Elliptic Curves with Prime Conductor and a Conjecture of Cremona

by

René-Michel Shumbusho

(Under the direction of Dino Lorenzini)

Abstract

We find the elliptic curves defined over imaginary quadratic number fields K with class number one that have prime conductor and a K-rational 2-torsion point. Any elliptic curve with K-rational 2-torsion point has an equation of the form $y^2 = x^3 + Ax^2 + Bx$. We find conditions on A and B for the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ to have prime conductor. We also use class field theory to find primes that cannot be conductors of elliptic curves over $K = \mathbb{Q}(\sqrt{d})$ for $d = -1$, -2, -3, -7 and -11.

Index words: Elliptic curves, conductor

Elliptic Curves with Prime Conductor and a Conjecture of Cremona

by

René-Michel Shumbusho

Baccalauréat, Université Nationale du Rwanda, 1989

Licence, Université Nationale du Rwanda, 1992

A Dissertation Submitted to the Graduate Faculty

of The University of Georgia in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2004

Elliptic Curves with Prime Conductor and a Conjecture of Cremona

by

René-Michel Shumbusho

Approved:

Major Professor: Dino Lorenzini

Committee: Matthew Baker
Andrew Granville
Robert Rumely
Robert Varley

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
August 2004

Acknowledgments

I would like to thank my advisor, Dino Lorenzini, for his guidance and patience during the preparation of this dissertation. His many observations and suggestions were very helpful for the completion of this work. I would also like to thank Sungkon Chang and Charles Pooh for answering the many questions that I had, especially about LaTeX and programming with gp-Pari and Maple.

Table of Contents

Chapter 1

Introduction

Since Shafarevich (see [44]) proved that for any number field K and any finite set S of prime ideals of K, the set $\mathbb{E}_{K,S}$ of isomorphic classes of elliptic curves E/K with good reduction outside S is finite, much has been written regarding the complete determination of the set $\mathbb{E}_{K,S}$ for specific K and S. When $K = \mathbb{Q}$, thanks to the Shimura-Taniyama-Weil correspondence (see [4]), given a set S of prime ideals of $\mathbb{Q}$, the set $\mathbb{E}_{\mathbb{Q},S}$ can be, in theory, effectively determined.

Prior to the work of Wiles, Neumann (see [32]) had proved that given a rational prime p distinct from 2, 3 and 17, there is an elliptic curve defined over $\mathbb{Q}$ with prime conductor p and a rational 2-torsion point if and only if p is of the form $p = A^2 + 64$, for some $A \in \mathbb{Z}$. For each prime of this form, Setzer showed that there are only two isogenous elliptic curves with conductor p and a rational 2-torsion point:

$$y^2 = x^3 + Ax^2 - 16x, \qquad \Delta = 2^{12}p \tag{1.1}$$

$$y^2 = x^3 - 2Ax^2 + px, \qquad \Delta = -2^{12}p^2. \tag{1.2}$$

where A is choosen so that $A \equiv 1 \bmod 4$. He also showed that the elliptic curves with conductor 17 are:

$$y^2 = x^3 - 15x^2 - 16x, \qquad \Delta = 2^{12}17^2, \tag{1.3}$$

$$y^2 = x^3 - 66x^2 + x, \qquad \Delta = 2^{12}17, \tag{1.4}$$

$$y^2 = x^3 + 9x^2 + 16x, \qquad \Delta = 2^{12}17, \tag{1.5}$$

$$y^2 = x^3 + 30x^2 + 289x, \qquad \Delta = -2^{12}17^4. \tag{1.6}$$

Much less is known about the sets $\mathbb{E}_{K,S}$ when $K \neq \mathbb{Q}$. Stroeker proved (see [48]) that, if K is an imaginary quadratic field with class number coprime to six, then there are no elliptic curves defined over K with good reduction everywhere i.e., with $S = \emptyset$. Results of this type have been extended for some specific imaginary quadratic fields to all abelian varieties. Indeed, Fontaine (see [13]) proved that there are no abelian varieties defined over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ with good reduction everywhere. From a result by Schoof (see [40]), it follows that there are no abelian varieties defined over $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-2})$ with good reduction everywhere. Assuming the General Riemann Hypothesis, Schoof also shows that there are no abelian varieties defined over $\mathbb{Q}(\sqrt{-11})$ with good reduction everywhere.

For a given $S \neq \emptyset$, the complete determination of the set $\mathbb{E}_{K,S}$ has been obtained in only few cases. Pinch determined the elliptic curves over certain imaginary quadratic fields with good reduction outside 2 or 3 (see [37] and [39]).

Cremona conjectured (see [9]) that when K is an imaginary quadratic number field, there is a one-to-one correspondence between isogeny classes of elliptic curves over K with conductor $\mathfrak{a}$, with no complex multiplication, and certain cuspidal automorphic forms of weight 2 for the congruence subgroup $\Gamma_0(\mathfrak{a})$. In the second line of the table below, we list the minimal norms $N^{min}_{K/\mathbb{Q}}(\mathfrak{a})$ of possible conductors of elliptic curves over K as predicted by Cremona's conjecture.

K	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{2}i)$	$\mathbb{Q}(\sqrt{3}i)$	$\mathbb{Q}(\sqrt{7}i)$	$\mathbb{Q}(\sqrt{11}i)$	$\mathbb{Q}(\sqrt{19}i)$	$\mathbb{Q}(\sqrt{43}i)$	$\mathbb{Q}(\sqrt{67}i)$	$\mathbb{Q}(\sqrt{163}i)$
$N^{min}_{K/\mathbb{Q}}(\mathfrak{a})$	25	9	49	16	11	19	43	67	≥ 100
$N^{min}_{K/\mathbb{Q}}(\mathfrak{a}) \geq$	7	2	12	3	1	1	1	1	1

The entries on the second line up follow from the tables 3.2.3, 3.3.3, 3.4.3, 3.5.3 and 3.6.3 in [9] and additional tables available from Cremona. The entries in the third line of the above table are obtained using the lower bound $N_{K/\mathbb{Q}}(\mathfrak{a}) \geq 100|\Delta_{K/\mathbb{Q}}|^{-2}$ of Mestre. Indeed, Mestre shows, under the conjecture that the L-function of an abelian variety has analytic continuation and functional equation, that an abelian variety $A/\mathbb{Q}$ of dimension d has conductor at least 10^d (see [26]). Applying this result to the Weil restriction $Res_{K/\mathbb{Q}}(E)$ of an elliptic curve E/K

and a formula for the conductor of the Weil restriction by Milne (see Proposition 1 in [28]), we obtain that $N_{K/\mathbb{Q}}(\mathfrak{f}_{E/K})|\Delta_{K/\mathbb{Q}}|^2 \geq 10^2$, where $\mathfrak{f}_{E/K}$ is the conductor of the elliptic curve E/K and $\Delta_{K/\mathbb{Q}}$ is the discriminant of the extension $K/\mathbb{Q}$.

In this work, we provide two types of results:

1) A criterion that ensures when applicable the non-existence of elliptic curves E/K with prime conductor (π),

2) For a given prime (π), a necessary and sufficient condition for the existence of an elliptic curve E/K with prime conductor (π) having a K-rational 2-torsion point.

We are also able to exhibit, in some instances, the complete list of elliptic curves E/K with conductor a given prime (π).

If E/K is an elliptic curve of prime conductor (π), let $N_{K/\mathbb{Q}}(\pi)$ be the norm of π. Then, the minimal norm of possible prime conductor $N_{K/\mathbb{Q}}^{min}(\pi)$ predicted by Cremona's conjecture is given in the table below:

K	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Q}(\sqrt{-19})$	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}(\sqrt{-67})$
$N_{K/\mathbb{Q}}^{min}(\pi)$	121	73	11	19	43	67

For $K = \mathbb{Q}(\sqrt{-2})$ (resp. $\mathbb{Q}(\sqrt{-7})$), the smallest norm for prime conductor is ≥ 300 (resp. ≥ 200).

We also get from Cremona's conjecture, that the smallest prime p_{min} such that there is an elliptic curve over K with prime conductor (π) dividing p_{min} is given in the table below:

K	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Q}(\sqrt{-19})$
p_{min}	11	11	11	19

To illustrate our results, we list below the primes p between 2 and 100 where we can show that there do not exist elliptic curves over K of conductor (π) dividing p. More complete lists are found in corollaries 3.3, 4.2, 5.3, 6.3 and 7.2.

Theorem 1.1 *a) If $K = \mathbb{Q}(i)$, there are no elliptic curves over K with prime conductor dividing $p = 2$, 3, 5, 7, 13, 17, 29, 31, 37, 41, 47, 53, 59, 61, 71, 73, 89 and 97.*

b) If $K = \mathbb{Q}(\sqrt{-2})$*, there are no elliptic curves over* K *with prime conductor dividing* $p = 2, 5, 7, 11, 13, 17, 19, 23, 31, 41, 43, 47, 59, 73, 83, 89$ *and* 97.

c) If $K = \mathbb{Q}(\sqrt{-3})$*, there are no elliptic curves over* K *with prime conductor dividing* $p = 2, 3, 5, 7, 19, 31, 43, 67, 71$ *and* 79.

d) If $K = \mathbb{Q}(\sqrt{-7})$*, there are no elliptic curves over* K *with prime conductor dividing* $p = 2, 11, 23, 41, 43, 67$ *and* 71.

e) If $K = \mathbb{Q}(\sqrt{-11})$*, there are no elliptic curves with prime conductor dividing* $p = 5, 7, 13, 23, 29, 31, 37, 53, 67$ *and* 71.

Our methods apply mainly to the case of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ of class number one, with $d = -1, -2, -3, -7, -11, -19, -43, -67$ and -163. We devote different chapters to the elliptic curves over these fields, taking into account what units are in the field and how 2 ramifies in that field:

a) In $\mathbb{Q}(i)$, 2 ramifies and there are 4 units, ± 1 and $\pm i$.

b) In $\mathbb{Q}(\sqrt{-2})$, 2 ramifies and the only units are ± 1.

c) In $\mathbb{Q}(\sqrt{-3})$, 2 is prime and there are six units, the six-th roots of unity.

d) In $\mathbb{Q}(\sqrt{-7})$, 2 splits and the only units are ± 1.

e) In $\mathbb{Q}(\sqrt{d})$, $d = -11, -19, -43, -67, -163$, 2 is prime and the only units are ± 1.

In the next chapter, we give properties that elliptic curves defined over K, with prime conductor and K-rational two-torsion point, have. We also give conditions under which an elliptic curve over K with prime conductor necessarily has a K-rational 2-torsion point. The conditions that we find can be applied in the case of $K = \mathbb{Q}(\sqrt{d})$, with $d = -1, -2, -3$ and -7. We also find all the elliptic curves defined over the imaginary quadratic number fields with class number one, that admit a K-rational 3-isogeny. We finally find conditions

under which an elliptic curve over K with prime conductor not dividing 3 necessarily has a K-rational 3-isogeny. The conditions that we find can be applied in the case of $K = \mathbb{Q}(\sqrt{d})$, with $d = -1$, -2 and -11. In chapter 3 through chapter 7, we determine the elliptic curves with prime conductor and K-rational 2-torsion points, defined over the imaginary quadratic fields with class number one, and give lists of primes that are not conductors for elliptic curves.

In this thesis, we treat only the case of number fields K. Let us note that the analogue problem of the determination of $\mathbb{E}_{K,S}$ where K is a function field is also of interest. This problem is studied, for instance, by Beauville (see [2]) over the function field $\mathbb{C}(t)$, and Nguyen (see [33]) over the function field $k(t)$, with k of positive characteristic.

Chapter 2

Elliptic curves over number fields

In this chapter, we give some properties that an elliptic curve defined over a number field K, with prime conductor not dividing 2 or 3 and having a K rational 2-torsion point, must satisfy. Let E/K be an elliptic curve over K with Weistrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. If this equation is a global minimal equation for E/K, and E/K has prime conductor (π), then its discriminant is $\Delta_{min} = u\pi^s$, for some unit u and some $s \in \mathbb{N}^*$. If in addition, E/K admits a K-rational 2-torsion point, then it admits an equation of the form $y^2 = x^3 + Ax^2 + Bx$ whose discriminant is $\Delta = 16B^2(A^2 - 4B)$. The relation between this discriminant and Δ_{min} is given by $\Delta = 2^{12}\Delta_{min}$, so that $B^2(A^2 - 4B) = 2^8u\pi^s$. Thus, to find the elliptic curves with prime conductor not dividing 2 or 3 having a K-rational 2-torsion points, it suffices to find the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ such that $B^2(A^2 - 4B) = 2^8u\pi^s$. For each such elliptic curve, we have to check whether it has good reduction at the primes in K dividing 2, and that it has multiplicative reduction at π. We will find conditions on A and B for this to be true. In later chapters, we solve the equation $B^2(A^2 - 4B) = 2^8u\pi^s$ and find all the elliptic curves with prime conductor π not dividing 2 or 3 having a K-rational 2-torsion point, for $K = \mathbb{Q}(\sqrt{d})$, with $d = -1$, -2, -3, -7, -11, -19, -43, -67 and -163. These are the imaginary quadratic fields with class number one. In this chapter, we also find conditions that garanty, for a given prime π in K, the non-existence of elliptic curves over K with conductor (π) and no K-rational 2-torsion points.

We will also study the elliptic curves with prime conductor (π) not dividing 3, and K-rational 3-isogeny. For $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$, -2, -7, -11, -19, -43, -67, -163, we

find the possible primes π not dividing 3 such that there exists an elliptic curve over K with prime conductor (π) and K-rational 3-isogeny. It turns out that the only possibilities are $(\pi) = (19)$, $(\sqrt{-19})$ or (37). We note here that Miyawake (see [29]) has shown that if $K = \mathbb{Q}$, the possible primes p such that there exists an elliptic curve over $\mathbb{Q}$ with conductor p and a $\mathbb{Q}$-rational 3-torsion point, are 19 and 37. For a given number field K, we also find conditions that garanty, for a given prime π, the non-existence of elliptic curves over K with conductor (π) and no K-rational 3-isogeny. Thus, for those imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with class number one where the conditions are satisfied, if (π) is not one of (19), $(\sqrt{-19})$ or (37), then those conditions garanty the non-existence of elliptic curves with conductor (π).

Let us first remark that for any number field K, there is the following easy

Lemma 2.1 *Let K be a number field. Let π be a prime of $\mathcal{O}_K$ not dividing 2, and let u and ϵ be units of K. If $A \in \mathcal{O}_K$ is such that $A^2 + 64u = \epsilon\pi^s$ and A is a square modulo 4, then the elliptic curve*

$$y^2 = x^3 + Ax^2 - 16ux \tag{2.1}$$

has conductor (π).

Proof. The elliptic curve (2.1) has discriminant $\Delta = 2^{12}\epsilon\pi^s$ and $c_4 = 16(A^2 + 48u)$. Since c_4 is coprime to π, the equation (2.1) is minimal at π and the elliptic curve has multiplicative reduction at π. We have that $A = a_1^2 + 4a_2$ for some $a_1, a_2 \in \mathcal{O}_K$. Hence, the elliptic curve (2.1) is isomorphic to $y^2 + a_1xy = x^3 + a_2x^2 - ux$, which has discriminant $\Delta' = \epsilon\pi^s$. This proves that our elliptic elliptic curve has good reduction everywhere except at π, where it has multiplicative reduction. Hence, it has conductor (π). □

Remark 2.2 a) For E an elliptic curve over K, with prime conductor (π), the minimal discriminant can be written in the form $\Delta = u\pi^s$, where u is a unit. By Szpiro's conjecture (see Spiro's Conjecture 10.6 in [46]), there should exist a constant $s(K)$, depending on K, such that $s \leq s(K)$, for any such elliptic curve.

b) The following curves are the only elliptic curves defined over an imaginary quadratic field K with class number 1, not defined over $\mathbb{Q}$, and found to have a K-rational point of order 2, prime conductor (π) dividing p, with $\Delta = u\pi^s$ and $s \geq 3$:

$$y^2 = x^3 - 2(1-16i)x^2 + (1+16i)^2 x, \qquad \Delta = -i(1+16i)^4, \quad p = 257, \qquad (3.8)$$

$$y^2 = x^3 + 2(1-17\theta)x^2 + \theta^2(16-\theta)^2 x, \quad \Delta = \theta^4(16-\theta)^4, \quad p = 241, \qquad (5.6)$$

$$y^2 = x^3 - (9+19\theta)x^2 - 16x, \qquad \Delta = \theta(8+\theta)^3, \quad p = 73, \qquad (5.9)$$

$$y^2 = x^3 + 2(9+19\theta)x^2 + \theta(8+\theta)^3 x, \qquad \Delta = -\theta^4(8+\theta)^6, \quad p = 73, \qquad (5.10)$$

where $\theta = (1+\sqrt{-3})/2$. It is natural to wonder whether the supremum of the integers $s(E/K)$, where K runs through all the imaginary quadratic fields, and E/K is an elliptic curve with K-rational 2-torsion points and prime conductor (π), is finite. We have not been able to settle this question, but as our remark below indicates, the analoguous question with $[K:\mathbb{Q}] = 4$ has a negative answer.

c) Let p be a rational prime. Let s be a positive integer. Write $A = B^2 + 4$. Then $A^2+64 = B^4+8B^2+80$. The equation $A^2+64 = p^s$ becomes $B^4+8B^2+80-p^s = 0$. Let $f(x) = x^4+8x^2+80-p^s$. This is irreducible if $p = 7$. Indeed, let $\bar{f}(x) = x^4+8x^2+80 = x^4+x^2+3$ be the reduction of $f(x)$ modulo 7. Let $\bar{g}(x) = x^2+x+3$. If $\bar{f}(x)$ has a root in $\mathbb{F}_p$, then $\bar{g}(x)$ has a root as well in $\mathbb{F}_p$. The discriminant of $\bar{g}(x)$ is $\Delta(\bar{g}) = -11$. Since -11 is not a square in $\mathbb{F}_7$, we have that $\bar{g}(x)$ has no roots in $\mathbb{F}_7$, and so $\bar{f}(x)$ itself has no roots in $\mathbb{F}_7$. Suppose $\bar{f}(x) = (x^2+ax+b)(x^2+cx+d)$. Expanding and identifying corresponding coefficients, we find that this cannot happen in $\mathbb{F}_7[x]$. Thus, $\bar{f}(x)$ is irreducible. We deduce that $f(x)$ itself is irreducible. Therefore, it defines an extension K_s of $\mathbb{Q}$ of degree 4. In K_s, there is an A such that $A^2+64 = 7^s$ and A is a square modulo 4. Let $S = \mathcal{O}_{K_s} - (7)$. The discriminant of $f(x)$ is $-256(-80+7^s)(-64+7^s)^2$ and is not divisible by 7. Hence, $S^{-1}\mathcal{O}_{K_s} = \mathbb{Z}_{(7)}[B]$. Since $\bar{f}(x)$ is irreducible, we deduce that 7 is inert in K_s. Thus, the curve $y^2 = x^3 + (B^2+4)x^2 - 16x$ is an elliptic curve over K_s with prime conductor (7) and minimal discriminant $\Delta_{min} = 7^s$. But s can be

taken arbitrarily. Thus, we deduce that there exists no constant C, such that for all number fields K of degree 4, any elliptic curve E/K over K with prime conductor $\mathfrak{p}$, and minimal discriminant $\mathfrak{p}^s$, is such that $s \leq C$.

