 11, 67, 163$ or $K = \mathbb{Q}(\sqrt{-1})$ and E is the curve:*

$$y^2 + (i+1)xy + iy = x^3 + ix^2, \qquad \textit{with label } 2.0.4.1\text{-}25.3\text{-CMa1}, \tag{21}$$

or its Galois conjugate with label 2.0.4.1-25.1-CMa1.

Note that the curve 2.0.4.1-25.3-CMa1 has CM by $\mathbb{Z}[i]$; in particular, the conductor exponent is 2.

Proof. Again we use Kubert's parametrization from [Kub76, Table 1]: such curves have a model of the form

$$y^2 + (1-d)xy - dy = x^3 - dx^2,$$

with $d \in K$. An integral model is then given by

$$E_{a,b} : y^2 + (b-a)xy - ab^2y = x^3 - abx^2, \qquad \text{with } \gcd(a,b) = 1.$$

This model has discriminant $\mathcal{D}(E_{a,b}) = a^5b^5(a^2 - 11ab - b^2)$, and c_4-invariant $a^4 - 12a^3b + 14a^2b^2 + 12ab^3 + b^4$. In the polynomial ring $\mathbb{Z}[a,b]$ the ideal these generate contains $5a^{15}$ and $5b^{15}$, so they are coprime away from 5. Hence at all primes except possibly those dividing 5 the model $E_{a,b}$ is minimal, and has multiplicative reduction.

Let $\mathfrak{p}$ be a prime above 5 and suppose that $\mathfrak{p}$ divides both $\mathcal{D}(E_{a,b})$ and $c_4(E_{a,b})$. Then $\mathcal{D}(E_{a,b}) \equiv a^5b^5(a+2b)^2 \pmod{\mathfrak{p}}$ and $c_4(E_{a,b}) \equiv (a+2b)^4 \pmod{\mathfrak{p}}$, so $\mathfrak{p} \mid (a+2b)$. Writing $a = -2b + c$ where $\mathfrak{p} \mid c$ and using the fact that 5 is not ramified in K, we find that $c_4 \equiv -5b^4 \pmod{\mathfrak{p}^2}$, so $\mathfrak{p}^2 \nmid c_4$. Hence $E_{a,b}$ is also minimal at $\mathfrak{p}$. Examples show that the reduction at such a prime may be either good or additive.

In the factorization $\mathcal{D}(E_{a,b}) = a^5b^5(a^2 - 11ab - b^2)$, the three factors are pairwise coprime. Then for $\mathcal{D}(E_{a,b})$ to be a prime power two of a, b and $a^2 - 11ab - b^2$ are units. Since we may scale a and b simultaneously by a unit we may assume that either $a = 1$ or $b = 1$. When $a = 1$, $b = \pm 1$ leads to discriminant -11 while $a^2 - 11ab - b^2 = \pm 1$ leads to discriminant -11^5, giving the curves 11.a2 or 11.a3 over any field in which 11 is not split. Over $\mathbb{Q}(\sqrt{-1})$, additionally, $(a,b) = (1, \pm\sqrt{-1})$ gives the curves with conductor $(2 \pm \sqrt{-1})^2$ as stated, while over $\mathbb{Q}(\sqrt{-3})$ none of the additional units gives a solution. Lastly if a is not a unit we may assume that $b = 1$ and require $u = a^2 - 11a - 1 \in \mathcal{O}_K^*$ so that $125 + 4u$ is a square in K; the only possibility is $u = -1$ and $a = 11$ giving discriminant -11^5 again. □

Theorem 3.8. *Let K be an imaginary quadratic field of class number 1 and E/K be an elliptic curve of odd prime power conductor with a point of order 7. Then $K = \mathbb{Q}(\sqrt{-3})$ and E is isomorphic to*

$$y^2 + ay = x^3 + (a-2)x^2 + (1-a)x \qquad \textit{with label } \text{2.0.3.1-49.3-CMa1}, \tag{22}$$

where $a = \frac{1+\sqrt{-3}}{2}$.

Proof. In this case, a general elliptic curve with a 7-torsion point is given by

$$E_{a,b} : y^2 + (b^2 + ab - a^2)xy - (a^3b^3 - a^2b^4)y = x^3 - (a^3b - a^2b^2)x^2,$$

where $a, b \in \mathcal{O}_K$ and $\gcd(a,b) = 1$ (see [Kub76]). Its discriminant is given by $\mathcal{D}(E_{a,b}) = a^7b^7(a-b)^7(a^3 - 8a^2b + 5ab^2 + b^3)$. As in the previous theorem we can show that $\gcd(\mathcal{D}(E_{a,b}), c_4(E_{a,b}))$ is not divisible by any prime except for those dividing 7, and that the model $E_{a,b}$ is minimal even at such primes.