The following result is about elliptic curves over imaginary quadratic fields K with class number one that have prime conductor (p), with p a rational prime that remains prime in K, and admitting a K-rational 2-torsion point:

Proposition 2.3 *Let K be an imaginary quadratic field with class number one. Let p be a rational prime, distinct from 2 and 3, that remains prime in K. Suppose E is an elliptic curve over K with prime conductor (p) having a K-rational 2-torsion point. Then, the elliptic curve E is defined over $\mathbb{Q}$.*

Proof. The proof is a combination of theorem 3.1, lemma 3.22, 4.1, 4.14, theorem 5.1, lemma 5.15, remark 5.16, theorem 6.1, lemma 6.13, theorem 7.1, lemma 7.12 and remark 7.13. By Theorems 3.1, 4.1, 5.1, 6.1 and 7.1, an elliptic curves over K with prime conductor p and a K-rational 2-torsion point exists only if the equation $A^2 + 64i = up^{2r+1}$ in the case of $K = \mathbb{Q}(i)$, and $A^2 + 64 = up^{2r+1}$ in the other cases, has a solution with $A \in \mathcal{O}_K$ a square modulo 4. But by lemma 3.22, the equation $A^2 + 64i = up^{2r+1}$ has no solutions $A \in \mathbb{Z}[i]$. By lemma 4.14, the equation $A^2 + 64 = up^{2r+1}$ has no solutions $A \in \mathbb{Z}[2]$. By lemma 5.15, remark 5.16, lemma 6.13, 7.12 and remark 7.13, the equation $A^2+64 = up^{2r+1}$ has a solution $A \in \mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{d})$, $d = -3$, -7, -11, -19, -43, -67 or -163, only if A is a rational integer, $u = 1$ and $r = 1$. The corresponding elliptic curves are then $y^2 = x^3 + Ax^2 - 16x$ and $y^2 = x^3 - 2Ax^2 + px$ which are defined over $\mathbb{Q}$. □

Let K be a number field, and let E/K be an elliptic curve given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

We have

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta. \end{aligned}$$

The invariants c_4, c_6 and Δ are related by

$$c_4^3 - c_6^2 = 1728\Delta. \tag{2.3}$$

The x-coordinates of the 2-torsion points are the roots of the polynomial

$$x^3 + b_2x^2 + 8b_4x + 16b_6. \tag{2.4}$$

The x-coordinates of the 3-torsion points are the roots of the polynomial

$$3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8. \tag{2.5}$$

A K-rational cyclic subgroup of order 3 of E/K is a cyclic subgroup of E generated by a point $P \in E(\bar{K})$ such that $3P = O$ and whose x-coordinate is in K.

Suppose the equation (2.2) is a global minimal Weirstrass equation of an elliptic curve E defined over K, with prime conductor $\mathfrak{p}$, $\mathfrak{p}$ principal not dividing 2 or 3. If Δ_{min} is the discriminant of this equation, then $\Delta_{min} = u\pi^s$, where u is a unit and π is a generator of $\mathfrak{p}$. Suppose that E has a K-rational 2-torsion point. Let $P = (x, y)$ be such a point. Then we know that $x \in K$ and $x^3 + b_2x^2 + 8b_4x + 16b_6 = 0$. Let $f(x) := x^3 + b_2x^2 + 8b_4x + 16b_6$.

Lemma 2.4 *Let E be an elliptic curve with global minimal equation (2.2) that has good reduction at the primes of K dividing 2. Then a prime $\mathfrak{p}_2$ in K above 2 cannot divide simultaneously a_1 and a_3.*

Proof. If $\mathfrak{p}_2$ divides a_1 and a_3, then it divides Δ_{min}, so that the elliptic curve E does not have good reduction at $\mathfrak{p}_2$, which contradicts the hypothesis on E. Thus $\mathfrak{p}_2$ cannot divide both a_1 and a_3. □

Lemma 2.5 *Let E be an elliptic curve defined over K, with global minimal equation (2.2) and good reduction at $\mathfrak{p}_2$. Let $e := \mathrm{ord}_{\mathfrak{p}_2}(2)$. If E has a K-rational 2-torsion point, then $\mathrm{ord}_{\mathfrak{p}_2}(a_1) < e$ or $\mathrm{ord}_{\mathfrak{p}_2}(a_1) \geq e$ and $3 \mid e$. If $e = 2$, then there are two cases:*

- $\mathrm{ord}_{\mathfrak{p}_2}(a_1) = 0$, *or*
- $\mathrm{ord}_{\mathfrak{p}_2}(a_1) = 1$ *and* $\mathrm{ord}_{\mathfrak{p}_2}(a_3) = 0$.

If $e = 1$, then we must have $\mathrm{ord}_{\mathfrak{p}_2}(a_1) = 0$.

Proof. Assume that $\mathrm{ord}_{\mathfrak{p}_2}(a_1) \geq 1$. Then $\mathrm{ord}_{\mathfrak{p}_2}(a_3) = 0$ by lemma 2.4 and

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}_2}(b_2) &\geq min(2\mathrm{ord}_{\mathfrak{p}_2}(a_1), 2e + \mathrm{ord}_{\mathfrak{p}_2}(a_2)),\\
\mathrm{ord}_{\mathfrak{p}_2}(b_4) &\geq min(\mathrm{ord}_{\mathfrak{p}_2}(a_1), e + \mathrm{ord}_{\mathfrak{p}_2}(a_4)),\\
\mathrm{ord}_{\mathfrak{p}_2}(8b_4) &\geq min(3e + \mathrm{ord}_{\mathfrak{p}_2}(a_1), 4e + \mathrm{ord}_{\mathfrak{p}_2}(a_4)),\\
\mathrm{ord}_{\mathfrak{p}_2}(b_6) &= 0,\\
\mathrm{ord}_{\mathfrak{p}_2}(16b_6) &= 4e.
\end{aligned}$$

The Newton polygon of $f(x)$ at $\mathfrak{p}_2$ is the lower boundary of the convex hull of the points $(0, \mathrm{ord}_{\mathfrak{p}_2}(16b_6))$, $(1, \mathrm{ord}_{\mathfrak{p}_2}(8b_4))$, $(2, \mathrm{ord}_{\mathfrak{p}_2}(b_2))$, $(3, 0)$. The line joining $(0, \mathrm{ord}_{\mathfrak{p}_2}(16b_6))$ and $(3, 0)$ has equation $y = -\frac{4e}{3}x + 4e$. Let $g(x) = -\frac{4e}{3}x + 4e$. We have $g(1) = \frac{8e}{3}$ and $g(2) = \frac{4e}{3}$. If $\mathrm{ord}_{\mathfrak{p}_2}(a_1) \geq e$, then $\mathrm{ord}_{\mathfrak{p}_2}(8b_4) \geq g(1)$ and $\mathrm{ord}_{\mathfrak{p}_2}(b_2) \geq g(2)$. In that case, the Newton polygon of $f(x)$ is the line $y = g(x)$. If e is coprime to 3, the slope of this line is not an

integer, which implies that $f(x)$ has no roots in K and, hence, our elliptic curve does not have any K-rational 2-torsion points. $\square$

The equation (2.2) for an elliptic curve E can be transformed into

$$y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6. \tag{2.6}$$

If the elliptic curve E has prime conductor (π), then its discriminant is $\Delta = u2^{12}\pi^s$. If in addition E has a K-rational 2-torsion point, then there is a $t \in \mathcal{O}_K$ such that $t^3 + b_2t^2 + 8b_4t + 16b_6 = 0$. The change of variables $x = X + t$, $y = Y$ gives the new equation for E

$$Y^2 = X^3 + AX^2 + BX, \tag{2.7}$$

with $A = b_2 + 3t$ and $B = 3t^2 + 2b_2t + 8b_4$. Equation (2.7) has same discriminant as equation (2.6), $\Delta = 16B^2(A^2 - 4B) = u2^{12}\pi^s$. After simplification, we get

$$B^2(A^2 - 4B) = u2^8\pi^s. \tag{2.8}$$

We have thus proved the following result:

Lemma 2.6 *An elliptic curve with prime conductor* $\mathfrak{f} = (\pi)$ *and a* K*-rational* 2*-torsion point has an equation of the form* $y^2 = x^3 + Ax^2 + Bx$ *with* A, $B \in \mathcal{O}_K$ *such that* $B^2(A^2 - 4B) = u2^8\pi^s$, *where* u *is a unit and* $s \in \mathbb{N}^*$.

The elliptic curve $y^2 = x^3 + Ax^2 + Bx$ has the invariants Δ, c_4, c_6 and j, with

$$\begin{aligned} \Delta &= 2^4B^2(A^2 - 4B), \\ c_4 &= 2^4(A^2 - 3B), \\ c_6 &= 32A(9B - 2A^2), \\ j &= \frac{16^2(A^2 - 3B)^3}{B^2(A^2 - 4B)}. \end{aligned}$$

There is also another invariant $[w]$ defined as follows. First, let

$$\begin{aligned} w &:= c_4/c_6 \quad \text{if} \quad j \neq 0 \text{ or } 1728, \\ w &:= c_4 \quad\quad\;\; \text{if} \quad j = 1728, \\ w &:= c_6 \quad\quad\;\; \text{if} \quad j = 0, \end{aligned}$$

then set $[w]$ to be the class of w in $K^*/(K^*)^{n(j)}$, where $n(j) = 2, 4$ or 6, if $j \neq 1728$ or 0, $j = 1728$, or $j = 0$ respectively. In our case, we have

$$\begin{aligned} w = &\ \tfrac{2A(9B-2A^2)}{A^2-3B} && \text{if} \quad j \neq 0 \text{ or } 1728, \\ w = &\ 2^4(A^2 - 3B) && \text{if} \quad j = 1728, \\ w = &\ 32A(9B - 2A^2) && \text{if} \quad j = 0. \end{aligned}$$

For a prime $\mathfrak{p}$ not dividing 2 or 3 where the equation is minimal, we know that if the elliptic curve does not have good reduction, then it has multiplicative reduction if and only if $\mathfrak{p}$ does not divide c_4. Hence the elliptic curve (2.7) satisfying (2.8) has multiplicative reduction at $\mathfrak{p}$ if $\mathfrak{p}$ does not divide B and A^2-4B simultaneously. It does not have multiplicative reduction at $\mathfrak{p}$ if $\mathfrak{p}$ divides B and $A^2 - 4B$ simultaneously. We also know that two elliptic curves are isomorphic over K if and only if they have the same j-invariants and the $[w]$'s are the same.

Lemma 2.7 *For an elliptic curve over K with multiplicative reduction at the prime $\mathfrak{p} = (\pi)$ and equation $y^2 = x^3 + Ax^2 + Bx$ minimal at $\mathfrak{p}$, we must have that π does not divide simultaneously A and B. If the elliptic curve has a global minimal equation of the form (2.2), and if $\mathfrak{p}_2$ is a prime that divides 2 such that $\mathfrak{p}_2 \nmid a_1$, then $\mathfrak{p}_2$ cannot divide simultaneously A and B.*

Proof. The equation $y^2 = x^3 + Ax^2 + Bx$ being minimal at $\mathfrak{p}$ and E being an elliptic curve with multiplicative reduction at $\mathfrak{p}$, π cannot divide $c_4 = 2^4(A^2 - 3B)$, so π cannot divide A and B simultaneously. In the case when $\mathfrak{p}_2 \nmid a_1$, the prime $\mathfrak{p}_2$ above 2 does not divide b_2 and thus cannot divide A and B simultaneously as well: indeed

$$\begin{aligned} \mathfrak{p}_2 \mid A = b_2 + 3t \quad &\Rightarrow \quad \mathfrak{p}_2 \nmid t \\ &\Rightarrow \quad \mathfrak{p}_2 \nmid 3t^2 + 2b_2t + 8b_4 = B, \\ \mathfrak{p}_2 \mid B = 3t^2 + 2b_2t + 8b_4 \quad &\Rightarrow \quad \mathfrak{p}_2 \mid t \\ &\Rightarrow \quad \mathfrak{p}_2 \nmid a_1^2 + 4a_2 + 3t = A. \end{aligned}$$

Therefore, $\mathfrak{p}_2$ cannot divide simultaneously A and B. $\square$

To check whether an elliptic curve defined over an imaginary quadratic field with equation (2.7) has good reduction at $\mathfrak{p}_2$, we use the following criterion, due to Bennett Setzer (the lemma after Theorem 3 in [43]):

Lemma 2.8 *Let K be an imaginary quadratic field, and let E be an elliptic curve defined over K, with equation (2.7). If $\mathfrak{Q}$ is an unramified prime in K dividing 2, then E has good reduction at $\mathfrak{Q}$ if and only if A and B satisfy one of the following conditions:*

1) $A \equiv -2\alpha^2 \bmod \mathfrak{Q}^3$ *and* $B \equiv \alpha^4 \bmod \mathfrak{Q}^3$, *or*

2) $A \equiv \alpha^2 \bmod \mathfrak{Q}^2$ *and* $B \equiv 0 \bmod \mathfrak{Q}^4$,

where $\alpha \in \mathcal{O}_K$ is coprime to $\mathfrak{Q}$.

If $\mathfrak{Q}$ is a ramified prime in K dividing 2, then E has good reduction at $\mathfrak{Q}$ if and only if A and B satisfy one of the following conditions:

1) $A \equiv -2\alpha^2 \bmod 8$ *and* $B \equiv \alpha^4 \bmod 8$, *or*

2) $A \equiv \alpha^2 \bmod 4$ *and* $B \equiv 0 \bmod 16$, *or*

3) $A \equiv 0 \bmod \mathfrak{Q}^5$, $B \equiv \pi^4 + 8\pi \bmod \mathfrak{Q}^8$ *and either* $\pi^2 A - B \equiv \pi^4 + \pi^6 \bmod \mathfrak{Q}^{10}$ *or* $\pi^2 A - B \equiv 5\pi^4 + 4\pi^5 + \pi^6 \bmod \mathfrak{Q}^{10}$,

where $\alpha \in \mathcal{O}_K$ and is coprime to $\mathfrak{Q}$, and π is a uniformizer at $\mathfrak{Q}$.

Let us introduce some notation. Let k be a number field, and $\mathcal{O}_k$ the ring of integers in k. If $\mathfrak{p}$ is a prime of $\mathcal{O}_k$, we denote by $N(\mathfrak{p})$ the cardinal of the finite field $\mathcal{O}_k/\mathfrak{p}$. For a modulus $\mathfrak{c}$ in k (for the definition of a modulus, see for example, Definition 3.2.1 in [6]), let $(\mathcal{O}_k/\mathfrak{c})^* = (\mathcal{O}_k/\mathfrak{c}_0)^* \times \mathbb{F}_2^{\mathfrak{c}_\infty}$. Let $I_\mathfrak{c}(k)$ be the group of fractional ideals in k coprime to $\mathfrak{c}_0$. Let $P_\mathfrak{c}$ be the set of all fractional principal ideals (α) of k, with $\alpha \in k^*$ such that $\mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{c}_0)$, for all $\mathfrak{p} \mid \mathfrak{c}_0$, and $\sigma_i(\alpha) > 0$ for all $\sigma_i \in \mathfrak{c}_\infty$. Let $k_\mathfrak{c}^*$ be the set of all such α. $P_\mathfrak{c}$ is a subgroup of $I_\mathfrak{c}$. Let $U(k)$ be the group of units in k, and $U_\mathfrak{c}(k) = U(k) \cap k_\mathfrak{c}^*$.The ray class group of $\mathfrak{c}$ is $Cl_\mathfrak{c}(k) = I_\mathfrak{c}(k)/P_\mathfrak{c}(k)$. Write $\mathfrak{c}_0 = \prod_{\mathfrak{p}|\mathfrak{c}_0} \mathfrak{p}^{a_\mathfrak{p}}$. Let $\phi(\mathfrak{c})$ be the cardinality

of $(\mathcal{O}_k/\mathfrak{c})^*$. Then $\phi(\mathfrak{c}) = 2^{|\mathfrak{c}_\infty|}\prod_{\mathfrak{p}|\mathfrak{c}_0} N(\mathfrak{p})^{a_\mathfrak{p}-1}(N(\mathfrak{p})-1)$. The cardinality of the ray class group $Cl_\mathfrak{c}(k)$ is finite. If we denote it by $h_\mathfrak{c}(k)$, then we have $h_\mathfrak{c}(k) = h_k \frac{\phi(\mathfrak{c})}{[U(k):U_\mathfrak{c}(k)]}$, where h_k is the class number of k (see Corollary 3.2.4 of [6]).

If L/k is a finite abelian extension of k, let $\mathfrak{f} = \mathfrak{f}_{L/k}$ be its conductor (see Definition 3.4.1 in [6]). Let $\mathfrak{c}$ be a suitable modulus for L/k (see Definition 3.4.2 in [6]). Let $\bar{C} = C/P_\mathfrak{c}(k)$ be the kernel of the Artin map $Cl_\mathfrak{c}(k) \longrightarrow \mathrm{Gal}(L/k)$ (see section 3.4.3 in [6] for a definition). Let $h_{\mathfrak{c},C} = |Cl_\mathfrak{c}(k)/\bar{C}|$. Then $h_{\mathfrak{c},C}$ divides $h_\mathfrak{c}$. On the other hand, $[L:k] = h_{\mathfrak{c},C}$ (Proposition 3.5.2 in [6]), hence, $[L:k]$ divides $h_\mathfrak{c}$.

If L/k is a cyclic extension of degree 3, unramified outside the primes in k that divide 2, including the primes at infinity, then its conductor is divisible only by primes in k that divide 2. Let $\mathfrak{f}$ be the conductor of L/k. Let $\mathfrak{p}$ be a prime in k that divides the conductor. It is a prime above 2. Let $\bar{C}$ be the kernel of the Artin map $Cl_\mathfrak{f}(k) \longrightarrow \mathrm{Gal}(L/k)$. Then $h_{\mathfrak{f},C} = [L:k] = 3$ (Proposition 3.5.2 in [6]). The conductor of the equivalence class of the congruence subgroup $(\mathfrak{f}, C)$ is equal to the conductor of L/k, which is $\mathfrak{f}$ (Proposition 3.4.6., (2) in [6]). Thus, we may conclude that $\mathrm{ord}_\mathfrak{p}(\mathfrak{f}) = 1$ (Proposition 3.3.21 in [6]). Therefore, (2) is a suitable modulus for any cyclic extension L/k of degree three unramified outside the primes of k that divide 2. So, if the ray class number $h_{(2)}(k)$ is coprime to 3, then k does not have any cyclic extension of degree 3 unramified outside the primes of k that divide 2.

If L/k is an abelian extension of degree 4, unramified outside the primes in k that divide 3, including the prime at infinity, then its conductor is divisible only by primes in k that divide 3. Let $\mathfrak{f}$ be the conductor of L/k. Let $\mathfrak{p}$ be a prime in k that divides the conductor. It is a prime above 3. Let $\bar{C}$ be the kernel of the Artin map $Cl_\mathfrak{f}(k) \longrightarrow \mathrm{Gal}(L/k)$. Then $h_{\mathfrak{f},C} = [L:k] = 4$ (Proposition 3.5.2 in [6]). Thus, we may conclude that $\mathrm{ord}_\mathfrak{p}(\mathfrak{f}) = 1$ (Proposition 3.3.21 in [6]). Therefore, (3) is a suitable modulus for any abelian extension L/k of degree 4 unramified outside the primes of k that divide 3. So, if the ray class number $h_{(3)}(k)$ is not divisible by 4, then k does not have any abelian extension of degree 4 unramified outside the primes of k that divide 3.

Lemma 2.9 *Let K be a number field. Let $\ell = 2$ or 3. Let $\mathfrak{p}$ be a prime in K not dividing ℓ. Let E be an elliptic curve defined over K with conductor $\mathfrak{p}$. Let $L = K(E[\ell])$ and $N = K(\Delta^{\frac{1}{\ell}})$. Then, $\Delta^{\frac{1}{\ell}} \in L$ and the extension L/N is unramified at the finite places outside ℓ.*

Proof. We know that $\Delta^{\frac{1}{\ell}} \in L$ (see Serre [41] page 305). We also know, by the Neron-Ogg-Shafarevitch criterion (Theorem 7.1 in [45]) that the extension L/K is unramified outside ℓ and $\mathfrak{p}$. We only need to show that the extension L/N is also unramified at $\mathfrak{p}$. For this, we use the theory of Tate curves (see Chapter V in [46]). Let $\mathfrak{Q}$ be a prime in L above $\mathfrak{p}$. Let $\mathfrak{q} = \mathfrak{Q} \cap \mathcal{O}_N$. Let $\gamma = -\frac{c_4}{c_6}$. There exists $q \in N_{\mathfrak{q}}^*$ with $\mathrm{ord}_{\mathfrak{q}}(q) > 0$ such that E is isomorphic over $M := N_{\mathfrak{q}}(\sqrt{\gamma})$ to the Tate curve E_q (see Theorem 5.3 and the comments just before Corollary 5.4 in [46]). Let $\Phi : \bar{M}^*/q^{\mathbb{Z}} \to E_q(\bar{M})$ be the p-adic uniformization (see Theorem 3.1 in [46]). It is an isomorphism which commutes with the Galois action. Let ζ be a primitive ℓ-th root of unity and $Q = q^{1/\ell}$. The isomorphism Φ induces an isomorphism $\Phi : (\zeta_\ell^{\mathbb{Z}} Q^{\mathbb{Z}})/q^{\mathbb{Z}} \xrightarrow{\sim} E_q[\ell]$. The discriminant of E_q is $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24}$ (see the proof of Theorem 3.1 in [46]). Hence $\Delta(q)^{1/\ell} = q^{1/\ell}\prod_{n\geq 1}(1-q^n)^{24/\ell}$. Since $\Delta^{1/\ell} \in M$, we deduce that $\Delta(q)^{1/\ell} \in M$, and so $q^{1/\ell} \in M$. The action of $\mathrm{Gal}(\bar{M}/M)$ on $E_q[\ell]$ and on $(\zeta^{\mathbb{Z}} \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}}$ are the same (see the proof of Proposition 6.1 in [46]). Thus $L_{\mathfrak{Q}}(\sqrt{\gamma}) = M(E_q[\ell]) = M(\zeta, q^{1/\ell}) = M(\mu_\ell)$. The extension $M(\mu_\ell)/M$ is unramified. The extension $N_{\mathfrak{q}}(\sqrt{\gamma})/N_{\mathfrak{q}}$ is also unramified (see Exercise 5.11 in [46]). Thus the extension L/N is unramified at $\mathfrak{p}$ as well. □

For elliptic curves with prime conductor that do not have any K-rational 2-torsion points, we have the following result:

Theorem 2.10 *Let K be a totally imaginary number field. Let $F_v = K(\sqrt{v})$, where v is a unit in K. Suppose that for any $v \in \mathcal{O}_K^*$, the ray class number $h_{(2)}(F_v)$ is coprime to 3. Let $\mathfrak{p}$ be a principal prime ideal of K not dividing 2. Let π be a generator of $\mathfrak{p}$. Let E be an elliptic curve defined over K, with discriminant $\Delta_{min} = u\pi^s$ and conductor $\mathfrak{f}(E/K) = \mathfrak{p}$.*

Let $L = K(E[2])$ and $N = K(\sqrt{\Delta})$. Suppose also that E has no K-rational 2-torsion points. Then

a) $\mathrm{Gal}(L/K) = S_3$

b) $N = K(\sqrt{u\pi})$

c) The extension L/N is unramified outside 2.

Proof.

c) This follows from lemma 2.9

b) Let $y^2 = f(x)$ be an equation of E/K over K. The 2-torsion points of E/K are of the form $(\alpha, 0)$, with $f(\alpha) = 0$. Thus $L = K(E[2])$ is the Galois group of the polynomial $f(x)$. Since E/K has no K-rational 2-torsion points, the polynomial $f(x)$ has no roots in K. Since it is of degree 3, it must be irreducible. Therefore, $\mathrm{Gal}(L/K) = S_3$ or A_3 and $\mathrm{Gal}(L/N) = A_3$ (see Corollary 12.4 and Theorem 13.1 in [30]). Thus, L/N is a cyclic extension of degree 3. Since $\Delta = u\pi^s$, N is either of the form as stated in b), or it is of the form $N = K(\sqrt{u})$. If $N = K(\sqrt{u})$, then the ray class number $h_{(2)}(N)$ is coprime to 3 by hypothesis, and N cannot have a cyclic extension of degree 3 unramified outside 2. But this contradicts c). Thus, N cannot be of the form $N = K(\sqrt{u})$. We conclude that N is of the form $N = K(\sqrt{u\pi})$.

a) We saw in the proof of b) that $f(x)$ is irreducible. If α is a root of $f(x)$, the extension $M = K(\alpha)$ is a subextension of L/K of degree 3. Since L/K also has a subextension of degree 2, namely N/K, by b), we deduce that $\mathrm{Gal}(L/K) = S_3$. □

Now, using the above theorem, we get the following result, which gives conditions in which any elliptic curve with prime conductor necessarily has a K-rational 2-torsion point:

Theorem 2.11 *Let K be a totally imaginary number field. Let $F_v = K(\sqrt{v})$, where v is a unit in K. Suppose that for any $v \in \mathcal{O}_K^*$, the ray class number $h_{(2)}(F_v)$ is coprime to 3. Let*

$\mathfrak{p} = (\pi)$ *be a principal prime ideal of* K *not dividing* 2. *Suppose that for any extension* N *of* K *of the form* $N = K(\sqrt{u\pi})$, *with* u *a unit in* K, *the ray class number* $h_{(2)}(N)$ *is coprime to* 3. *Then any elliptic curve over* K *with conductor* $\mathfrak{p}$ *must have a* K*-rational* 2*-torsion point.*

Proof. Suppose that E has no K-rational 2-torsion points. Then by Theorem 2.10, if Δ is the discriminant of E, then $N = K(\sqrt{\Delta})$ is of the form $N = K(\sqrt{u\pi})$ and $L = K(E[2])$ is a cyclic extension of degree 3 of N, unramified outside 2; however, by class field theory (see 2), such an extension cannot exist, since $h_{(2)}(N)$ is coprime to 3. Thus, E must have a K-rational 2-torsion point. □

Remark 2.12 Suppose K is an imaginary quadratic field with class number 1. The extensions $F_v = K(\sqrt{v})$, where v is a unit of K are:

a) $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_8)$ when $K = \mathbb{Q}(i)$.

b) K and $K(i)$ when $d = -2, -3, -7, -11, -19, -43, -67, -163$.

We have $h_{(2)}(\mathbb{Q}(i)) = h_{(2)}(\mathbb{Q}(\zeta_8)) = 1$. The table below gives the other values $h_{(2)}(F_v)$:

K	$\mathbb{Q}(\sqrt{2}i)$	$\mathbb{Q}(\sqrt{3}i)$	$\mathbb{Q}(\sqrt{7}i)$	$\mathbb{Q}(\sqrt{11}i)$	$\mathbb{Q}(\sqrt{19}i)$	$\mathbb{Q}(\sqrt{43}i)$	$\mathbb{Q}(\sqrt{67}i)$	$\mathbb{Q}(\sqrt{163}i)$
$h_{(2)}(K)$	2	1	1	3	3	3	3	3
$h_{(2)}(K(i))$	1	1	1	3	3	3	3	3

Thus theorem 2.11 can be used when $K = \mathbb{Q}(\sqrt{d})$, with $d = -1, -2, -3$ and -7.

Under the hypotheses of theorem 2.10, we note that $\mathrm{ord}_\pi(\Delta_{min})$ is odd. This need not be the case in general, as the following example shows.

Example 2.13 Let $K = \mathbb{Q}(\sqrt{-11})$, and $\theta = (1 + \sqrt{-11})/2$. The curve E/K given by the equation $y^2 + y = x^3 + (1-\theta)x^2 - x$ has no K-rational 2-torsion points, conductor $\mathfrak{f} = (5+2\theta)$ and discriminant $\Delta = (5 + 2\theta)^2$. We found this curve in Cremona's Table 3.6.3 in [9]. The ideal $(5 + 2\theta)$ is a prime ideal in $\mathcal{O}_K$ above 47. Here, the extension L/K, with $L = K(E[2])$, is a cyclic extension of degree 3, unramified outside 2. We have $L = K(\alpha)$, α a root of

$f(x) = x^3 + 4(1-\theta)x^2 - 16x + 16$. The extension L/K is cyclic of degree 3, has discriminant $\Delta_{L/K} = (4)$ and $h_{(2)}(K) = 3$.

We now study the elliptic curves with a K-rational 3-isogeny and prime conductor. Here, K will be an imaginary quadratic field with class number 1, distinct from $\mathbb{Q}(\sqrt{-3})$. We first mention a result by Pinch (Theorem 1.2 in [39]):

Theorem 2.14 *Let E and E' be elliptic curves that are 3-isogenous over K. Define the function $j(x) := \frac{(x+27)(x+3)^3}{x}$. Then the j-invariants $j = j(E)$ and $j' = j(E')$ of E and E' are given by $j = j(\tau)$ and $j' = j(\tau')$ where τ, $\tau' \in K$, and $\tau\tau' = 729 = 3^6$.*

We are now going to find the possible primes $\mathfrak{p} = (\pi)$ in K not dividing 3 for which there exists an elliptic curve E with conductor $\mathfrak{p}$ and a K-rational 3-isogeny. Here is the result:

Proposition 2.15 *Let $K = \mathbb{Q}(\sqrt{d})$, with $d = -1$, -2, -7, -11, -19, -43, -67 or -163. Let π be a prime in K not dividing 3. Let E/K be an elliptic curve over K with conductor (π). If E/K admits a K-rational 3-isogeny, then $(\pi) = (19)$, $(\sqrt{-19})$ or (37).*

For the proof, we need several lemmas. We use ideas of Takaaki Kagawa in [19]. Suppose E is an elliptic curve over K with prime conductor $\mathfrak{p} = (\pi)$ not dividing 3 and is given by a global minimal equation of the form (2.2). Its discriminant is $\Delta = u\pi^s$ for some $s \in \mathbb{N}^*$. If E/K has a K-rational 3-isogeny, we have

$$j = \frac{c_4^3}{\Delta} = \frac{(\tau+27)(\tau+3)^3}{\tau}, \tag{2.9}$$

with $\tau \in K$. Since E has good reduction outside $\mathfrak{p}$, and multiplicative reduction at $\mathfrak{p}$, we have that j is $\mathfrak{q}$-integral for all primes $\mathfrak{q}$ distinct from $\mathfrak{p}$, and $\mathrm{ord}_{\mathfrak{p}}(j) < 0$. We deduce that $\mathrm{ord}_{\mathfrak{q}}(\tau) \geq 0$ for all primes $\mathfrak{q}$ distinct from $\mathfrak{p}$, and that $\mathrm{ord}_{\mathfrak{p}}(\tau) \neq 0$. This is also true when τ is replaced by τ'. We can thus write τ and τ' in the form $\tau = \pi^m t, \tau' = \pi^n t'$, where t, $t' \in \mathcal{O}_K$ are integral and coprime to π, and m, $n \in \mathbb{Z} \setminus 0$. Since $\tau\tau' = 729 = 3^6$, we can deduce that $m = -n$. We can thus assume, without loss of generality, that $m = \mathrm{ord}_{\mathfrak{p}}(\tau) > 0$. In that case,

we can see that $\mathrm{ord}_{\mathfrak{p}}(j) = -\mathrm{ord}_{\mathfrak{p}}(\tau)$, so that $\mathrm{ord}_{\mathfrak{p}}(\tau) = \mathrm{ord}_{\mathfrak{p}}(\Delta)$. We can thus write $\Delta = u\pi^m$, where u is a unit. Note that in this case, if the elliptic curve E'/K is 3-isogenous over K to E/K, then it has discriminant Δ' with $\mathrm{ord}_{\mathfrak{p}}(\Delta') = 3m$. Indeed, $\mathrm{ord}_{\mathfrak{p}}(\tau') = -m < 0$. From the formula $j' = \frac{(\tau'+27)(\tau'+3)^3}{\tau'}$, we get $-\mathrm{ord}_{\mathfrak{p}}(\Delta') = \mathrm{ord}_{\mathfrak{p}}(j') = 3\mathrm{ord}_{\mathfrak{p}}(\tau') = -3m$.

Lemma 2.16 *The ideals (t) and (t') are sixth powers.*

Proof. To prove that (t) is a sixth power, we prove that (t) is a square and a cube. We have $j - 1728 = \frac{c_6^2}{\Delta}$. On the other hand, $j - 1728 = \frac{c_4^3}{\Delta} - 1728 = \frac{(\tau+27)(\tau+3)^3}{\tau} - 1728 = \frac{(\tau^2+18\tau-27)^2}{\tau}$. Thus, $\frac{c_6^2}{\Delta} = \frac{(\tau^2+18\tau-27)^2}{\tau}$. Since j is not integral, we have $j \neq 1728$, so that $c_6 \neq 0$. Therefore, $(t) = ((\tau^2 + 18\tau - 27)/c_6)^2$. This shows that (t) is a square. To show that (t) is a cube, we use the identity $\frac{c_4^3}{\Delta} = \frac{(\tau+27)(\tau+3)^3}{\tau}$. We get that $(t) = (\pi^m t + 27)((\tau + 3)/c_4)^3$. Since $tt' = 3^6$ and t and t' are integral, to show that (t) is a third power, we only need to show that for any prime $\mathfrak{p}$ dividing 3, $\mathrm{ord}_{\mathfrak{p}}(t) \equiv 0 \bmod 3$. Let $\mathfrak{p}$ be a prime dividing 3. If $\mathrm{ord}_{\mathfrak{p}}(t) = \mathrm{ord}_{\mathfrak{p}}(27) = 3\mathrm{ord}_{\mathfrak{p}}(3)$, we are done. If $\mathrm{ord}_{\mathfrak{p}}(t) > \mathrm{ord}_{\mathfrak{p}}(27)$, then the facts that $\mathrm{ord}_{\mathfrak{p}}((\tau + 27)/t) \equiv 0 \bmod 3$ and $\mathrm{ord}_{\mathfrak{p}}((\tau + 27)/t) = \mathrm{ord}_{\mathfrak{p}}(27) - \mathrm{ord}_{\mathfrak{p}}(t)$ implies also that $\mathrm{ord}_{\mathfrak{p}}(t) \equiv 0 \bmod 3$. If $\mathrm{ord}_{\mathfrak{p}}(t) < \mathrm{ord}_{\mathfrak{p}}(27)$, then $\mathrm{ord}_{\mathfrak{p}}(t') > \mathrm{ord}_{\mathfrak{p}}(27)$, so that $\mathrm{ord}_{\mathfrak{p}}(t') \equiv 0 \bmod 3$. The identity $tt' = 3^6$ implies then that $\mathrm{ord}_{\mathfrak{p}}(t) \equiv 0 \bmod 3$ as well. This finishes the proof of the fact that (t) is a cube. □

By the lemma above, we can assume that $t = v$ or $729v$, with v a unit, in the case where 3 is prime in K, which is the case when $K = \mathbb{Q}(\sqrt{d})$ for $d = -1, -7, -19, -43, -67, -163$. We can notice that in all these fields, all the units are cubes. When 3 splits (which is the case when $K = \mathbb{Q}(\sqrt{d})$ with $d = -2$ or -11), say as $3 = \pi_3\bar{\pi}_3$, then we can assume $t = v$, $\pi_3^6 v$ or $729v$, where v is a unit. If $t = v$, equation (2.9) gives $X^3 = v\pi^m + 27$ (where $X = (v/u)^{1/3}\frac{c_4}{\tau+3}$). If $t = v\pi_3^6$, then equation (2.9) gives $X^3 = v\pi_3^3\pi^m + \bar{\pi}_3^3$ (where $X = (v/u)^{1/3}\pi_3\frac{c_4}{\tau+3}$). If $t = 729v$, then equation (2.9) gives $X^3 = 27\pi^m v + 1$ (where $X = (v/u)^{1/3}\frac{3c_4}{\tau+3}$).

Thus, there is an elliptic curve with conductor (π) not dividing 3 admitting a K-rational 3-isogeny only if one of the equations $X^3 = v\pi^m + 27$ with $X = (v/u)^{1/3}\frac{c_4}{\tau+3}$, $X^3 = v\pi_3^3\pi^m + \bar{\pi}_3^3$ with $X = (v/u)^{1/3}\pi_3\frac{c_4}{\tau+3}$ or $X^3 = 27\pi^m v + 1$ with $X = (v/u)^{1/3}\frac{3c_4}{\tau+3}$, has a solution.

Lemma 2.17 *Let π be a prime of $K = \mathbb{Q}(\sqrt{d})$ not dividing 3, with $d = -1$, -2, -7, -11, -19, -43, -67, -163.*

a) If $(\pi) \neq (19)$, $(\sqrt{-19})$, (37) or $(26 \pm 9i)$, then the equations $X^3 = v\pi^m + 27$ and $X^3 = 27\pi^m v + 1$ have no solutions $X \in \mathcal{O}_K$, $v \in \mathcal{O}_K^*$, with $m > 0$.

When $K = \mathbb{Q}(i)$, $X = 3 \pm i$ is the only solution of $X^3 = \pi^m v + 27$, with $(\pi) = (26 \pm 9i)$ a prime dividing 757, and $m = 1$. Moreover, $X = 1 \pm 9i$ is the only solution of $X^3 = 27\pi^m v + 1$, with $\pi = (26 \pm 9i)$ a prime dividing 757, and $m = 1$.

b) If $K = \mathbb{Q}(\sqrt{d})$, with $d = -2$ or $d = -11$, then the equation $X^3 = \pi_3^3\pi^m v + \bar{\pi}_3^3$ has no solutions with $m > 0$.

Proof.

a) Assume X is a solution of $X^3 = \pi^m v + 27$. Then $(X - 3)(X^2 + 3X + 9) = v\pi^m$. We must then have $X - 3 = w\pi^n$ for some $n \leq m$, and $X^2 + 3X + 9 = vw^{-1}\pi^{m-n}$, where w is a unit. Substituting $X = 3 + w\pi^n$ in $X^2 + 3X + 9 = vw^{-1}\pi^{m-n}$, we get $\pi^{2n}w^2 + 9w\pi^n + 27 = vw^{-1}\pi^{m-n}$. If $n \neq 0$, we must have $n = m$. If $n = m$, we get $\pi^{2m}w^2 + 9w\pi^m + 27 = vw^{-1}$. But the equation $Y^2 + 9Y + 27 - vw^{-1} = 0$ has no solutions in $\mathcal{O}_K$. So there are no solutions when $n = m$. Suppose now that $n = 0$. We then have $w^2 + 9w + 27 = vw^{-1}\pi^m$. If $w = 1$, we get $37 = vw^{-1}\pi^m$. There is a solution only if 37 is a prime in K and $m = 1$. If $w = -1$, we get $19 = vw^{-1}\pi^m$, and there is a solution if 19 is a prime in K and $m = 1$, or 19 ramifies in K and $m = 2$. If $w = \pm i$, which happens only when $K = \mathbb{Q}(i)$, we get $26 \pm 9i = vw^{-1}\pi^m$. The norm of $26 \pm 9i$ is the prime 757. Thus $X = 3 \pm i$ is the only solution to $X^3 = \pi^m v + 27$ (with π dividing 757 and $m = 1$).