Since $(a,b) = 1$ two of a, b and $c = (a-b)^7(a^3 - 8a^2b + 5ab^2 + b^3)$ are units. If a is a unit but not b then we can scale so $a = 1$ and now $1 - b$ is a unit. None of the possibilities gives an odd prime power discriminant. Similarly if $b = 1$ and a is not a unit. Lastly if $a = 1$ and b is a unit, the only possibility which works is when b is a 6th root of unity, giving the curve as stated in the theorem (which is isomorphic to its Galois conjugate while not being a base-change from $\mathbb{Q}$). □

Remark 3.9. Note that in all the exceptional cases, the discriminant exponent is at most 5, except for the curve 11.a2 over $\mathbb{Q}(\sqrt{-11})$, where it is 10 (as 11 ramifies in the extension).

4. Bianchi modular forms and modularity of elliptic curves

In this section we summarize the facts and conjectures on Bianchi modular forms which we will need for our main result, which will take up the final section.

For background on Bianchi modular forms and modularity of elliptic curves defined over imaginary quadratic fields, we refer to the survey article of Şengün [cS14] and the work of the second author ([Cre84], [Cre92], [CW94]). For our purposes we may restrict our attention to the space $S_2(\mathfrak{n})$ of Bianchi modular forms which are cuspidal and of weight 2 for the congruence subgroup $\Gamma_0(\mathfrak{n}) \leq \mathrm{GL}_2(\mathcal{O}_K)$, where the level $\mathfrak{n} \subseteq \mathcal{O}_K$ is an integral ideal of K. This space is a finite-dimensional vector space equipped with a Hecke action, spanned by eigenforms which are simultaneous eigenvectors for the algebra of Hecke operators. Bianchi modular forms can also be seen within the context of cohomological automorphic forms, since we have the isomorphism $S_2(\mathfrak{n}) \cong H^1(Y_0(\mathfrak{n}), \mathbb{C})$, where $Y_0(\mathfrak{n})$ is the quotient of hyperbolic 3-space $\mathcal{H}_3$ by $\Gamma_0(\mathfrak{n})$. A more concrete description of these Bianchi modular forms is as real analytic functions $\mathcal{H}_3 \to \mathbb{C}^3$ satisfying certain conditions. In the work of the second author and his students ([Cre84], [CW94]) explicit methods were developed to compute the spaces $S_2(\mathfrak{n})$ over K for each of the nine imaginary quadratic fields K of class number 1. Such computations establish the following result:

Theorem 4.1. *For each of the nine imaginary quadratic fields of class number* 1*, the space* $S_2(1)$ *of weight* 2 *cuspidal Bianchi modular forms of level* 1 *is trivial.*

It is known that these Bianchi modular forms have associated ℓ-adic Galois representations $\rho_{F,\ell}$. These were first constructed by Taylor *et al.* in [HST93], [Tay94] with subsequent results by Berger and Harcos in [BH07]. Below we only need to refer to the residual mod-ℓ representations $\overline{\rho_{F,\ell}}$.

For an elliptic curve E defined over an imaginary quadratic fields K, we say that E is modular if $L(E, s) = L(F, s)$ for some $F \in S_2(\mathfrak{n})$ over K, where $\mathfrak{n}$ is the conductor of E. The following conjecture, a version of which was first made by Mennicke, is part of Conjecture 9.1 of [cS14], following [Cre92]:

Conjecture 1. *Let E be an elliptic curve defined over an imaginary quadratic field K of class number* 1*, which does not have complex multiplication by an order in K. Then E is modular.*

Some cases of the conjecture have been proved (see [DGP10]). Finally, following the classical result of Ribet ([Rib91]), we make the following conjecture.

Conjecture 2. *Let F be a weight* 2 *Bianchi newform of level $\Gamma_0(\mathfrak{np})$, with $\mathfrak{p}$ a prime number. Suppose that ℓ is a prime for which the representation $\rho_{F,\ell}$ satisfies:*

- *The residual representation is absolutely irreducible.*
- *The residual representation is unramified at $\mathfrak{p}$.*

Then there is an automorphic form $G \in H^1(Y_0(\mathfrak{n}), \mathbb{Z})$ whose Galois representations is isomorphic to $\overline{\rho_{F,\ell}}$.