Assume now that X is a solution of $X^3 = 27\pi^m v+1$. Then $(X-1)(X^2+X+1) = 27\pi^m v$. We must then have $X-1 = w\pi_3^a\bar{\pi}_3^b\pi^n$ and $X^2+X+1 = vw^{-1}\pi_3^{3-a}\bar{\pi}_3^{(3-b)}\pi^{m-n}$. Since $X^2+X+1 = (X-1)^2+3X$, we must have that $a = b = 2$. We thus have $X-1 = 9w\pi^n$ and $X^2+X+1 = vw^{-1}3\pi^{m-n}$. Substituting $X = 1+9w\pi^n$ in the second equation, we get $81\pi^{2n}w^2+27w\pi^n+3 = 3\pi^{m-n}vw^{-1}$. If $n \neq 0$, we must have $n = m$. Suppose that $n = m$. Then $81\pi^{2m}w^2+27w\pi^m+3 = vw^{-1}3$. Putting $Y = 9\pi^m w$, we get $Y^2+3Y+3 = vw^{-1}3$. But the equation $Y^2+3Y+3-3vw^{-1} = 0$ has no solutions in $\mathcal{O}_K$ of the form $Y = 9c, c \in \mathcal{O}_K$. For $n = 0$, we get $81w^2+27w+3 = vw^{-1}3\pi^m$, which after simplifying becomes $27w^2+9w+1 = vw^{-1}\pi^m$. If $w = 1$, we get $37 = vw^{-1}\pi^m$ and there is a solution if 37 is prime in K. If $w = -1$, we get $19 = vw^{-1}\pi^m$, and there is a solution if 19 is a prime in K and $m = 1$ or 19 ramifies in K and $m = 2$. If $w = \pm i$, with $K = \mathbb{Q}(i)$, we get $-26 \pm 9i = vw^{-1}\pi^m$. There is a solution when π is a prime that divides 757 and $m = 1$. $X = 1 \pm 9i$ is a solution to $X^3 = 27\pi^m v+1$, with π a prime that divides 757, and $m = 1$.

b) Assume $K = \mathbb{Q}(\sqrt{-11})$. Assume X is a solution of $X^3 = \pi_3^3 v\pi^m + \bar{\pi}_3^3$. Then $(X-\bar{\pi}_3^3)(X^2+\bar{\pi}_3 X+\bar{\pi}_3^2) = \pm\pi_3^3\pi^m$. We must then have $X-\bar{\pi}_3 = w\pi_3^a\pi^n$ and $X^2+\bar{\pi}_3 X+\bar{\pi}_3^2 = \pm\pi_3^{3-a}\pi^{m-n}$. Since $X^2+\bar{\pi}_3 X+\bar{\pi}_3^2 = (X-\bar{\pi}_3)^2+3\bar{\pi}_3 X$, we must have $a = 2$. Substituting $X = \bar{\pi}_3+w\bar{\pi}_3^2\pi^m$ in $X^2+\bar{\pi}_3 X+\bar{\pi}_3^2$, we get $\pi_3^4\pi^{2n}+9w\pi_3\pi^n+3\bar{\pi}_3^2 = w\pi_3\pi^{m-n}$. If $n \neq 0$, then $n = m$. If $n = m$, we have $\pi_3^4\pi^{2m}+9w\pi_3\pi^m+3\bar{\pi}_3^2 = w\pi_3$ which has no solutions. If $n = 0$, we get $\pi_3^4+9w\pi_3+3\bar{\pi}_3^2 = w\pi_3\pi^m$. If $w = 1$, we get $\pi_3 = w\pi_3\pi^m$, which is impossible. If $w = -1$, we get $-17\pi_3 = w\pi_3\pi^m$, and this is possible only when $w = -1$, $\pi = 17$, $m = 1$. However, this is not a solution of the equation in the statement c). When $K = \mathbb{Q}(\sqrt{-2})$, there are no solutions as well. □

Lemma 2.18 *There are no elliptic curves over $\mathbb{Q}(i)$ with conductor dividing 757 admitting a K-rational 3-isogeny.*

Proof. Let π be a prime in $\mathbb{Q}(i)$ that divides 757. Write $\tau = \pi^m t$ and $\Delta = \pi^m u$. Assume first that $t = v$, so that X is a solution of $X^3 = \pi^m v + 27$. Then $(X-3)(X^2+3X+9) = v\pi^m$. We must then have $X - 3 = \pi^n w$ and $X^2 + 3X + 9 = vw^{-1}\pi^{m-n}$, where w is a unit. Since π is a prime above 757, from the proof of lemma 2.17, a), there is a solution only when $n = 0$ and $w = \pm i$. In that case, we get $\pi = -v\pi^m$ with $\pi = 26 \pm 9i$. We must then have $v = -1$ and $m = 1$. Thus, $\tau = -\pi$, $\Delta = \pi u$, $X = 3 + w = 3 \pm i$ and $X = (v/u)^{1/3}\frac{c_4}{\tau+3} = \frac{c_4}{u^{1/3}(\pi-3)} = \frac{c_4}{u^{1/3}(23\pm 9i)}$, so that $c_4^3 = ((3 \pm i)(23 \pm i))^3 u$. From equation (2.3), we get that $c_6^2 = (((3 \pm i)(23 \pm 9i))^3 - 1728(26 \pm 9i))u$, as can be checked by taking norms. But the righthand side is not a square.

Assume now that $t = 729v$, so that X is a solution of $X^3 = 27\pi^m v + 1$. Then $(X-1)(X^2+X+1) = v27 \cdot \pi^m$. We thus have $X - 1 = 9w\pi^n$ and $X^2 + X + 1 = vw^{-1}3\pi^{m-n}$. From the proof of lemma 2.17, a), there is a solution only when $n = 0$, $m = 1$ and $w = \pm i$. We get $\pi = -\pi v$, so that $v = -1$. Thus, $\tau = -729 \cdot \pi$, $\Delta = \pi u$, $X = 1 \pm 9i$ and $X = \frac{c_4}{u^{1/3}(729(-26\pm 9i)-3)}$, so that $c_4^3 = ((1 \pm 9i)(729(-26 \pm 9i) - 3))^3 u$. The equation (2.3) gives $c_6^2 = (c_4^3 - 1728(-26 \pm 9i)u$. But the right hand side is not a square. Thus, there are no elliptic curves with prime conductor dividing 757 admitting a K-rational 3-isogeny. □

We have that 19 is prime in $\mathbb{Q}(\sqrt{d})$ for $d = -1$, -7, -11, -43, -163, is ramified in $\mathbb{Q}(\sqrt{-19})$, and 37 is prime in $\mathbb{Q}(\sqrt{d})$, for $d = -2$, -19, -43, and -163.

Theorem 2.19 *Let $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$, -2, -7, -11, -19, -43, -67, -163.*

a) When K is such that 19 is prime in K (resp. $K = \mathbb{Q}(\sqrt{-19})$), the elliptic curves over K with conductor (19) (resp. $(\sqrt{-19})$) admitting a K-rational 3-isogeny are

$$\begin{aligned}
y^2 &= x^3 + 27 \cdot 32x - 54 \cdot 8, && \Delta_{min} = -19,\\
y^2 &= x^3 - 12096x - 544752, && \Delta_{min} = -19^3,\\
y^2 &= x^3 - 27 \cdot 36928x - 54 \cdot 7096328, && \Delta_{min} = -19,\\
y^2 &= x^3 - 979776x - 397124208, && \Delta_{min} = -19^3.
\end{aligned}$$

b) When 37 is prime in K, the elliptic curves with conductor 37 admitting a K-rational 3-isogeny are

$$\begin{aligned} y^2 &= x^3 - 27 \cdot 160x + 54 \cdot 2008, & \Delta_{min} = 37, \\ y^2 &= x^3 - 30240x - 1959984, & \Delta_{min} = 37^3, \\ y^2 &= x^3 - 27 \cdot 89920x - 54 \cdot 26964008, & \Delta_{min} = 37, \\ y^2 &= x^3 - 2449440x - 1428828336, & \Delta_{min} = 37^3. \end{aligned}$$

Proof. Notice that if an elliptic curve with equation (2.2) has invariants c_4 and c_6, then

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{2.10}$$

is also an equation for E/K (see [25] page 22). By corollary 2.15, to find the curves in the statement of the lemma, it suffices to solve the equations $X^3 = v\pi^m + 27$ with $X = (v/u)^{1/3}\frac{c_4}{\tau+3}$, and $X^3 = 27\pi^m v + 1$ with $X = (v/u)^{1/3}\frac{3c_4}{\tau+3}$.

a) If $\pi = 19$, write $\tau = 19^m t$ and $\Delta = 19^m u$. Assume first that $t = v$, so that X is a solution of $X^3 = 19^m v + 27$. Then $(X-3)(X^2+3X+9) = v19^m$. We must then have $X - 3 = 19^n w$ and $X^2 + 3X + 9 = vw^{-1}19^{m-n}$, where w is a unit. From the proof of lemma 2.17, *a*), there is a solution only when $n = 0$ and $w = -1$. In that case, we get $19 = -v\pi^m$. We must then have $v = -1$ and $m = 1$. Thus, $\tau = -19$, $\Delta = 19u$, $X = 3 + w = 2$ and $X = (v/u)^{1/3}\frac{c_4}{\tau+3} = \frac{c_4}{u^{1/3}16}$, so that $c_4^3 = 32^3 u$. From equation (2.3), we get that $c_6^2 = -64u$. If $d \neq -1$, we must have $u = -1$. In that case $c_4 = -32$ and $c_6 = \pm 8$. From [23], Proposition 1, Théorème 1 and 2, these values are the c_4 and c_6 invariants of an elliptic curve (2.2) only when $c_6 = 8$. The corresponding elliptic curve has discriminant -19. An equation of the form (2.10) for this elliptic curve is $y^2 = x^3 + 27 \cdot 32x - 54 \cdot 8$. This curve has only one K-rational cyclic subgroup of order 3, $V =< (12, 108) >$. Using formulas from [49], we can see that the corresponding elliptic curve E/V has equation $y^2 = x^3 - 12096x - 544752$. When $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-19})$, we get exactly the same elliptic curves. When $K = \mathbb{Q}(\sqrt{-19})$, the conductor is $(\sqrt{-19})$, and not (19).

Assume now that $\tau = 729v$, so that X is a solution of $X^3 = 2719^m v + 1$. Then $(X - 1)(X^2+X+1) = v27\cdot 19^m$. We thus have $X-1 = 9w\pi^n$ and $X^2+X+1 = vw^{-1}3\pi^{m-n}$. From the proof of lemma 2.17, a), there is a solution only when $n = 0$, $m = 1$ and $w = -1$. We get $19 = -19^m v$, so that $v = -1$. Thus, $\tau = -729 \cdot 19$, $\Delta = 19u$, $X = -8$ and $X = \frac{c_4}{u^{1/3}4616}$, so that $c_4^3 = -(8\cdot 4616)^3 u$. The equation (2.3) gives $c_6^2 = -(8\cdot 23\cdot 38567)^2 u$. Hence $u = -1$, $c_4 = 8 \cdot 4616$, and $c_6 = \pm 8 \cdot 23 \cdot 38567$. Again, by [23], these are the c_4 and c_6 invariant of an elliptic curve with prime conductor 19 only if $c_6 = 8 \cdot 23 \cdot 38567$. An equation for this elliptic curve is $y^2 = x^3 - 27 \cdot 8 \cdot 4616x - 54 \cdot 8 \cdot 23 \cdot 38567$. This curve has only one K-rational cyclic subgroup of order 3, $V =< (-576, 12\sqrt{-3}) >$. Using Vélu's formulas, we get an equation for E/V is $y^2 = x^3 - 979776x - 397124208$. When $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-19})$, we get exactly the same elliptic curves.

b) If $\pi = 37$, we have $\tau = 37^m t$ and $\Delta = 37^m u$. Assume $t = v$, so that X is a solution of $X^3 = 37^m v + 27$. Then $(X-3)(X^2+3X+9) = v37^m$. We must then have $X-3 = 37^n w$ and $X^2 + 3X + 9 = vw^{-1}37^{m-n}$, where w is a unit. From the proof of lemma 2.17, a), there is a solution only when $n = 0$ and $w = 1$. In that case, we get $37 = 37v$. We must then have $v = 1$ and $m = 1$. Thus, $\tau = 37$, $\Delta = 37u$, $X = 3 + w = 4$ and $X = (v/u)^{1/3}\frac{c_4}{\tau+3} = \frac{c_4}{u^{1/3}16}$, so that $c_4^3 = 160^3 u$. From equation (2.3), we get that $c_6^2 = (2008)^2 u$. If $d \neq -1$, we must have $u = 1$. In that case $c_4 = 160$ and $c_6 = \pm 2008$. From [23], Proposition 1, Théorème 1 and 2, these values are the c_4 and c_6 invariants of an elliptic curve (2.2) only when $c_6 = -2008$. The corresponding elliptic curve has discriminant 37. An equation of the form (2.10) for this elliptic curve is $y^2 = x^3 - 27 \cdot 160x + 54 \cdot 2008$. This curve has only one K-rational cyclic subgroup of order 3, $V =< (48, 108) >$. Using formulas from [49], we can see that the corresponding elliptic curve E/V has equation $y^2 = x^3 - 30240x - 1959984$. When $K = \mathbb{Q}(i)$, we get exactly the same elliptic curves.

Assume now that $\tau = 729v$, so that X is a solution of $X^3 = 2737^m v + 1$. Then $(X - 1)(X^2 + X + 1) = v27 \cdot 37^m$. We thus have $X - 1 = 9 \cdot 37^n w$ and $X^2 + X + 1 =$

$vw^{-1}3 \cdot 37^{m-n}$. From the proof of lemma 2.17, a), there is a solution only when $n = 0$, $m = 1$ and $w = 1$. We get $37 = 37v$, so that $v = 1$. Thus, $\tau = 729 \cdot 37$, $\Delta = 37u$, $X = 10$ and $X = \frac{3c_4}{u^{1/3}26976}$, so that $c_4^3 = 89920^3 u$. The equation (2.3) gives $c_6^2 = 2^6 \cdot 3370501^2 u$. Hence $u = 1$, $c_4 = 89920$, and $c_6 = \pm 8 \cdot 3370501$. Again, by [23], these are the c_4 and c_6 invariants of an elliptic curve with prime conductor 37 only if $c_6 = 8 \cdot 3370501$. An equation for this elliptic curve is $y^2 = x^3 - 27 \cdot 89920x - 54 \cdot 8 \cdot 3370501$. This curve has only one K-rational cyclic subgroup of order 3, $V =< (-900, 12\sqrt{-3}) >$. Using Vélu's formulas, we get an equation for E/V, $y^2 = x^3 - 2449440x - 1428828336$. When $K = \mathbb{Q}(i)$ we get exactly the same elliptic curves. □

We can now prove proposition 2.15:

Proof of proposition 2.15. By theorem 2.14, the j-invariant of an elliptic curve that admits a K-rational 3-isogeny is of the form 2.9. By the comments just before lemma 2.17, equation 2.9 can be transformed into one of the three equations considered in lemma 2.17. The result then follows from lemma 2.17 and lemma 2.18. □

We now give conditions under which an elliptic curve with prime conductor must necessarily have a K-rational three isogeny.

We quote the following theorem by Takaaki Kagawa (Lemma 10 in [19])

Theorem 2.20 *Let K be a number field not containing $\sqrt{-3}$. Let E be an elliptic curve defined over K, and Δ its discriminant. Let $L = K(E[3])$. Let $G = \mathrm{Gal}(L/K)$. Let $\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tau = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_3)$, which satisfy the relation $\rho^2 = \sigma^2 = \tau^8 = 1$, $\sigma\tau\sigma^{-1} = \tau^3$. Then*

a) G is conjugate in $GL_2(\mathbb{F}_3)$ to one of the following:

(i) $< \rho > \cong \mathbb{Z}/2\mathbb{Z}$.

(ii) $< -1 > \times < \rho > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iii) $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \cong S_3$.

(iv) $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \cong S_3$.

(v) $<\sigma, \tau^2> \cong D_8$.

(vi) $<\tau> \cong \mathbb{Z}/8\mathbb{Z}$.

(vii) $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$.

(viii) $<\sigma, \tau> \cong SD_{16}$

(ix) $GL_2(\mathbb{F}_3)$.

b) Δ is a cube in K if and only if G is conjugate in $GL_2(\mathbb{F}_3)$ to one of the groups in (i), (ii), (v), (vi) or (viii).

c) E admits a 3-isogeny defined over K if and only if G is conjugate in $GL_2(\mathbb{F}_3)$ to one of the groups in (i), (ii), (iii), (iv), or (vii).

Theorem 2.21 *Let K be a totally imaginary number field not containing $\sqrt{-3}$. Let $\mathfrak{p}$ be a principal prime ideal in $\mathcal{O}_K$, not dividing 3, and π a generator of $\mathfrak{p}$. Suppose that, for all $F_v = K(v^{1/3})$ with v a unit in K, the ray class number $h_{(3)}(F_v)$ is not divisible by 4. Let E be an elliptic curve defined over K with conductor $\mathfrak{p}$ and no K-rational 3-isogeny. Let $\Delta = u\pi^s$ be its minimal discriminant, where u is a unit in K. Let $L = K(E[3])$ and $N = K(\Delta^{\frac{1}{3}})$. Then*

a) $\mathrm{Gal}(L/K) \cong GL_2(\mathbb{F}_3)$.

b) $N = K((u\pi^{\epsilon})^{\frac{1}{3}})$, with $\epsilon = 1, 2$.

c) The extension L/N is unramified outside 3.

Proof.

c) This follows from lemma 2.9.

b) Since $\Delta = u\pi^s$, then, either N is of the form stated in b) or $N = K(u^{1/3})$, where u is a unit in K. The case $N = K(u^{1/3})$ happens when s is a multiple of 3. The discriminant of the elliptic curve E_N/N is then a cube in N. By theorem 2.20 b), $\mathrm{Gal}(L/N)$ must then be conjugate to one of (i), (ii), (v), (vi) or $(viii)$. If $N = K$, then $\mathrm{Gal}(L/N)$ is conjugate to one of (v), (vi) or $(viii)$, since E/K has no K-rational 3-isogeny and Δ is a cube in K. If $N \neq K$, then $[N : K] = 3$. If, in addition, $\mathrm{Gal}(L/N)$ is conjugate to the group in (i) (resp. (ii)), then $\#\mathrm{Gal}(L/N) = 2$ (resp. 4), and so $\mathrm{Gal}(L/K)$ must be conjugate to the group in (iii) or (iv) (resp. (vii)). Then, by theorem 2.20 c), E/K admits a K-rational 3-isogeny, contradicting the hypothesis on E/K. Hence, $\mathrm{Gal}(L/N)$ cannot be conjugate to the groups in (i) and (ii). Now, we know from c) that L/N is unramified outside 3. By hypothesis, the ray class number $h_{(3)}(N)$ is not divisible 4. Then, by class field theory, $\mathrm{Gal}(L/N)$ cannot be of the form (vi) (see 2). A group of the form (v) (resp. $(viii)$) has, as group of commutators, a group of order 2 (resp. 4) (see [15], pp $238 - 239$), so that it has a quotient which is abelian and of order 4. This implies that if $\mathrm{Gal}(L/N)$ is conjugate to a group of the form (v) or $(viii)$, then L/N has a subextension of degree 4 which is abelian. But again, by class field theory, such an extension of N cannot exist. We can thus conclude that s is not a multiple of 3. This implies that N is of the form as described in b).

a) By b), we have that $\#\mathrm{Gal}(L/K)$ is divisible by 3. Then, by a result of Serre (Proposition 15 in [41]), $\mathrm{Gal}(L/K)$ must either contain $SL_2(\mathbb{F}_3)$ or be contained in a Borel subgroup of $GL_2(\mathbb{F}_3)$. A Borel subgroup of $GL_2(\mathbb{F}_3)$ is a subgroup conjugate to a group of the form (vii) in theorem 2.20 (see section 2.3 in [41]). Thus, if $\mathrm{Gal}(L/K)$ is contained in a Borel subgroup, then it is conjugate in $GL_2(\mathbb{F}_3)$ to (i), (ii), (iii), (iv) or (vii) (see Proof

of Lemma 10 in [19]). In that case, by theorem 2.20 *c*), E/K admits a K-rational 3-isogeny, contradicting the hypotheses on E/K. Therefore, $\mathrm{Gal}(L/K)$ contains $SL_2(\mathbb{F}_3)$. It must then be all of $GL_2(\mathbb{F}_3)$. This follows from the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \stackrel{\rho}{\longrightarrow} & GL_2(\mathbb{F}_3) \\ Res \downarrow & & \downarrow det \\ \mathrm{Gal}(K(\mu_3)/K) & \stackrel{\kappa}{\longrightarrow} & \mathbb{F}_3^* \end{array}$$

Indeed, from the diagram, we get a surjective map $\mathrm{Gal}(L/K) \longrightarrow \mathbb{F}_3^*$. Since $SL_2(\mathbb{F}_3)$ is mapped to 1 by the map *det*, $\mathrm{Gal}(L/K)$ must be the whole of $GL_2(\mathbb{F}_3)$. The commutativity of the diagram is proved using the Weil pairing, $e_3 : E[3] \times E[3] \to \mu_3$ (see Chapter III, paragraph 8 in [45]). Let ζ_3 be a generator of μ_3. Let T_1, T_2 be a basis of $E[3]$ such that $e_3(T_1, T_2) = \zeta_3$. Such a basis exists and we have that $K(\mu_3) \subset L$ (see Corollary 8.1.1 in [45]). For $\sigma \in \mathrm{Gal}(L/K)$, write $\sigma(T_1) = aT_1 + bT_2$, $\sigma(T_2) = cT_1 + dT_2$. Using Proposition 8.1 in [45], we have

$$\begin{aligned} \sigma(\zeta_3) &= \sigma(e_3(T_1, T_2)) \\ &= e_3(\sigma(T_1), \sigma(T_2)) \\ &= e_3(T_1, T_2)^{ad-bc} \\ &= e_3(T_1, T_2)^{det(\rho(\sigma))} \\ &= \zeta_3^{det(\rho(\sigma))}. \end{aligned}$$

Thus, $\kappa \circ Res = det \circ \rho$. □

Corollary 2.22 *Let K be a totally imaginary number field not containing $\sqrt{-3}$. Let $\mathfrak{p}$ be a principal prime ideal in $\mathcal{O}_K$, not dividing 3, and π a generator of $\mathfrak{p}$. Suppose that, for all $F_v = K(v^{1/3})$ with v a unit in K, the ray class number $h_{(3)}(F_v)$ is not divisible by 4. Let E be an elliptic curve defined over K with conductor $\mathfrak{p}$ and no K-rational 3-isogeny. Let $\Delta = u\pi^s$ be its minimal discriminant, where u is a unit in K. Then $3 \nmid s$.*

Proof. By theorem 2.21, the extension $N = K(\Delta^{1/3})$ must be of the form $N = K((u\pi^\epsilon)^{1/3})$, with $\epsilon = 1$ or 2. Hence s cannot be divisible by 3. □

Theorem 2.23 *Let K be a totally imaginary number field not containing $\sqrt{-3}$. Suppose that for all $F_v = K(v^{1/3})$ with v a unit in K, the ray class number $h_{(3)}(F_v)$ is not divisible by 4. Let π be a prime of K not dividing 3. Suppose that for any extension $N = K((u\pi^\epsilon)^{\frac{1}{3}})$, with $\epsilon = 1$ or 2 and u a unit in K, the ray class number $h_{(3)}(N)$ is not divisible by 4. Then any elliptic curve over K with conductor (π) has a K-rational 3-isogeny.*

Proof. Suppose E has no K-rational 3-isogeny. Let $L = K(E[3])$. Let $\Delta = u\pi^s$ be the discriminant of E, where u is a unit. Then, by the previous theorem, $N = K((u\pi)^{\epsilon/3})$, with $\epsilon = 1$ or 2, $\mathrm{Gal}(L/K) \cong GL_2(\mathbb{F}_3)$ and the extension L/N is unramified outside 3. The discriminant of the elliptic curve E_N defined over N, is a cube in N. Since $L = N(E_N[3])$, and $\#\mathrm{Gal}(L/N) = 16$, we have, by theorem 2.20, that $\mathrm{Gal}(L/N) \cong SD_{16}$. Its group of commutators has order 4 (see [15] page 239). Therefore, the extension L/N has a subextension M/N which is an abelian extension of degree 4. But, by hypothesis, $h_{(3)}(N)$ is not divisible by 4. Hence, such an extension M/N cannot exist, by class field theory (see 2). Therefore, the elliptic curve E/K must have a K-rational 3-isogeny. □

Corollary 2.24 *Let $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$, -2, -7, -11, -19, -43, -67 or -163. Suppose that for all $F_v = K(v^{1/3})$ with v a unit in K, the ray class number $h_{(3)}(F_v)$ is not divisible by 4. Let π be a prime of K not dividing 3. Suppose that for any extension $N = K((u\pi^\epsilon)^{\frac{1}{3}})$, with $\epsilon = 1$ or 2 and u a unit in K, the ray class number $h_{(3)}(N)$ is not divisible by 4. If (π) is not (19), $(\sqrt{-19})$ or (37), then there are no elliptic curves over K with conductor (π).*

Proof. By theorem 2.23, any elliptic curve with prime conductor (π) must admits a K-rational 3-isogeny. By proposition 2.15, any elliptic curve with prime conductor not dividing 3 and K-rational 3-isogeny must have conductor (19), $(\sqrt{-19})$ or (37). Since (π) is not one of (19), $(\sqrt{-19})$ or (37), there are no elliptic curves over K with conductor (π). □

Remark 2.25 Suppose K is an imaginary quadratic field with class number 1, distinct from $\mathbb{Q}(\sqrt{-3})$. The extensions $F_v = K(v^{1/3})$, where v is a unit of K are K or $K(\sqrt{-3})$. The table

below gives the values of $h_{(3)}(F_v)$:

K	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{2}i)$	$\mathbb{Q}(\sqrt{7}i)$	$\mathbb{Q}(\sqrt{11}i)$	$\mathbb{Q}(\sqrt{19}i)$	$\mathbb{Q}(\sqrt{43}i)$	$\mathbb{Q}(\sqrt{67}i)$	$\mathbb{Q}(\sqrt{163}i)$
$h_{(3)}(K)$	2	2	4	2	4	4	4	4
$h_{(3)}(K(\sqrt{3}i))$	1	1	2	1	2	2	2	2

Thus, theorem 2.23 can be used when $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$, -2 and -11.

When studying the elliptic curves with prime conductor and K-rational 2-torsion points, we will see in the next chapters that we are led to study the equations $y^2 = x^{2r+1} - 64i$ for the case $K = \mathbb{Q}(i)$, $y^2 = wx^{2r+1} - 64$ for the case $K = \mathbb{Q}(\sqrt{-3})$ and $y^2 = x^{2r+1} - 64$ for the case $K = \mathbb{Q}(\sqrt{d})$ with $d = -2$, -7, -11, -19, -43, -67 or -163. Integral points with $(x, y) = (\pi, A)$, such that π is a prime and $A \in \mathcal{O}_K$ are the ones we are interested in. For example, if $(x, y) = (\pi, A)$ is a solution to the equation $y^2 = x^{2r+1} - 64i$, and A is a square modulo 4, then $y^2 = x^3 + Ax^2 - 16ix$ is an elliptic curve with prime conductor (π) and discriminant $\Delta = 2^{12}\pi^{2r+1}$.

If $x = \pi$ is a solution to the equation $y^2 = x^{2r+1} - 64i$ with $r > 0$, then the equation $y^2 = x^3 - 64i$ (resp. $y^2 = \pi x^3 - 64i$, $y^2 = \pi^2 x^3 - 64i$) has a solution as well, when $2r + 1 \equiv 0 \bmod 3$ (resp. $2r + 1 \equiv 1 \bmod 3$, $2r + 1 \equiv 2 \bmod 3$). Thus, to find whether there is an integral point (x, y) on $y^2 = x^{2r+1} - 64$ with $r > 0$ and $x = \pi$ a given prime, it suffices to study the three elliptic curves $y^2 = x^3 - 64i$, $y^2 = \pi x^3 - 64i$ and $y^2 = \pi^2 x^3 - 64i$. Similarly, when $K = \mathbb{Q}(\sqrt{d})$ with $d = -2$, -7, -11, -19, -43, -67 or -163, we would have to study the equations $y^2 = x^3 - 64$, $y^2 = \pi x^3 - 64$ and $y^2 = \pi^2 x^3 - 64$. For any given field K, we would like to know what possible values r can take so that the corresponding elliptic curves $y^2 = x^3 + Ax^2 - 16ux$, with $u = i$ when $d = -1$, and $u = 1$ when $d \neq -1$, has prime conductor. If $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$, -2 or -11, and if $(\pi) \neq (19)$, or (37), then $2r + 1$ cannot be a multiple of 3 by Corollary 2.22. Thus, in the cases $d = -1$, $d = -2$ and $d = -11$, it suffices to study the equations $y^2 = \pi x^3 - 64u$ and $y^2 = \pi^2 x^3 - 64u$, with $u = i$ if $d = -1$, and $u = 1$ if $d = -2$ or -11. Let E^{π} be the elliptic curve $y^2 = \pi x^3 - 64u$. Let E^{π^2} be the

elliptic curve $y^2 = \pi^2 x^3 - 64u$. Suppose π is a prime such that the Mordell-Weil ranks of E^{π} and E^{π^2} are 0 and that E^{π}_{tors} and $E^{\pi^2}_{tors}$ do not contain any point $(x, y) = (\pi, A)$ such that the corresponding curve $y^2 = x^3 + Ax^2 - 16ux$ has prime conductor (π). Then we can conclude that there are no elliptic curves with conductor (π) having a K-rational 2-torsion point.

Lemma 2.26 *a) Let $K = \mathbb{Q}(i)$. Let E/K be the elliptic curve $y^2 = x^3 - 64i$. Let π be a prime dividing a rational prime $p > 13$. Let E^{π^ϵ} be the elliptic curve $y^2 = \pi^\epsilon x^3 - 64i$, where $\epsilon = 1$ or 2. Then $E^{\pi^\epsilon}_{tors}(K) = 0$.*

b) Let $K = \mathbb{Q}(\sqrt{-2})$. Let E/K be the elliptic curve $y^2 = x^3 - 64$. Let π be a prime dividing a rational prime $p > 19$. Let E^{π^ϵ} be the elliptic curve $y^2 = \pi^\epsilon x^3 - 64i$, where $\epsilon = 1$ or 2. Then $E^{\pi^\epsilon}_{tors}(K) = 0$.

Proof.

a) Let $\pi_5 = 2 + i$. It is a prime above 5. Let $\pi_{13} = 3 + 2i$. It is a prime above 13. We have $i \equiv -2 \bmod \pi_5$ and $i \equiv 5 \bmod 13$. The elliptic curve E^{π^ϵ} has good reduction outside 2, 3 and π. Hence, it has good reduction at π_5 and π_{13}. The reduction of E^{π^ϵ} modulo π_5 (resp. π_{13}) is of the form $\tilde{E}^a_5 : y^2 = ax^3 + 3$ (resp. $\tilde{E}^a_{13} : y^2 = ax^3 + 5$). For all $a \in \mathbb{F}^*_5$, we have $\#(\tilde{E}^a_5) = 6$. For all $a \in \mathbb{F}^*_{13}$, we have $\#\tilde{E}^a_{13}) = 7$, 16 or 19. Hence $gcd(\#(\tilde{E}^a_5), \#(\tilde{E}^a_{13})) = 1$ or 2. Since E^{π^ϵ} has no K-rational 2-torsion points, we have that $E^{\pi^\epsilon}_{tors}$ is trivial.

b) Let π_{17} (resp. π_{19}) be a prime in $\mathbb{Q}(\sqrt{-2})$ above 17 (resp. 19). The elliptic curve E^{π^ϵ} has good reduction outside 2, 3 and π. Hence, it has good reduction at π_{17} and π_{19}. The reduction of E^{π^ϵ} modulo π_{17} (resp. π_{19}) is of the form $\tilde{E}^a_{17} : y^2 = ax^3 - 64$ (resp. $\tilde{E}^a_{19} : y^2 = ax^3 - 64$). For all $a \in \mathbb{F}^*_{17}$, we have $\#(\tilde{E}^a_{17}) = 18$. For all $a \in \mathbb{F}^*_{19}$, we have $\#\tilde{E}^a_{19}) = 13$, 19 or 28. Hence $gcd(\#(\tilde{E}^a_{17}), \#(\tilde{E}^a_{19})) = 1$ or 2. Since E^{π^ϵ} has no K-rational 2-torsion points, we have that $E^{\pi^\epsilon}_{tors}$ is trivial. □

Lemma 2.27 *Let $K = \mathbb{Q}(\sqrt{d})$ with $d = -1$ or -2. Let π be a prime of K distinct from 19 and 37. Suppose that π divides a prime $p > 13$ if $d = -1$, $p > 19$ if $d = -2$. Let E^{π^ϵ} be the elliptic curve $y^2 = \pi^\epsilon x^3 - 64u$, where $\epsilon = 1$ or 2 and $u = i$ when $d = -1$, $u = 1$ when $d = -2$. If the Mordell-Weil ranks of E^{π^ϵ}, for $\epsilon = 1$ and 2, are 0, then there are no elliptic curves of the form $y^2 = x^3 + Ax^2 - 16ux$ with prime conductor (π) and discriminant of the form $\Delta = \pm 2^{12}\pi^{2r+1}$.*

Proof. The elliptic curve $y^2 = x^3 + Ax^2 - 16ux$ has discriminant $\Delta = \pm 2^{12}(A^2 + 64u)$. Hence Δ is of the form $\Delta = \pm 2^{12}\pi^{2r+1}$ only if $A^2 + 64u = \pi^{2r+1}$, i.e., only if $(x, y) = (\pi, A)$ is a solution to the equation $y^2 = x^{2r+1} - 64u$. By Corollary 2.22, $2r + 1$ cannot be divisible by 3. Thus, if $y^2 = x^3 + Ax^2 - 16ux$ has conductor (π), then $(x, y) = (\pi, A)$ is a solution to the equation $y^2 = x^{2r+1} - 64u$ with $2r + 1 \equiv 1$ or 2 mod 3. In that case, the equations $y^2 = \pi x^3 - 64u$ or $y^2 = \pi^2 x^3 - 64u$ have a solution as well, which contradicts lemma 2.26, since these 2 elliptic curves have rank 0 by hypothesis. □

Lemma 2.28 *Let p be an odd rational prime that remains prime in $\mathbb{Q}(\sqrt{d})$, with $d = -3$, -7, -11, -19, -43, -67 or -163. If $d \neq -3$ or -11, then the equation $A^2 + 64 = up^{2r+1}$ has a solution only when $r = 0$, in which case A must be a rational integer. In $\mathbb{Q}(\sqrt{-3})$, the equation $A^2 + 64 = up^{2r+1}$ has solutions only when $p = 37$, for which the solutions are $A = \pm 3\sqrt{-3}$, $u = 1$, $r = 0$, or when p is of the form $p = a^2 + 64$. In $\mathbb{Q}(\sqrt{-11})$, the equation $A^2 + 64 = up^{2r+1}$ has solutions only when $p = 53$, for which the solutions are $A = \pm\sqrt{-11}$, $u = 1$, $r = 0$, or when p is of the form $p = a^2 + 64$.*

Proof. Let $A = \frac{1}{2}(a + b\sqrt{d})$, with $a, b \in \mathbb{Z}$ of same parity, be such that $A^2 + 64 = \pm p^{2r+1}$. We get $\frac{1}{4}(a^2 + db^2) + 64 + \frac{1}{2}ab\sqrt{d} = \pm p^{2r+1}$. The imaginary part of the lefthand side must then be 0. If $b = 0$, we have $(a/2)^2 + 64 = \pm p^{2r+1}$. This is possible only with the positive sign on the righthand side, so that $(a/2)^2 + 64 = p^{2r+1}$. There are solutions only when $r = 0$ (see [42], section 2.5). If $a = 0$, we get $\frac{d}{4}b^2 + 64 = \pm p^{2r+1}$. The case $\frac{d}{4}b^2 + 64 = p^{2r+1}$ has one solution only. Indeed, we must then have $b^2 \leq 256/(-d)$. Since $b \equiv 2$ mod 4, the only

cases are $b = \pm 2$ or $b = \pm 6$, and there is a solution only when $d = -3$ or -11. In the case $d = -3$, we must have $b = \pm 6$, which gives $A = \pm 3\sqrt{-3}$, $p = 37$, $u = 1$ and $r = 0$. In the case $d = -11$, we must have $b = \pm 2$, which gives $A = \pm\sqrt{-11}$, $u = 1$, $p = 53$, $r = 0$. The case $\frac{d}{4}b^2 + 64 = -p^{2r+1}$ has no solutions. To show this, we rewrite the equation in the form $(16 + b\sqrt{-d})(16 - b\sqrt{-d}) = -4p^{2r+1}$. The quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number one, its ring of integers is $\mathbb{Z}[\sqrt{-d}]$ and its fundamental unit has norm one.

Assume first that p is prime in $\mathbb{Q}(\sqrt{-d})$. Using valuation theory, we can see that $16+b\sqrt{-d}$ must be of the form $16 + b\sqrt{-d} = 2\epsilon p^{2r+1}$ or $16 + b\sqrt{-d} = 2\epsilon$. But $16 + b\sqrt{-d}$ cannot be equal to $2\epsilon p^{2r+1}$, since otherwise p^{2r+1} divides 16 (and b). Similarly, $16 + b\sqrt{-d}$ cannot be equal to 2ϵ, since otherwise, $16 - b\sqrt{-d} = -2\epsilon^{-1}p^{2r+1}$.

Assume now that p splits in $\mathbb{Q}(\sqrt{-d})$ as $p = \pi\bar{\pi}$. Using valuation theory, we can see that $16 + b\sqrt{-d}$ must be of the form $16 + b\sqrt{-d} = 2\epsilon\pi^{2r+1}$, $2\epsilon p^{2r+1}$, or $2\epsilon\bar{\pi}^{2r+1}$. We have already seen that $16 + b\sqrt{-d}$ cannot be equal to $2\epsilon p^{2r+1}$. The two other cases are similar, so we consider only $16 + b\sqrt{-d} = 2\epsilon\pi^{2r+1}$. In that case, we have $16 - b\sqrt{-d} = -2\epsilon^{-1}\bar{\pi}^{2r+1}$. But since $16 - b\sqrt{-d}$ is the conjugate of $16 + b\sqrt{-d}$, we must also have $16 - b\sqrt{-d} = 2\bar{\epsilon}\bar{\pi}^{2r+1}$. We must then have $-\epsilon^{-1} = \bar{\epsilon}$. But this is impossible in $\mathbb{Q}(\sqrt{-d})$, since all units have norm 1. $\square$

Chapter 3

Elliptic curves over $\mathbb{Q}(i)$

3.1 Main theorem

Let $K = \mathbb{Q}(i)$. We are interested in finding the elliptic curves over K whose conductor is a prime ideal not dividing 2 or 3 and having a K-rational 2-torsion point. We also find primes that cannot be conductors of elliptic curves over K. The following is the main result of this chapter:

Theorem 3.1 *Let p be a prime not equal to 2, 3, or 257. Let $\mathfrak{p}$ be a prime above p.*

a) Then, there is an elliptic curve with conductor $\mathfrak{p}$ and having a K-rational 2-torsion point if and only if, for some generator $\pi = u + iv$ of $\mathfrak{p}$, the equation $x^2 + 64i = \pi^{2r+1}$ has a solution $(A, r) \in \mathcal{O}_K \times \mathbb{N}$, such that $A^2 + 64i = \pi^{2r+1}$, where A is such that $A \equiv \pm 1 \bmod 4$ or $Ai \equiv \pm 1 \bmod 4$. For r fixed, there is at most one generator π of $\mathfrak{p}$ for which this is possible, and it must be such that u is odd and v is even.

There is a solution (A, r) such that $A^2 + 64i = \pi^{2r+1}$ only when $p \equiv 1 \bmod 8$. There is a solution (A, r) such that $A^2 + 64i = \pi^{2r+1}$ and $A \equiv \pm 1 \bmod 4$ or $Ai \equiv \pm 1 \bmod 4$ only if $p \equiv 1 \bmod 16$. When there is a solution for some $p \equiv 1 \bmod 16$, then one of the congruences $A \equiv \pm 1 \bmod 4$ or $Ai \equiv \pm 1 \bmod 4$ is automatically satisfied.

In the case $p \equiv 1 \bmod 16$, to each solution (A, r) with $A \equiv \pm 1 \bmod 4$, corresponds the following two isogenous curves with conductor $\mathfrak{p}$:

$$y^2 = x^3 + Ax^2 - 16ix, \qquad \Delta = -2^{12}\pi^{2r+1}, \tag{3.1}$$

$$y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x, \qquad \Delta = -2^{12}i\pi^{4r+2}, \tag{3.2}$$

while if $Ai \equiv \pm 1 \bmod 4$*, then the two corresponding isogenous curves, which are twists by* i *of the above, are:*

$$y^2 = x^3 + Aix^2 + 16ix, \qquad \Delta = 2^{12}\pi^{2r+1}, \tag{3.3}$$

$$y^2 = x^3 - 2Aix^2 - \pi^{2r+1}x, \qquad \Delta = 2^{12}i\pi^{4r+2}. \tag{3.4}$$

These two are the only elliptic curves with conductor (π)*,* K*-rational* 2*-torsion points and discriminant* Δ *such that* $\mathrm{ord}_\pi(\Delta) = 2r + 1$*.*

b) Let π *be a prime of* K*. If for any extension of the form* $N = K(\sqrt{\pi})$ *or* $K(\sqrt{\pi i})$*, the ray class number* $h_{(2)}(N)$ *is coprime to* 3*, then any elliptic curve over* K *with conductor* (π) *must have a* K*-rational* 2*-torsion point.*

c) Let π *be a prime in* K *such that* $(\pi) \neq (3)$ *and* (19)*. If for any extension of the form* $N = K(\pi^{\epsilon/3})$*, with* $\epsilon = 1$ *or* 2*, the ray class number* $h_{(3)}(N)$ *is not divisible by* 4*, then, there are no elliptic curves over* K *with conductor* (π)*.*

The table below indicates which primes p satisfy the conditions on $h_{(2)}$ of Theorem 3.1, and which satisfy the conditions on $h_{(3)}$:

$3 \nmid h_{(2)}$	$3 \nmid h_{(2)}, 4 \nmid h_{(3)}$	$4 \nmid h_{(3)}$
29,47,71,127,137,151	3,5,7,17,37,41,53	31,59,193,227,239,269
171,191,197,229,317,383	59,61,73,89,97,101,103	283,353,367,419,433,439
463,487,569,577,599,631	109,113,149,167,173,181,241	491,547,601,619,691,751
647,719,727,797,809,857	263,281,293,311,313,337,349	787,823
877,881,887,911,919,937	373,389,397,401,409,421,449	
941,967,991,997	457,461,479,521,541,557,593	
	607,613,617,641,653,661,673	
	701,709,761,769,773,821	

Remark 3.2 No examples of elliptic curves of the form (3.1) or (3.3) with $\mathrm{ord}_\pi(\Delta) \geq 3$ was found. In fact, no example of solutions to the equation $x^2 + 64i = \pi^{2r+1}$ with $r > 0$ was found.