Some results in the direction of the conjecture are proven in [CV12]. What happens in general is that the homology (and the cohomology) of $Y_0(\mathfrak{n})$ has a lot of torsion, and the form

G comes from the torsion part. Still, thanks to [Sch15], we know that we can attach residual Galois representations to such automorphic forms. In particular, if this is the case, the Galois representation will not lift to characteristic zero.

5. Modular elliptic curves of prime power conductor

Recall the following result due to Serre and Mestre-Oesterlé (see [MO89]).

Theorem 5.1. *Let $E/\mathbb{Q}$ be a modular elliptic curve of prime conductor p. If $p > 37$ then $\mathcal{D}(E) = \pm p$ up to 2-isogenies (i.e., there exists a curve isogenous to E over $\mathbb{Q}$ with discriminant $\pm p$).*

The main ingredients of the proof are the following two theorems.

Theorem 5.2 (Mazur)**.** *Let K be a number field, let E/K be a semistable elliptic curve with discriminant $\mathcal{D}(E)$, and let ℓ be a prime number. Then $E[\ell]$ is a finite flat group scheme if and only if $\ell \mid v_{\mathfrak{q}}(\mathcal{D}(E))$ for all primes $\mathfrak{q}$ in $\mathcal{O}_K$, i.e. if the ideal $(\mathcal{D}(E))$ is an ℓ-th power.*

Proof. See [Maz72] Proposition 9.1. □

Mazur's Theorem gives the second hypothesis of a level-lowering result. One also needs a *big image* hypothesis, i.e. that the residual representation at ℓ is absolutely irreducible; this follows from a result of Fontaine.

Theorem 5.3 (Fontaine)**.** *Let J be a finite flat p-group scheme over $\mathrm{Spec}(\mathcal{O}_K)$. Then if either*

- *$K = \mathbb{Q}$ and $\ell \in \{3, 5, 7, 11, 13, 17\}$; or*
- *$K = \mathbb{Q}(\sqrt{-1})$ and $\ell \in \{3, 5, 7\}$; or*
- *$K = \mathbb{Q}(\sqrt{-3})$ and $\ell \in \{5, 7\}$,*

then J is a direct sum of constant p-groups (i.e. isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$) and diagonalizable p-groups (i.e. isomorphic to the group μ_{p^n}).

Proof. See [Fon85] Theorem B. □

If E/K is a semistable elliptic curve of prime power conductor, and ℓ is a prime dividing the exponent of $\mathcal{D}(E)$, then $E[\ell]$ is a finite flat group scheme over $\mathrm{Spec}(\mathcal{O}_K)$ by Mazur's result. Then if K and ℓ are in the cases considered by Fontaine, we deduce that E must have a point of order ℓ (as $E[\ell]$ cannot be the sum of two diagonalizable groups).

Although over $\mathbb{Q}$ Fontaine's result includes enough primes ℓ to prove Theorem 5.1, a stronger result is needed to cover any imaginary quadratic field of class number 1.

Theorem 5.4. *Let K be an imaginary quadratic field of class number 1 and E/K be a semistable elliptic curve. Let $\ell \geq 3$ be a prime number such that the residual representation of E at ℓ is absolutely reducible. Then either E, or a curve ℓ-isogenous to E over K, has a point of order ℓ defined over K.*

Proof. The residual representation associated to E takes values in $\mathrm{GL}(2, \mathbb{F}_\ell)$, and may be either reducible (over $\mathbb{F}_\ell$) , irreducible but absolutely reducible (i.e., reducible over $\mathbb{F}_{\ell^2}$) or absolutely irreducible. The hypothesis in the theorem excludes only the absolutely irreducible case. Over $\mathbb{Q}$ or any totally real number field, the second case cannot occur, due to the action of complex conjugation: any invariant line over $\mathbb{F}_{\ell^2}$ must be defined over $\mathbb{F}_\ell$. In our situation, we need to consider both the reducible and the absolutely reducible cases separately.

• **Reducible case:** without loss of generality, the residual representation is of the form

$$\overline{\rho_{E,\ell}} \simeq \begin{pmatrix} \theta_1 & * \\ 0 & \theta_2 \end{pmatrix}, \tag{23}$$

for θ_i characters of $\mathrm{Gal}(\overline{K}/K)$ such that $\theta_1\theta_2 = \chi_\ell$ (the cyclotomic character). Since E is semistable, the conductor of the characters θ_i are supported in ℓ. Also since K has class number 1, the only unramified character is the trivial character. Hence we must show that at least one of the characters is unramified, since θ_1 trivial implies that E has a point of order ℓ while if θ_2 is trivial then the isogenous curve has such a point. If ℓ is unramified in K, then the result follows from the proof of Corollaire 1 in [Kra96](pages 249-250), as we now explain.