Corollary 3.3 *a) There are no elliptic curves over* $\mathbb{Q}(i)$ *with prime conductor dividing* p*, for the following* 110 *values of* p *among the 168 prime numbers in* $[2, 1000]$*;* 2, 3, 5, 7, 13, 17, 29, 31, 37, 41, 47, 53, 59, 61, 71, 73, 89, 97, 101, 103, 109, 113, 127, 137, 149, 151, 167, 173, 181, 191, 193, 197, 227, 229, 239, 241, 263, 269, 271, 281, 283, 293, 311, 313, 317, 337, 349, 353, 367, 373, 383, 389, 397, 401, 409, 419, 421, 433, 439, 449, 457, 461, 463, 479, 487, 491, 521, 541, 547, 557, 569, 593, 599, 601, 607, 613, 617, 619, 631, 641, 647, 653, 661, 673, 691, 701, 709, 719, 727, 751, 761, 769, 773, 787, 797, 809, 821, 823, 829, 857, 877, 881, 887, 911, 919, 937, 941, 967, 991 *and* 997.

b) Any elliptic curve with prime conductor (π) *dividing* 577 *must have a* K*-rational* 2*-torsion point and discriminant* Δ *such that* $\mathrm{ord}_\pi(\Delta) > 1$.

Proof.

a) Let p be a prime appearing in the list a), and let π be a prime in K above p; we note first that there are no elliptic curves defined over K with conductor $(1+i)$ or (3) (see [37], where a list of all the elliptic curves defined over K with good reduction away from 2 is given in Table 2, page 34, and [25] where all the elliptic curves with good reduction outside $S = \{(1+i), (3)\}$ is given in the appendix). If $p \neq 2, 3$, $p \not\equiv 1 \bmod 16$, then p satisfies the conditions of theorem 3.1, part b) or c). Since $A^2 + 64i = \pi^{2r+1}$ has no solutions $A \in \mathcal{O}_K$ with $A \equiv \pm 1 \bmod 4$ or $Ai \equiv \pm 1 \bmod 4$ in this case, we conclude that there are no elliptic curves with conductor (π).

If $p \equiv 1 \bmod 16$ with $p \neq 881$, then $p \neq 19$ and satisfies the conditions of 3.1, part c). Hence, there are no elliptic curves with conductor (π).

For a prime π above 881, we use lemma 2.27. Let E^{π^ϵ} be the elliptic curve $y^2 = \pi^\epsilon x^3 - 64i$. Using a program by Denis Simon (see [47]), we see that these elliptic curves have rank 0. Thus, by lemma 2.27, there are no elliptic curves over K with K-rational 2-torsion points and prime conductor (π). Since the conditions in Theorem 3.1, b) are satisfied for π, any elliptic curve with conductor (π) must have a K-rational 2-torsion point. We conclude that there are no elliptic curves over K with prime conductor dividing 881.

b) This prime satisfies the conditions in Theorem 3.1 b). The first part of the statement b) follows from this. The claim about the discriminant follows from the tables at the end of this chapter. Indeed, from those tables, we deduce that there are no solutions to the equation $A^2 + 64i = \pi$ with π dividing 577. Thus, any elliptic curve with prime conductor (π) dividing 577 must have discriminant Δ such that $\mathrm{ord}_\pi(\Delta) > 1$. □

Remark 3.4 There exist elliptic curves over $\mathbb{Q}$ with prime conductor $p < 1000$ inert in K for $p = 11$, 19, 43, 67, 79, 83, 131, 139, 163, 179, 307, 331, 347, 359, 431, 443, 467, 503, 563, 571, 643, 659, 739, 811 and 827 (see [8]). Cremona's table 3.2.3 in [9] of elliptic curves over K with conductor of norm at most 500 exhibits additional curves with prime conductor π dividing $p = 233$, 257 and 277. Thus, in view of corollary 3.3, the question of the existence of an elliptic curve defined over K with prime conductor π dividing $p < 1000$ is open only for the 30 primes $p = 23$, 107, 157, 199, 211, 223, 251, 379, 499, 509, 523, 577, 587, 677, 683, 733, 743, 757, 839, 853, 859, 863, 883, 907, 929, 947, 953, 971, 977 and 983.

Proposition 3.5 *The elliptic curves of conductor a prime dividing* 257 *are given by*

$$y^2 = x^3 + (1 - 16i)x^2 - 16ix, \qquad \Delta = -2^{12}(1 + 16i)^2, \tag{3.5}$$

$$y^2 = x^3 + (1 + 8i)x^2 - 16x, \qquad \Delta = 2^{12}(1 + 16i), \tag{3.6}$$

$$y^2 = x^3 + (-2 - 64i)x^2 + x, \qquad \Delta = 2^{12}i(1 + 16i), \tag{3.7}$$

$$y^2 = x^3 - 2(1 - 16i)x^2 + (1 + 16i)^2x, \qquad \Delta = -2^{12}i(1 + 16i)^4, \tag{3.8}$$

and their conjugates. These four curves are isogenous over $\mathbb{Q}(i)$ *and only the first has all its* 2*-torsion points rational over* $\mathbb{Q}(i)$*.*

The proofs of Theorem 3.1 and Proposition 3.5 are given in section 3.4

3.2 Elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with prime conductor

We are now going to find solutions (A, B) of equation (2.8) such that the corresponding elliptic curves (2.7) have prime conductor not dividing 2 or 3. We denote $1+i$ by π_2 and the ideal (π_2) by $\mathfrak{p}_2$. The prime $\mathfrak{p}_2$ is the prime in $\mathbb{Q}(i)$ above 2. By lemma 2.5, a global minimal equation of the form (2.2) for our elliptic curve has coefficients a_1 and a_3 such that either $\mathrm{ord}_{\pi_2}(a_1) = 0$, or $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. We will show that, when $\mathrm{ord}_{\pi_2}(a_1) = 1$, any such elliptic curve does not have good reduction at π_2.

Lemma 3.6 *Let* $\alpha = a + bi$ *be an algebraic integer in* $\mathbb{Q}(i)$*, coprime to* π_2*. Then*

$$\begin{aligned} \alpha^2 &\equiv \pm 1 \mod 4, \\ -2\alpha^2 &\equiv \pm 2 \mod 8, \\ \alpha^4 &\equiv 1 \mod 8. \end{aligned}$$

Proof. First, since α is coprime to π_2, we must have that a and b have distinct parity. We have that $\alpha^2 = a^2 - b^2 + 2abi$. If a is even and b is odd, then $\alpha^2 \equiv -1 \bmod 4$ and $2\alpha^2 \equiv -2 \bmod 8$. If a is odd and b is even, then $\alpha^2 \equiv 1 \bmod 4$ and $2\alpha^2 \equiv 2 \bmod 8$. We have that $\alpha^4 = a^4 + 4a^3bi - 6a^2b^2 - 4ab^3i + b^4$. If a is even and b is odd, or vice-versa, then $\alpha^4 \equiv 1 \bmod 8$. □

To check whether an elliptic curve $y^2 = x^3 + Ax^2 + Bx$ with $A,\ B \in \mathcal{O}_K$, has good reduction at $\mathfrak{p}_2$, we use the following criterion, which is lemma 2.8 applied to the case of $K = \mathbb{Q}(i)$:

Lemma 3.7 *Let $K = \mathbb{Q}(i)$. The elliptic curve $y^2 = x^3 + Ax^2 + Bx$ with A, $B \in \mathcal{O}_K$, has good reduction at $\mathfrak{p}_2$ if and only if A and B satisfy the following conditions:*

1) $A \equiv \pm 2 \bmod 8$ and $B \equiv 1 \bmod 8$, or

2) $A \equiv \pm 1 \bmod 4$ and $B \equiv 0 \bmod 16$, or

3) $A \equiv 0 \bmod 4(1+i)$, $B \equiv 4 + 8i \bmod 16$ and $B - 2Ai \equiv 4 \pm 8i \bmod 32$.

Proof. We have that $\pi_2^5 = (1+i)^5 = -4(1+i)$, $\pi_2^8 = 16$, $\pi_2^{10} = 32i$, $\pi_2^4 + 8\pi_2 = -4 + 8(1+i) = 4 + 4i$, $\pi_2^4 + \pi_2^6 = -4 - 8i$, $5\pi_2^4 + 4\pi_2^5 + \pi_2^6 = -20 - 16(1+i) - 8i \equiv -4 + 8i \bmod 32$. The lemma then follows from the above computation, lemma 2.8 and 3.6. □

Remark 3.8 By lemma 2.6, the elliptic curves with prime conductor and a K-rational 2-torsion point have an equation of the form (2.7) with (A, B) satisfying equation (2.8). Whenever (A, B) is a solution of the equation (2.8), then $(-A, B)$ is also a solution. However, the corresponding elliptic curves $y^2 = x^3 + Ax^2 + Bx$ and $y^2 = x^3 - Ax^2 + Bx$ are isomorphic over K (this is true because -1 is a square and a sixth power in $K = \mathbb{Q}(i)$). In addition, if (A, B) is a solution with s odd, then $(Ai, -B)$ is a solution to $(-B)^2((Ai)^2 + 4B) = B^2(-A^2 + 4B) = -u2^8\pi^s$. The corresponding curves are $y^2 = x^3 + Ax^2 + Bx$ and $y^2 = x^3 + Aix^2 - Bx$, which are twists of each other.

Let E/K be an elliptic curve with prime conductor (π) not dividing 2 or 3. For a global minimal equation for E/K of the form (2.2), the discriminant is $\Delta_{min} = u\pi^s$. Suppose that for such an equation, the coefficient a_1 satisfies $\mathrm{ord}_{\pi_2}(a_1) = 0$. Then, by lemma 2.7, for an equation of the form (2.7), A and B cannot be simultaneously divisible by π_2 , nor by π. Also, such an equation has discriminant $\Delta = 16B^2(A^2 - 4B)$. Hence, A and B satisfy the equation $B^2(A^2 - 4B) = u2^8\pi^s$. We solve this equation in several steps:

a) Case where $u = \pm 1$ and s even.

b) Case where s odd.

c) Case where $u = \pm i$ and s even.

When $u = \pm 1$ and $s = 2r$, we have to consider the equation $B^2(A^2 - 4B) = \pm 2^8\pi^{2r}$. When s is odd, u can be absorbed in π^s, and so we only have to consider the equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$. When $u = \pm i$ and $s = 2r$, we have to consider the equation $B^2(A^2 - 4B) = \pm i2^8\pi^{2r}$.

Lemma 3.9 *The curves $y^2 = x^3+Ax^2+Bx$ with A and B not simultaneously divisible by π_2, that have prime conductor (π) not dividing 2 or 3 and discriminant of the form $\Delta = \pm 2^{12}\pi^{2r}$, are the curve (3.5) and its conjugate.*

Proof. We have $B^2(A^2 - 4B) = \pm 2^8\pi^{2r}$. Since ± 1 is a square in K, $A^2 - 4B$ is also a square in K, and so, the equation $X^3 + AX^2 + BX = 0$ has all its three roots in $\mathcal{O}_K$. Say 0, a and b are those three roots. Since the elliptic curve has multiplicative reduction at π, there is one simple root and one double root modulo π. By making a change of variables if necessary, we may assume that 0 is the simple root and so that $a \not\equiv 0 \bmod \pi$, $b \not\equiv 0 \bmod \pi$ and $a \equiv b \bmod \pi$. Then the equation (2.8) becomes

$$a^2b^2(a - b)^2 = \pm 2^8\pi^{2r}. \tag{3.9}$$

We have that $A = -a-b$ and $B = ab$. So, since π_2 cannot divide simultaneously A and B by lemma 2.7, it cannot divide simultaneously a and b as well. Furthermore, equation (3.9) shows that π_2 divides at least one of a or b. We may thus assume that $a = v\pi_2^8 = 16v$ and $b = w$, where v and w are units in K. The equation (3.9) then becomes $v^2w^2(16v - w)^2 = \pm\pi^{2r}$. The possible values for $16v - w$ are $\pm 16 \pm 1$, $\pm 16 \pm i$, $\pm 16i \pm 1$ and $\pm 16i \pm i$. Only $\pm 16i \pm 1$ and $\pm 16 \pm i$ are powers of primes; they are indeed primes. Hence, there are solutions only for $r = 1$ and $(v, w) = (\pm 1, \pm i)$ or $(\pm i, \pm 1)$. Thus, $(a, b) = (\pm 16, \pm i)$ or $(\pm 16i, \pm 1)$. Pairs of the form (a, b) and $(-a, -b)$ correspond to isomorphic elliptic curves, and for each such pair

we record only one equation. Thus, the corresponding elliptic curves are:

$$y^2 = \quad x^3 + (1 - 16i)x^2 - 16ix, \quad \Delta = -2^{12}(1 + 16i)^2, \tag{3.10}$$

$$y^2 = \quad x^3 + (16 + i)x^2 + 16ix, \quad \Delta = 2^{12}(16 - i)^2, \tag{3.11}$$

and their conjugates. Using lemma 3.7, we can see that equation (3.10) has good reduction at $\mathfrak{p}_2$, and (3.11) does not. The curve (3.10) is the elliptic curve (3.5). □

Remark 3.10 The curve (3.5) is of the form $y^2 = x^3 + Ax^2 + Bx$, with $B = -16i$ and $A^2 + 64i = -(1 + 16i)^2$. Its conjugate is of the form $y^2 = x^3 + ax^2 + bx$, with $b = 16i$ and $a^2 - 64i = -(1 - 16i)^2$. Let $u = \pm i$. From lemma 3.9, we deduce that the only elliptic curves of the form $y^2 = x^3 + Ax^2 + 16ux$ with prime conductor (π) not dividing 2 or 3 such that $A^2 + 64u = \pm\pi^{2r}$ are the curve (3.5) and its conjugate.

Now, when s is odd, u can be absorbed in π^s so that we may just consider the equation:

$$B^2(A^2 - 4B) = 2^8\pi^{2r+1}.$$

We can also see that π cannot divide B. Indeed, if π divides B, then it must also divide $A^2 - 4B$, and, hence, it must also divide A; but this contradicts the fact that it cannot divide simultaneously A and B. We already know that π_2 cannot divide simultaneously A and B.

Lemma 3.11 *The elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with A and B not simultaneously divisible by π_2, that have prime conductor (π) not dividing 2 or 3, discriminant of the form $\Delta = 2^{12}\pi^{2r+1}$ and such that π_2 divides B are the curve (3.6) and its conjugate, the curves (3.1), (3.3) and their conjugates.*

Proof. We have $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$. If $\pi_2 \mid B$, then $\pi_2 \nmid A$ and so $\pi_2 \nmid (A^2 - 4B)$ and $\mathrm{ord}_{\pi_2}(B) = 8$. So $B = \pi_2^8 v = 16v$, and the equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ becomes, after simplification, $v^2(A^2 - 64v) = \pi^{2r+1}$. By remark 3.8, it suffices to consider only the cases $v = 1$ and $v = i$.

If $v = 1$, then $B = 16$, and the equation becomes $A^2 - 64 = \pi^{2r+1}$ which can be rewritten as $(A - 8)(A + 8) = \pi^{2r+1}$. But π cannot divide simultaneously $A - 8$ and $A + 8$. So, if π divides one of them, then the other is a unit. Thus, it suffices to find A such that $A - 8 = w$ or $A + 8 = w$, with w a unit and $A^2 - 64 = \pi^{2r+1}$. We consider only $A - 8 = w$ (the case $A + 8 = w$ produces elliptic curves that are isomorphic to those that come from $A - 8 = w$). If $w = 1$, we get $A = 9$ and $A^2 - 64 = 17$. Since 17 is not a prime, $A = 9$ is not a solution. If $w = -1$, we get $A = 7$ and $A^2 - 64 = -15$. Since 15 is not a prime, $A = 7$ is not a solution. If $w = \pm i$, we get $A = 8 \pm i$ and $A^2 - 64 = -1 \pm 16i$, which is a prime in K above 257. The corresponding elliptic curves are:

$$y^2 = x^3 + (8 - i)x^2 + 16x, \qquad \Delta = -2^{12}(1 + 16i), \tag{3.12}$$

$$y^2 = x^3 + (8 - i)ix^2 - 16x, \qquad \Delta = 2^{12}(1 + 16i). \tag{3.13}$$

and their conjugates. The first curve does not have good reduction at $\mathfrak{p}_2$, while the second does have good reduction at $\mathfrak{p}_2$ by lemma 3.7. We can also see that the curve (3.13) is the elliptic curve (3.6).

The case of $v = i$ leads to the equation

$$A^2 + 64i = \pi^{2r+1} \tag{3.14}$$

whose solutions correspond to the elliptic curves $y^2 = x^3 + Ax^2 - 16ix$ and $y^2 = x^3 + Aix^2 + 16ix$. One of these elliptic curves have prime conductor (π) by lemma 3.24. The first (resp. second) curve is the elliptic curve (3.1) (resp. (3.3)). □

We will devote later a section to the equation (3.14). We will give necessary conditions on π for this equation to have solutions, and sufficient conditions so that there are no solutions. We will also give necessary and sufficient conditions for the elliptic curves that correspond to the solutions of this equation to have good reduction at π_2.

Lemma 3.12 *The elliptic curves $y^2 = x^3+Ax^2+Bx$ with prime conductor (π), discriminant $\Delta = 2^{12}\pi^{2r+1}$ and such that $\pi_2 \nmid B$ are the curve (3.7) and its conjugate.*

Proof. Suppose π_2 does not divide B. Then $B = v \in \mathcal{O}_K^*$ and the equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ becomes $v^2(A^2 - 4v) = 2^8\pi^{2r+1}$. We can see that A must be of the form $A = 2C$. Then, the equation becomes $v^2(C^2 - v) = 64\pi^{2r+1}$.

If $v = 1$, then $B = 1$ and the equation becomes $C^2 - 1 = 64\pi^{2r+1}$, which can be rewritten as $(C-1)(C+1) = 2^8\pi^{2r+1}$. We can see that π divides one and only one of $C-1$ and $C+1$. On the other hand $\mathrm{ord}_{\pi_2}(C-1) + \mathrm{ord}_{\pi_2}(C+1) = 12$. Since $\mathrm{ord}_{\pi_2}(2) = 2$ and $C+1 = C-1+2$, we must have $\mathrm{ord}_{\pi_2}(C-1) \geq 2$. So, either $\mathrm{ord}_{\pi_2}(C-1) = 2$ and $\mathrm{ord}_{\pi_2}(C+1) = 10$, or $\mathrm{ord}_{\pi_2}(C-1) = 10$ and $\mathrm{ord}_{\pi_2}(C+1) = 2$. Thus $C+1$ (or $C-1$) is twice a unit or 32 times a unit. We consider only the cases $C+1 = 2w$ or $C+1 = 32w$ (the case $C-1 = 2w$ or $C-1 = 32w$ produces isomorphic elliptic curves). Suppose first that $C+1 = 2w$. Then $(C-1)(C+1) = (2w-2)2w = 4w(-1+w)$, which cannot possibly be a multiple of 64. Suppose now that $C+1 = 32w$. Then $(C-1)(C+1) = (32w-2)32w = 64w(-1+16w)$. But $-1+16w$ is the odd power of a prime only if $w = \pm i$. In that case we get $C = -1 \pm 32i$ and the corresponding elliptic curves are $y^2 = x^3 - (2+64i)x^2 + x$ and $y^2 = x^3 - (2+64i)ix^2 - x$ and their conjugates. Using lemma 3.7, we can see that the first curve has good reduction at $\mathfrak{p}_2$, while the other does not. The first curve is the elliptic curve (3.7).

Now, if $v = i$, then $B = i$ and the corresponding equation becomes $-C^2 + i = 64\pi^{2r+1}$. Putting $C = x + iy$, we get $-x^2 + y^2 + (-2xy + 1)i = 64\pi^{2r+1}$. The lefthand side has odd imaginary part while the righthand side has even imaginary part. Hence, there are no solutions when $v = i$. □

The following lemma will be useful:

Lemma 3.13 *Let $\pi = u + iv$ be a prime above some odd prime of $\mathbb{Q}$. Then the real part of π^{2r} is always odd and the imaginary part is always even.*

Proof. We know that u and v have distinct parity. Hence, the real part of $\pi^2 = u^2 - v^2 + 2uvi$ is odd and the imaginary part is even. Suppose that for some even number n, the real part u_n of $\pi^n = u_n + iv_n$ is odd. We show that the real part of π^{n+2} is also odd and the imaginary part is even. Indeed, writing $\pi^2 = u_2 + iv_2$, we have seen that then u_2 is odd, while v_2 is even. We have that $\pi^{n+2} = \pi^n\pi^2 = (u_n + iv_n)(u_2 + iv_2) = u_nu_2 - v_nv_2 + i(u_nv_2 + v_nu_2)$, whose real part is also odd and imaginary part is even. □

Lemma 3.14 *The elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with A and B not simultaneously divisible by π_2, that have prime conductor (π) not dividing 2 and 3, and discriminant of the form $\Delta = \pm i2^{12}\pi^{2r}$ are the curve (3.8), and (3.2) or (3.4).*

Proof. Let $u = \pm i$. We have $B^2(A^2 - 4B) = u2^8\pi^{2r}$. There are four possibilities: the first is $B = w$, the second is $B = \pi_2^8 w = 16w$, the third is $B = \pi^r w$, and the last is $B = \pi_2^8\pi^r w = 16\pi^r w$.

If $B = w$ is a unit, then $w^2(A^2 - 4B) = u2^8\pi^{2r}$. We can see that A must be of the form $A = 2C$ for some C in $\mathcal{O}_K$ not divisible π_2. The equation becomes $w^2(C^2 - w) = 64u\pi^{2r}$. Write $C = x + yi$. If $w = \pm i$, the equation becomes $-(x^2 - y^2 + (2xy \pm 1)i) = 64u\pi^{2r}$. The lefthand side has odd imaginary part, while the righthand side has even imaginary part, so there are no solutions in this case. If $w = \pm 1$, the equation becomes $C^2 \pm 1 = 64u\pi^{2r}$. It suffices to solve the equation $C^2 + 1 = 64\pi^{2r}u$, by remark 3.8. The equation $C^2 + 1 = 64u\pi^{2r}$ can be rewritten as $(C + i)(C - i) = 64u\pi^{2r}$. Here too, π cannot divide $C + i$ and $C - i$ simultaneously. We also have that $\mathrm{ord}_{\pi_2}(C + i) = 2$ or 10. Thus $C + i = 2t$, $C + i = 32t$, $C - i = 2t$ or $C - i = 32t$, where t is a unit. It suffices to consider only the first two cases, since the last two would produce isomorphic curves to the curves produced by the first two. If $C + i = 2t$, then $(C + i)(C - i) = 2t(2t - 2i) = 4t(t - i)$ which cannot be a multiple of 64. If $C + i = 32t$, then $(C + i)(C - i) = 32t(32t - 2i) = 64t(16t - i)$. But $(16t - i)t$ cannot be of the form $u\pi^{2r}$ where π is a prime. Thus, there are no solutions when $B = w$ is a unit.

Suppose now that $B = 16w$. Then the equation becomes $w^2(A^2 - 64w) = u\pi^{2r}$. This equation has no solutions since the imaginary part of the lefthand side is even, while that of the righthand side is odd, by lemma 3.13.

Suppose now that $B = w\pi^r$. Then π does not divide A and $\mathrm{ord}_{\pi_2}(A^2 - 4B) = 16$, so that $\mathrm{ord}_{\pi_2}(A) = 2$. Therefore, A can be written as $A = 2C$, with $C \in \mathcal{O}_K$. The equation becomes $w^2(C^2 - w\pi^r) = 64u$. We first consider the case of r even, say $r = 2t$. If $w = \pm 1$, then $C^2 - 64u = \pm\pi^{2t}$ and the corresponding elliptic curve is

$$y^2 = x^3 + 2Cx^2 + \pi^{2t}x. \tag{3.15}$$

Notice that this elliptic curve is 2-isogenous to the curve $y^2 = x^3 + Cx^2 - 16ux$. By remark 3.10, there are only two such curves with prime conductor not dividing 2 or 3, the curve (3.5) and its conjugate. Hence, the curve (3.15) has to be $y^2 = x^3 - 2(1-16i)x^2 + (1+16i)^2x$ which is (3.8), or its conjugate. Consider now the case of $w = \pm i$. The equation is then $-C^2 + w\pi^{2t} = 64u$. But the imaginary part of the righthand side is even, while that of the lefthand side is odd by lemma 3.13. Hence, there are no solutions in this case. Let us now consider the case of $r = 2t+1$. Then $B = w\pi^{2t+1}$. But since w can be absorbed in π^{2t+1}, we can consider only the case $B = \pi^{2t+1}$. The equation then becomes $C^2 - \pi^{2t+1} = 64u$, which can be rewritten as $C^2 - 64u = \pi^{2t+1}$. The corresponding elliptic curves are:

$$y^2 = x^3 + 2Cx^2 + \pi^{2t+1}x. \tag{3.16}$$

We can notice that this elliptic curve is 2-isogenous to $y^2 = x^3 + Cx^2 + 16u$. This is an elliptic form of the form (3.1) or (3.3). Thus, (3.16) is the curve (3.2) or (3.4).

Finally, if $B = 16w\pi^r$, the equation becomes, after simplifications, $A^2 - 16w\pi^r = uw^{-2}$, which has no solutions, since the lefthand side has even imaginary part, which is not the case for the righthand side. □

Let us now consider the case $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. Let E/K be an elliptic curve over K with equation (2.2) that has a K-rational 2-torsion point. Suppose that

$\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. We will show that such an elliptic curve cannot have good reduction at π_2. For this, we will consider an equation for E/K of the form $y^2 = x^3+Ax^2+Bx$. It will turn out that $\mathrm{ord}_{\pi_2}(A) > 4$ and $\mathrm{ord}_{\pi_2}(B) = 4$ and in that case, the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ cannot have good reduction at π_2.

We have that $\mathrm{ord}_{\pi_2}(b_2) = 2$, $\mathrm{ord}_{\pi_2}(b_4) = 1$ and $\mathrm{ord}_{\pi_2}(b_6) = 0$. Then, the Newton polygon of the polynomial $x^3 + b_2x^2 + 8b_4x + 16b_6$ has two segments, the first of length 2 and slope -3, the second of length 1 and slope -2. Hence, if $t \in \mathcal{O}_K$ is a root of that polynomial, then $\mathrm{ord}_{\pi_2}(t) = 2$ or 3. We show however that the case $\mathrm{ord}_{\pi_2}(t) = 3$ is not possible.

Suppose that $t^3 + b_2t^2 + 8b_4t + 16b_6 = 0$ with $\mathrm{ord}_{\pi_2}(t) = 3$. Then $t^3 + 8b_4t = -b_2t^2 - 16b_6$. The left hand side has valuation 9, hence, the righthand side should also have that same valuation. We need the following lemma.

Lemma 3.15 *An element $x + yi$ of $\mathbb{Z}[i]$ is divisible by $1 + i$ if and only if $x \equiv y \bmod 2$. It is exactly divisible by $1 + i$ if and only if x and y are odd.*

Proof. Write $x + yi = (a + bi)(1 + i)$. Then $x + yi = a - b + (a + b)i$, so that $x = a - b$ and $y = a + b$. Solving for a and b, we get $a = (x + y)/2$ and $b = (-x + y)/2$. Thus, $1 + i$ divides $x + yi$ in $\mathbb{Z}[i]$ if and only if x and y have the same parity, and it divides exactly $x + yi$ if and only if x and y are odd. □

We can now show that $\mathrm{ord}_{\pi_2}(t)$ cannot be equal to 3.

Lemma 3.16 *Suppose $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. Then a solution t to the equation $x^3 + b_2x^2 + 8b_4x + 16b_6 = 0$ cannot have valuation 3 at the prime π_2.*

Proof. We have that $t^3+8b_4t = -b_2t^2-16b_6$. It $\mathrm{ord}_{\pi_2}(t) = 3$, then $\mathrm{ord}_{\pi_2}(t^3+8b_4t) = 9$, while the two terms of the righthand expression have valuation 8. We show that the righthand expression does not have valuation 9, which will prove that t cannot possibly have valuation 3. We use the fact that $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. This means that the real and imaginary parts of a_1 are odd, while those of a_3 have distinct parity. Thus, $a_1^2 = 2(\alpha+i\beta)$, with α

even, and β odd, while, since $b_6 = a_3^2 + 4a_2$, we have that $b_6 = \gamma + i\delta$ with γ odd and δ even. Now, since $\mathrm{ord}_{\pi_2}(t) = 3$, we have that $t = 2i(1+i)(a+bi)$, where a and b have distinct parity, and so $t^2 = -8i(a^2 - b^2 + 2abi) = 8(\epsilon + i\zeta)$, where ϵ is even and ζ is odd. We can now write $b_2t^2+16b_6 = 16(\alpha+i\beta+2a_2)(\epsilon+i\zeta)+16\gamma+16i\delta = 16(\alpha\epsilon-\beta\zeta+\gamma+(\alpha\zeta+\beta\epsilon+\delta)i+2a_2(\epsilon+i\zeta))$. We have that $\alpha\epsilon - \beta\zeta + \gamma$ and $\alpha\zeta + \beta\epsilon + \delta$ are even so that $b_2t^2 + 16b_6$ cannot possibly have valuation 9. Thus, the case $\mathrm{ord}_{\pi_2}(t) = 3$ is impossible. □

As already seen, the change of variable $x = X + t$ and $y = Y$ leads to the equation (2.7) $Y^2 = X^3 + AX^2 + BX$ for the elliptic curve, with $A = b_2 + 3t$ and $B = 8b_4 + 2b_2t + 3t^2$. So, since $\mathrm{ord}_{\pi_2}(t) = 2$, then $\mathrm{ord}_{\pi_2}(B) = 4$ and $\mathrm{ord}_{\pi_2}(A) > 4$. The fact that $\mathrm{ord}_{\pi_2}(A) > 4$ is the one that is not obvious. Since $B^2(A^2 - 4B) = u2^8\pi^s$, and $\mathrm{ord}_{\pi_2}(B) = 4$, we must have $\mathrm{ord}_{\pi_2}(A^2 - 4B) = 8$. Hence, we must have $\mathrm{ord}_{\pi_2}(A) \geq 4$. If $\mathrm{ord}_{\pi_2}(A) = 4$, we can write $A = 4(\alpha + \beta i)$, with α and β integers of distinct parity, by lemma 3.15. By the same lemma, we can write $B = 4(\epsilon + \delta i)$, with ϵ and δ integers of distinct parity. Then, $A^2 - 4B = 16(\alpha^2 - \beta^2 - \epsilon + (2\alpha\beta - \delta)i)$. But, since $\alpha^2 - \beta^2 - \epsilon$ and $2\alpha\beta - \delta$ have same parity, we cannot have $\mathrm{ord}_{\pi_2}(A^2 - 4B) = 8$. Therefore, $\mathrm{ord}_{\pi_2}(A) > 4$.

Lemma 3.17 *Any elliptic curve of the form* $y^2 = x^3 + Ax^2 + Bx$, *with* $\mathrm{ord}_{\pi_2}(A) > 4$ *and* $\mathrm{ord}_{\pi_2}(B) = 4$, *does not have good reduction at* $\mathfrak{p}_2$.

Proof. Dividing by π_2^6 gives the new equation $y^2 = x^3 + ax^2 + bx$, with $\mathrm{ord}_{\pi_2}(a) > 2$, $\mathrm{ord}_{\pi_2}(b) = 0$. By lemma 3.7, such a curve does not have good reduction at $\mathfrak{p}_2$. Indeed, since π_2 does not divide b, b does not satisfy any of the conditions in lemma 3.7 2) or 3). Now, if $a \equiv \pm 2 \bmod 8$, then $\mathrm{ord}_{\pi_2}(a) = 2$, contradicting the fact that $\mathrm{ord}_{\pi_2}(a) > 2$. Therefore, the conditions in lemma 3.7 1) are also not satisfied. Thus, the elliptic curve $y^2 = x^3 + ax^2 + bx$ does not have good reduction at π_2. □

Lemma 3.18 *Any elliptic curve with prime conductor* (π) *not dividing* 2 *or* 3, *admitting a* K*-rational* 2*-torsion point, is one of the four curves (3.5), (3.6), (3.7), (3.8), with prime conductor dividing* 257, *or is of the form (3.1), (3.2), (3.3) or (3.4).*

Proof. Let E/K be an elliptic curve over K with prime conductor (π) not dividing 2, 3 or 257, admitting a K-rational 2-torsion point. Consider a global minimal equation of the form (2.2) for E/K. Then, by lemma 2.5, we must have $\mathrm{ord}_{\pi_2}(a_1) = 0$, or $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. By the comments just before lemma 3.17, if $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$, then E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $\mathrm{ord}_{\pi_2}(A) > 4$ and $\mathrm{ord}_{\pi_2}(B) = 4$. But such an elliptic curve does not have good reduction at π_2, by lemma 3.17. Now, if $\mathrm{ord}_{\pi_2}(a_1) = 0$, then E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $(A, B, \pi_2) = 1$, by lemma 2.7. By lemma 3.9, 3.11, 3.12, 3.14, the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with $(A, B, \pi_2) = 1$ that have prime conductor (π) not dividing 2 or 3 are the elliptic curves with prime conductor dividing 257 and the elliptic curves of the form (3.1), (3.2), (3.3) or (3.4). □

3.3 The equation $x^2 + 64i = \pi^{2r+1}$.

In the previous section, we have seen that the elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with prime conductor not dividing 2 or 3 are those with prime conductor dividing 257 and the elliptic curves of the form $y^2 = x^3 + Ax^2 - 16ix$ or $y^2 = x^3 + Aix^2 + 16ix$ and their 2-isogenies, where A is such that $A^2 + 64i = \pi^{2r+1}$ for some prime π of K, and some $r \in \mathbb{N}$. In this section, we study the equation $x^2 + 64i = \pi^{2r+1}$. We find sufficient conditions on π for the equation to have no solutions.

The following lemma will be useful

Lemma 3.19 *Let ζ_8 be a primitive eight-th root of unity. Let $K = \mathbb{Q}(i)$ and $L = K(\sqrt{i}) = \mathbb{Q}(\zeta_8)$. Let p be an odd rational prime. The p splits completely in L if and only if $p \equiv 1 \bmod 8$.*

Proof. The field L is the composite of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$. Hence, by Corollary 2.7 in [16], a rational prime p splits completely in L if and only if it splits completely in $\mathbb{Q}(i)$ and in $\mathbb{Q}(\sqrt{2})$. But p splits completely in $\mathbb{Q}(i)$ if and only if $p \equiv 1 \bmod 4$, and p splits completely in $\mathbb{Q}(\sqrt{2})$ if and only if $p \equiv \pm 1 \bmod 8$. The result follows. □

Corollary 3.20 *Let $K = \mathbb{Q}(i)$, $L = K(\sqrt{i}) = \mathbb{Q}(\zeta_8)$, and $\mathfrak{p}$ a prime of K. Then*

a) $\mathfrak{p}_2$ ramifies in L.

b) if $\mathfrak{p}$ divides a prime p of $\mathbb{Q}$, with $p \equiv 1 \bmod 4$, there are two cases:

- *if $p \equiv 1 \bmod 8$, then $\mathfrak{p}$ splits in L.*
- *if $p \equiv 5 \bmod 8$, then $\mathfrak{p}\mathcal{O}_L$ is a prime in $\mathcal{O}_L$*

Proof. For part a), it suffices to see that the extension L/K is defined by the polynomial $x^2 + 2x + 1 + i \in K[x]$, which is $\mathfrak{p}_2$-Eisenstein. For part b), we use the previous lemma. A prime $p \equiv 1 \bmod 4$ splits completely in K. A prime $p \equiv 1 \bmod 8$ splits completely in L. Hence a prime $\mathfrak{p}$ of K above $p \equiv 1 \bmod 8$ (resp. $p \equiv 5 \bmod 8$) must split (resp. be inert) in L. □

We now show that the equation $x^2 + 64i = \pi^{2r+1}$ has no solutions for $\pi = pu$ with $p \equiv 3 \bmod 4$ and u a unit, or π above a prime $p \equiv 5 \bmod 8$.

Lemma 3.21 *Let p be a rational prime such that $p \equiv 5 \bmod 8$. If π is a prime in $\mathbb{Q}(i)$ above p, then the equation $A^2 + 64i = \pi^{2r+1}$ has no solution.*

Proof. By Corollary 3.20, π is inert in $\mathbb{Q}(\sqrt{i})$. The equation can be rewritten as $(A+8i\sqrt{i})(A-8i\sqrt{i}) = \pi^{2r+1}$. We can easily see that π cannot divide simultaneously $A+8i\sqrt{i}$ and $A-8i\sqrt{i}$ in $\mathbb{Z}[\sqrt{i}]$ which is a principal ideal domain. If π divides the former, then $A + 8i\sqrt{i} = \epsilon\pi^{2r+1}$ and $A - 8i\sqrt{i} = \epsilon^{-1}$. Taking normes, we get $N_{L/K}(A + 8i\sqrt{i}) = N_{L/K}(\epsilon\pi^{2r+1})$. But the lefthand side is π^{2r+1} and the right hand side is $N_{L/K}(\epsilon)\pi^{4r+2}$, which cannot be equal to each other. □

Lemma 3.22 *The equation $A^2 + 64i = (up)^{2r+1}$ has no solutions in $\mathbb{Z}[i]$ for u a unit, and $p \equiv 3 \bmod 4$.*

Proof. If $u = \pm 1$ the equation is $A^2 + 64i = \pm p^{2r+1}$. Writing $A = x + yi$, then we must have $x^2 - y^2 = \pm p^{2r+1}$ and $2xy + 64 = 0$. There are finitely many solutions to the second equation, and all of them do not satisfy the first equation. Therefore, there are no solutions for the equation with $u = \pm 1$.