If ℓ is inert in K then only one of the θ_i can be ramified at ℓ (see [Kra96, Lemme 1]) hence the statement. Then we can restrict to the case when both characters are ramified at a prime dividing ℓ.

If $\ell = \mathfrak{l}_1\mathfrak{l}_2$ splits, we can assume that θ_i has conductor $\mathfrak{l}_i$ since by [Kra96, Lemme 1] they cannot both be ramified at the same prime. Then θ_i is on one hand a character of level 1, so $\theta_1(-1) = -1$, and on the other hand a character of $(\mathcal{O}_K/\mathfrak{l}_i)^\times$ which is trivial in $\mathcal{O}_K^\times$ (as it factors through the Artin map), so $\theta_1(-1) = 1$. This is impossible since $\ell \neq 2$.

Lastly, suppose that ℓ ramifies in K, so $\ell \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{-\ell})$. In particular, the restriction of the cyclotomic character to $\mathrm{Gal}(\overline{K}/K)$ has (odd) order $(\ell-1)/2$. Let $\mathfrak{l}$ denote the prime of K dividing ℓ and $I_\mathfrak{l}$ the associated inertia subgroup. Then the θ_i are both characters of level 1 at $\mathfrak{l}$ (since characters of level 2 have irreducible image), $\theta_1\theta_2 = \chi_\ell$ and E has good supersingular reduction at ℓ. In the notation of [Ser72], let a_ℓ denote the ℓ-th coefficient in the series for multiplication by ℓ in the formal group of $\tilde{E}$, the reduced curve over $\mathcal{O}_K/\mathfrak{l} \cong \mathbb{F}_\ell$. By [Ser72, Proposition 10, page 272], if $v_\ell(a_\ell) > 1$, then $\theta_i|_{I_\mathfrak{l}}$ for $i = 1, 2$ would both equal the square of fundamental characters of level 2, whose image is not in $\mathbb{F}_\ell$; hence the valuation is 1, and the same Proposition implies that $\theta_i|_{I_\mathfrak{l}}$ equals the fundamental character of level 1 for $i = 1, 2$, and $*$ is unramified at ℓ. So θ_1/θ_2 is unramified, hence trivial, and so $\theta_1 = \theta_2$ and $\theta_1^2 = \chi_\ell$.

The order of θ_1 equals $\ell - 1$ and it factors through a cyclic degree $(\ell-1)$-extension of K unramified outside ℓ, containing ζ_ℓ (the ℓ-th roots of unity). This implies in particular the existence of a quadratic extension of K unramified outside ℓ. It can be easily verified (using [PAR14] for example) that there are no such quadratic extensions, hence this case cannot occur.

• **Irreducible but absolutely reducible case**. In this case, there is a character of K of order $\ell^2 - 1$ or $\frac{\ell^2-1}{2}$ unramified outside ℓ (by the same argument as before). This implies the existence of a quadratic extension of K unramified outside ℓ which, as we saw in the previous case, does not exist. □

We can now state and prove the main theorem.

Theorem 5.5. *Let K be an imaginary quadratic field of class number 1. Let E/K be a modular elliptic curve of prime conductor. Assume Conjecture 2 holds. Then there exists a curve isogenous to E over K with prime discriminant.*

Proof. Let $\mathfrak{p}$ be the conductor of E. If $\mathfrak{p} \mid 2$, we compute for each of the quadratic fields, all elliptic curves of conductor $\mathfrak{p}$ using [Kou17], and it turns out that there is no such curve. This is consistent with the tables of automorphic forms of [Cre84].

When $\mathfrak{p} \nmid 2$, Corollary 2.13 implies that up to 2-isogeny we can assume that $v_\mathfrak{p}(\mathcal{D}(E))$ is odd. Suppose there exists an odd prime number ℓ dividing $v_\mathfrak{p}(\mathcal{D}(E))$. By Theorem 5.2, $E[\ell]$

is a finite flat group scheme. Theorem 5.4 implies that either the residual representation is absolutely irreducible, or the curve (or another ℓ-isogenous curve) has a rational torsion point of order ℓ. In section 3 all curves of odd prime conductor with an ℓ-torsion point were computed (see Table 3.1) except for $\ell = 3$ over the field $\mathbb{Q}(\sqrt{-3})$, where we proved that the curve or the 3-isogenous curve has discriminant valuation prime to 3 (see Theorem 3.3). In particular in all cases there is a curve in the isogeny class of discriminant with valuation prime to ℓ, so we can assume that the residual representation is indeed absolutely irreducible. Since we assume E to be modular, Conjecture 2 implies the existence a mod ℓ Bianchi modular form of level 1 whose Galois representation matches the residual representation of E modulo ℓ. This contradicts Theorem 4.1, and the result follows. □

As a corollary, we have the following version of Szpiro's conjecture.

Corollary 5.6. *Let K be an imaginary quadratic field of class number 1. Assume that Conjecture 2 holds. Let E/K be a modular elliptic curve of prime power conductor. Then $\mathcal{N}(\mathcal{D}_{\min}(E)) \leq \mathcal{N}(\mathrm{cond}(E))^6$, except for the curve 11.a2 over $\mathbb{Q}(\sqrt{-11})$, whose conductor has valuation 1 while its discriminant has valuation 10.*

Proof. If E has potentially good reduction, then the result is well known, see for example Table 4.1 of [Sil94]. Otherwise, either E is semistable or is a quadratic twist of a semistable curve. For the semistable ones, Theorem 5.5 proves that up to isogeny the discriminant valuation is 1. In the case where there is a 2-isogeny, the isogenous curve has discriminant valuation 2. When there is a 3-isogeny, the isogenous curve has discriminant valuation 3 or 6 (depending whether the conductor ramifies or not), and there is a unique one with a 5-isogeny, which is precisely the curve 11.a2. Since twisting raises the discriminant valuation by 6, and the conductor valuation by 1, the result follows. □

References

[BH07] Tobias Berger and Gergely Harcos. l-adic representations associated to modular forms over imaginary quadratic fields. *Int. Math. Res. Not. IMRN*, 23:Art. ID rnm113, 16, 2007.

[CL07] J. E. Cremona and M. P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.*, 16(3):303–312, 2007.

[Cre84] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984.

[Cre92] J. E. Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc. (2)*, 45(3):404–416, 1992.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[cS14] Mehmet Haluk ¸Sengün. Arithmetic aspects of Bianchi groups. In *Computations with modular forms*, volume 6 of *Contrib. Math. Comput. Sci.*, pages 279–315. Springer, Cham, 2014.

[CV12] F. Calegari and A. Venkatesh. A torsion jacquet-langlands correspondence. *arXiv:1212.3847*, 2012.

[CW94] J. E. Cremona and E. Whitley. Periods of cusp forms and elliptic curves over imaginary quadratic fields. *Math. Comp.*, 62(205):407–429, 1994.

[DGP10] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.*, 79(270):1145–1170, 2010.

[Fon85] Jean-Marc Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[HST93] Michael Harris, David Soudry, and Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to $\mathrm{GSp}_4(\mathbf{Q})$. *Invent. Math.*, 112(2):377–411, 1993.

[IR82] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Number 84 in Graduate Texts in Mathematics. Springer-Verlag, 1982.

[Kam92] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[Kou17] A. Koutsianas. Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction. *Experimental Mathematics*, pages 1–15 (electronic), 2017.

[Kra89] Alain Kraus. Quelques remarques à propos des invariants c_4, c_6 et δ d'une courbe elliptique. *Acta Arith.*, 54:75–80, 1989.

[Kra96] Alain Kraus. Courbes elliptiques semi-stables et corps quadratiques. *J. Number Theory*, 60(2):245–253, 1996.

[Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[LMF13] The LMFDB Collaboration. The l-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 16 September 2013].

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[MO89] J.-F. Mestre and J. Oesterlé. Courbes de Weil semi-stables de discriminant une puissance m-ième. *J. Reine Angew. Math.*, 400:173–184, 1989.

[PAR14] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`.

[Rib91] Kenneth A. Ribet. Lowering the levels of modular representations without multiplicity one. *Internat. Math. Res. Notices*, (2):15–19, 1991.

[S$^+$17] W. A. Stein et al. *Sage Mathematics Software (Version 8.0)*. The Sage Development Team, 2017. `http://www.sagemath.org`.

[Sch15] Peter Scholze. On torsion in the cohomology of locally symmetric varieties. *Ann. of Math. (2)*, 182(3):945–1066, 2015.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Set75] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Tay94] Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. II. *Invent. Math.*, 116(1-3):619–643, 1994.

Warwick Mathematics Institute, University of Warwick, Coventry, CV4 7AL, UK
E-mail address: `j.e.cremona@warwick.ac.uk`

FaMAF-CIEM, Universidad Nacional de Córdoba. C.P:5000, Córdoba, Argentina.
E-mail address: `apacetti@famaf.unc.edu.ar`