If $u = \pm i$, writing $A = x + yi$, the equation implies that $x^2 - y^2 = 0$ and $2xy + 64 = \pm p^{2r+1}$. The last equation has no solutions since the lefthandside is even, while the righthand side is odd. □

Lemma 3.23 *Fix π, a prime not dividing 2, and r. If the equation $x^2 + 64i = \pi^{2r+1}$ has a solution, then it does not when π is replaced by one of its associates.*

Proof. Suppose $x^2 + 64i = \pi^{2r+1}$ has a solution. Since the righthand side of the equation has even imaginary part, π must have even imaginary part as well. In that case, $\pm i\pi$ has odd imaginary part. Hence, when π is replaced by $\pm i\pi$, the equation has no solutions. Let us now consider the case when π is replaced by $-\pi$. We would like to see if the two equations $x^2 + 64i = \pi^{2r+1}$ and $y^2 + 64i = -\pi^{2r+1}$ can possibly have solutions simultaneously. Adding the above two equations, we get $x^2 + y^2 = -128i$, which can be rewritten as $(x+yi)(x-yi) = -128i$. The valuation of $128i$ at π_2 is 14, so if the valuation of $x - yi$ at π_2 is m, then that of $x + yi$ must be $14 - m$. Since $x + yi$ and $x - yi$ differ by $2yi$, with y not divisible by π_2, we can easily see that the valuation of $x - yi$ must be 2 or 12. We treat the case when the valuation is 2, the other case is similar. We then write $x - yi = 2\epsilon$ and $x + yi = -64i\epsilon^{-1}$. Solving for x, we get $x = \epsilon - 32i\epsilon^{-1}$ so that $x^2 + 64i = \epsilon^2 - 32^2\epsilon^{-2} = \pm(1 - 32^2)$. But $1 - 32^2 = -1023$ is not the power of a prime in $\mathbb{Q}(i)$. We conclude that the equation $y^2 + 64i = -\pi^{2r+1}$ has no solutions when $x^2 + 64i = \pi^{2r+1}$ does. □

3.4 Proof of The Main Theorem

Let E/K be an elliptic curve with a K-rational 2-torsion point. Then E/K admits an equation of the form $y^2 = x^3 + ax^2 + bx$. Assume E/K has prime conductor $\mathfrak{p}$ not dividing

2, 3 and 257. Then, by lemma 3.18, there exists A such that $A^2 + 64i = \pi^{2r+1}$ for some generator π of $\mathfrak{p}$, and $a = A$, $b = -16i$ or $a = Ai$, $b = 16i$. By lemma 3.23, for fixed r, the generator π can be choosen uniquely. What has not been done yet is to give conditions in which the converse holds: if there exists (A, π, r) such that $A^2 + 64i = \pi^{2r+1}$, when is it true that one of the curves $y^2 = x^3 + Ax^2 - 16ix$ or $y^2 = x^3 + Aix + 16ix$ has prime conductor (π). In this section, we give those conditions and complete the proof of the main theorem.

Lemma 3.24 *If A is such that $A^2 + 64 = \pi^{2r+1}$, with π dividing a prime $p \equiv 1 \bmod 16$, then either $A \equiv \pm 1 \bmod 4$ or $Ai \equiv \pm 1 \bmod 4$. In the case $A \equiv \pm 1 \bmod 4$, the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has prime conductor (π). In the case $Ai \equiv \pm 1 \bmod 4$, the elliptic curve $y^2 = x^3 + Aix^2 + 16ix$ has prime conductor (π). If π divides a prime $p \equiv 9 \bmod 16$, the elliptic curves $y^2 = x^3 + Ax^2 - 16ix$ and $y^2 = x^3 + Aix^2 + 16ix$ always have bad reduction at π_2.*

Proof. Suppose $A \in \mathcal{O}_K$ is such that $A^2 + 64i = \pi^{2r+1}$ with π a prime in $\mathcal{O}_K$ dividing some rational $p \equiv 1 \bmod 8$. Writing $A = x + yi$ and $\pi^{2r+1} = u + vi$ with x, y, u and $v \in \mathbb{Z}$, we get $x^2 - y^2 + (2xy + 64)i = u + vi$. Then v must be even and u must be odd, so that x and y have distinct parity. Taking norms, we get

$$x^4 + 2x^2y^2 + y^4 + 256xy + 64^2 = p^{2r+1}. \tag{3.17}$$

Assume first that $p \equiv 1 \bmod 16$. Then $p^{2r+1} \equiv 1 \bmod 16$. Looking at the equation (3.17) mod 16, we get $x^4 + 2^2y^2 + y^4 \equiv 1 \bmod 16$. Since x and y have distinct parity, we always have $x^4 + y^4 \equiv 1 \bmod 16$. Thus the equation (3.17) gives $2x^2y^2 \equiv 0 \bmod 16$. If x is odd and y even, this implies that $y \equiv 0 \bmod 4$, so that $A \equiv \pm 1 \bmod 4$. Then, by lemma 3.7, the elliptic curve $y^2 = x^3 + Ax^2 - 16ix$ has good reduction at $\mathfrak{p}_2$, and thus has conductor (π). If x is even and y is odd, we must have $x \equiv 0 \bmod 4$, so that $Ai \equiv \pm 1 \bmod 4$. Again, by lemma 3.7, the elliptic curve $y^2 = x^3 + Aix^2 + 16ix$ then has good reduction at $\mathfrak{p}_2$, and thus has conductor (π).

Assume now that $p \equiv 9 \bmod 16$. Then $p^{2r+1} \equiv 9 \bmod 16$. Looking at the equation (3.17) mod 16, we get $x^4 + 2x^2y^2 + y^4 \equiv 9 \bmod 16$. Since $x^4 + y^4 \equiv 1 \bmod 16$, we get $2x^2y^2 \equiv 8 \bmod 16$. If x is odd and y is even, this implies that $y \equiv 2 \bmod 4$. If x is even and y is odd, this implies that $x \equiv 2 \bmod 4$. In any case, A, $Ai \not\equiv \pm 1 \bmod 4$, so that, by lemma 3.7, the elliptic curves $y^2 = x^3 + Ax^2 - 16ix$ and $y^2 = x^3 + Aix^2 + 16ix$ do not have good reduction at $\mathfrak{p}_2$. □

Let us now give the proof of Theorem 3.1 and Proposition 3.5:

Proof of Theorem 3.1.

a) By lemma 2.6, we know that in order to find the elliptic curves that have prime conductor and a K-rational 2-torsion point, we have to solve the diophantine equation $B^2(A^2 - 4B) = u2^8\pi^s$. By lemma 3.18, except for those elliptic curves that have prime conductor dividing 257, all the others are of the form

$$y^2 = x^3 + Ax^2 - 16ix$$

or

$$y^2 = x^3 + Aix^2 + 16ix,$$

and their isogenies, where A satisfies the equation $A^2+64i = \pi^{2r+1}$. By lemma 3.7, if the first (resp. the second) curve is the one with prime conductor, then we must necessarily have $A \equiv \pm 1 \bmod 4$ (resp. $Ai \equiv \pm 1 \bmod 4$). By lemma 3.21 and lemma 3.22, we know that equation $A^2 + 64i = \pi^{2r+1}$ has no solution when $p \equiv 5 \bmod 8$ and $p \equiv 3 \bmod 4$. By lemma 3.24, if $p \equiv 9 \bmod 16$, any elliptic curve corresponding to a solution of $A^2 + 64i = \pi^{2r+1}$ does not have good reduction at π_2. Conversely, if A is such that $A^2 + 64i = \pi^{2r+1}$, for some π above a $p \equiv 1 \bmod 16$, then by lemma 3.24, one of the two above curves has prime conductor (π).

b) By remark 2.12, the hypotheses of theorem 2.11 are satisfied. The result then follows from theorem 2.11

c) By remark 2.25, the hypotheses of theorem 2.23 and corollary 2.24 are satisfied. The result then follows from corollary 2.24. □

Proof of Proposition 3.5. Let π be a prime in K above 257. Let E^{π^ϵ} be the elliptic curve $y^2 = \pi^\epsilon x^3 - 64i$, with $\epsilon = 1$ or 2. Using a program by Denis Simon (see [47]), we see that these elliptic curves have rank 0. Thus, by lemma 2.27, there are no elliptic curve of the form $y^2 = x^3 + Ax^2 - 16ix$ or $y^2 = x^3 + Aix^2 + 16ix$ with prime conductor (π) dividing 257, where A is such that $A^2 + 64i = \pi^{2r+1}$. Thus, by lemma 3.18, the elliptic curves with prime conductor dividing 257 having a K-rational 2-torsion point are the ones given in Proposition 3.5. We only need to show that any curve with prime conductor dividing 257 must have a K-rational 2-torsion point. For this, we use theorem 2.11. Using Pari, we find that the ray class numbers $h_{(2)}(N)$ with $N = K(\sqrt{16+i})$ or $N = K(\sqrt{i(16+i)})$ are coprime to 3. Thus, any elliptic curve with conductor $(16+i)$ must have a K-rational 2-torsion point. This finishes the proof of the Proposition. □

3.5 Tables of values A such that $y^2 = x^3 + Ax^2 - 16ix$ is an elliptic curve with prime conductor

The tables below contain values for $A \in \mathbb{Z}[i]$ such that $A \equiv \pm 1 \bmod 4$ and $A^2 + 64i$ is a prime π in $\mathbb{Q}(i)$. The letter p stands for the rational prime below $A^2 + 64i$. For each such A, the elliptic curve $y^2 = x^3 + Ax^2 - 16ix$ has conductor (π). The tables contain all the possible values for A such that $N_{\mathbb{Q}(i)/\mathbb{Q}}(A^2 + 64i) \leq 10^6$.

A	$\pi = A^2 + 64i$	p
$7 - 4i$	$33 + 8i$	1153
$5 - 8i$	$-39 - 16i$	1777
$1 - 4i$	$-15 + 56i$	3361
3	$9 + 64i$	4177
$9 - 4i$	$65 - 8i$	4289
$5i$	$25 + 64i$	4721
$9 - 8i$	$17 - 80i$	6689
$3 + 4i$	$-7 + 88i$	7793
$1 + 8i$	$-63 + 80i$	10369
$9i$	$81 + 64i$	10657
$3 + 8i$	$-55 + 112i$	15569
$3 - 12i$	$-135 - 8i$	18289
$7 - 12i$	$-95 - 104i$	19841
$9 + 4i$	$65 + 136i$	22721
$9 - 12i$	$-63 - 152i$	27073
$11 + 4i$	$105 + 152i$	34129
$3 + 12i$	$-135 + 136i$	36721
$11 - 12i$	$-23 - 200i$	40529

A	$\pi = A^2 + 64i$	p
$15 - 4i$	$209 - 56i$	46817
$5 + 12i$	$-119 + 184i$	48017
$15i$	$225 + 64i$	54721
$15 - 8i$	$161 - 176i$	56897
$13 - 12i$	$25 - 248i$	62129
$7 - 16i$	$-207 - 160i$	68449
$13 + 8i$	$105 + 272i$	85009
$17 - 8i$	$225 - 208i$	93889
$19i$	$361 + 64i$	134417
$17 - 12i$	$145 - 344i$	139361
$15 - 16i$	$-31 - 416i$	174017
$9 - 20i$	$-319 - 296i$	189377
$11 + 16i$	$-135 + 416i$	191281
$21 - 4i$	$425 - 104i$	191441
$21 - 8i$	$377 - 272i$	216113
$11 - 20i$	$-279 - 376i$	219217
$19 + 8i$	$297 + 368i$	223633
$7 + 20i$	$-351 + 344i$	241537

A	$\pi = A^2 + 64i$	p
$17 + 12i$	$145 + 472i$	243809
$23i$	$529 + 64i$	283937
$23 - 8i$	$465 - 304i$	308641
$19 + 12i$	$217 + 520i$	317489
$15 - 20i$	$-175 - 536i$	317921
$23 + 4i$	$513 + 248i$	324673
$3 - 24i$	$-567 - 80i$	327889
$1 + 24i$	$-575 + 112i$	343169
$3 + 24i$	$-567 + 208i$	364753
$23 - 12i$	$385 - 488i$	386369
$25i$	$625 + 64i$	394721
$21 - 16i$	$185 - 608i$	403889
$21 + 12i$	$297 + 568i$	410833
$11 - 24i$	$-455 - 464i$	422321
$7 + 24i$	$-527 + 400i$	437729
$15 + 20i$	$-175 + 664i$	471521
$9 + 24i$	$-495 + 496i$	491041
$25 - 12i$	$481 - 536i$	518657

A	$\pi = A^2 + 64i$	p
$25 + 8i$	$561 + 464i$	530017
$11 + 24i$	$-455 + 592i$	557489
$21 + 16i$	$185 + 736i$	575921
$27 + 4i$	$713 + 280i$	586769
$3 - 28i$	$-775 - 104i$	611441
$1 - 28i$	$-783 + 8i$	613153
$13 + 24i$	$-407 + 688i$	638993
$7 - 28i$	$-735 - 328i$	647809
$25 - 16i$	$369 - 736i$	677857
$9 - 28i$	$-703 - 440i$	687809
$23 + 16i$	$273 + 800i$	714529
$15 + 24i$	$-351 + 784i$	737857
$19 - 24i$	$-215 - 848i$	765329
$29 + 4i$	$825 + 296i$	768241
$21 + 20i$	$41 + 904i$	818897
$27 - 16i$	$473 - 800i$	863729
$29 - 12i$	$697 - 632i$	885233
$15 - 28i$	$-559 - 776i$	914657

Chapter 4

Elliptic curves over $\mathbb{Q}(\sqrt{-2})$

4.1 Main theorem

Let $K = \mathbb{Q}(\sqrt{-2})$. We are interested in finding all the elliptic curves whose conductor is a prime ideal not dividing 2 or 3. Note that the rational primes p that split in $\mathbb{Q}(\sqrt{-2})$ are those that are such that $p \equiv 1, 3 \bmod 8$, and those that are inert in $\mathbb{Q}(\sqrt{-2})$ are those that satisfy $p \equiv 5, 7 \bmod 8$. Let $\mathfrak{p}_2$ be the prime in K above 2 and $\pi_2 = \sqrt{-2}$ a generator of $\mathfrak{p}_2$.

Here is the main theorem of this chapter:

Theorem 4.1 *Let $K = \mathbb{Q}(\sqrt{-2})$.*

a) Let p be a rational prime distinct from 2 and 3. Let $\mathfrak{p}$ be a prime above p. Then, there is an elliptic curve with conductor $\mathfrak{p}$ and having a K-rational 2-torsion point if and only if, for some generator π of $\mathfrak{p}$, the equation $x^2 + 64 = \pi^{2r+1}$ has a solution $(A, r) \in \mathcal{O}_K \times \mathbb{N}$ such that $A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$. For fixed r, there is at most one generator π of $\mathfrak{p}$ such that $A^2 + 64 = \pi^{2r+1}$, with $A \in \mathcal{O}_K$.

There is a solution (A, r) such that $A^2 + 64 = \pi^{2r+1}$ only when $p \equiv 1 \bmod 8$. There is a solution (A, r) such that $A^2 + 64 = \pi^{2r+1}$ and $A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$ only if $p \equiv 1 \bmod 16$. When there is a solution for some $p \equiv 1 \bmod 16$, then one of the congruence $\pm A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$ is automatically satisfied. Given a solution (A, r) with $A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$, we obtain the (isogenous) elliptic curves with prime conductor $\mathfrak{p}$

$$y^2 = x^3 + Ax^2 - 16x, \qquad \Delta = 2^{12}\pi^{2r+1}, \tag{4.1}$$

$$y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x, \qquad \Delta = -2^{12}\pi^{4r+2}. \tag{4.2}$$

b) Let π be a prime not dividing 2 or 3. If for all the extensions of the form $N = K(\sqrt{\pm\pi})$, the ray class number $h_{(2)}(N)$ is coprime to 3, then any elliptic curve with prime conductor (π) must have a K-rational 2-torsion point.

c) Let π be a prime not dividing 3. Suppose that $(\pi) \neq (37)$. If for all the extensions of the form $N = K(\pi^{\epsilon/3})$, the ray class number $h_{(3)}(N)$ is not divisible by 4, then there are no elliptic curves with conductor (π).

The table below indicates which primes p satisfy the conditions on $h_{(2)}$, and which satisfy the conditions on $h_{(3)}$:

$3 \nmid h_{(2)}$	$3 \nmid h_{(2)}, 4 \nmid h_{(3)}$	$4 \nmid h_{(3)}$
$7, 41, 47, , 179, 191$	$5, 11, 17, 19, 43$	$13, 31, 83, 137, 167$
$227, 313, 317, 331, 337$	$59, 73, 89, 97, 103$	$281, 311, 349, 367, 439$
$353, 419, 443, 463, 479$	$107, 113, 131, 139, 163$	$461, 491, 691, 761$
$521, 523, 541, 569, 607$	$193, 211, 233, 241, 251$	
$647, 719, 787, 827, 853$	$257, 283, 307, 347, 379$	
$859, 881, 887, 907, 911$	$401, 409, 433, 449, 467$	
$919, 937$	$499, 547, 563, 571, 577$	
	$593, 601, 617, 619, 643$	
	$659, 673, 739, 769, 811$	

Corollary 4.2 *a) There are no elliptic curves over $\mathbb{Q}(\sqrt{-2})$ with prime conductor dividing p, for the following 85 values of p among the 168 prime numbers in $[2, 1000]$;* $p = 2,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 31,\ 41,\ 43,\ 47,\ 59,\ 73,\ 83,\ 89,\ 97,\ 103,\ 107,\ 113,\ 131,\ 137,\ 139,\ 163,\ 167,\ 179,\ 191,\ 193,\ 211,\ 227,\ 233,\ 241,\ 251,\ 257,\ 281,\ 283,\ 307,\ 311,\ 313,\ 317,\ 331,\ 347,\ 349,\ 367,\ 379,\ 401,\ 409,\ 419,\ 433,\ 439,\ 443,\ 449,\ 461,\ 463,\ 467,\ 479,\ 491,\ 499,\ 521,\ 523,\ 541,\ 547,\ 563,\ 569,\ 571,\ 577,\ 593,\ 601,\ 607,\ 617,\ 619,\ 643,\ 647,\ 659,\ 673,\ 683,\ 691,\ 719,\ 739,\ 761,\ 769,\ 787,\ 811,\ 827,\ 853,\ 859,\ 887,\ 907,\ 911,\ 919$ *and* 937.

b) Any elliptic curve with conductor dividing $p = 353$ *or* 881 *must have a* K*-rational* 2*-torsion point and discriminant* Δ *such* $\mathrm{ord}_\pi(\Delta) > 1$.

c) There exist elliptic curves with conductor dividing 337. *Any elliptic curve with prime conductor dividing* 337 *has a* K*-rational* 2*-torsion point.*

Proof.

a) Let p be a prime appearing in the list a). Let $\mathfrak{p}$ be a prime above p. We note first that there are no elliptic curves defined over K with conductor $(\sqrt{-2})$ (see Table 3 in [37]). If $p \equiv 1 \bmod 16$, then it satisfies the conditions of Theorem 4.1 c). If $p \equiv 9 \bmod 16$, then it satisfies either the conditions of Theorem 4.1 b) or c). If $p \not\equiv 1 \bmod 8$, then it satisfies the conditions in 4.1 b), and the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions, by 4.1 a).

b) Let p be a prime appearing in the list b). Then $p \equiv 1 \bmod 8$. The table at the end of this chapter shows that there are no elliptic curves with prime conductor dividing p, having a K-rational 2-torsion point and discriminant Δ such that $\mathrm{ord}_\pi(\Delta) = 1$. This prime p also satisfies the conditions in 3.1 b). The statement then follows.

c) As can be seen in the tables at the end of the chapter, there exist elliptic curves with prime conductor dividing 337. The prime 337 satisfies the conditions of 3.1 b). Hence, the second statement in c) follows. □

4.2 Elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with prime conductor

By lemma 2.6, to find the elliptic curves with prime conductor not dividing 2 and 3 having a K-rational 2-torsion point, we have to consider the equation $B^2(A^2 - 4B) = u2^8\pi^s$. Since 2 ramifies in $\mathbb{Q}(\sqrt{-2})$, by lemma 2.5, there are two cases, one when $\mathrm{ord}_{\pi_2}(a_1) = 0$, and the other when $\mathrm{ord}_{\pi_2}(a_1) = 1$.

We will show that when $\mathrm{ord}_{\pi_2}(a_1) = 1$, the elliptic curve (2.2) does not have good reduction at π_2. In the case when $\mathrm{ord}_{\pi_2}(a_1) = 0$, we will find the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3 by solving the equation $B^2(A^2 - 4B) = u2^8\pi^s$. We will find these curves by considering the different cases:

a) Case when $u = 1$ and $s = 2r$.

b) Case when $u = -1$ and $s = 2r$.

c) Case when $s = 2r + 1$.

When $u = 1$ and $s = 2r$, the equation is $B^2(A^2-4B) = 2^8\pi^{2r}$. When $u = -1$ and $s = 2r$, the equation is $B^2(A^2-4B) = -2^8\pi^{2r+1}$. When $s = 2r+1$, the equation is $B^2(A^2-4B) = 2^8\pi^{2r+1}$.

We will need the following lemma:

Lemma 4.3 *Let $\alpha = a + b\sqrt{-2}$ be an algebraic integer in $\mathbb{Q}(\sqrt{-2})$ coprime to $\sqrt{-2}$. Then*

$$\begin{aligned} \alpha^2 &\equiv 1 \text{ or } -1 + 2\sqrt{-2} \mod 4, \\ -2\alpha^2 &\equiv 6 \text{ or } 2 + 4\sqrt{-2} \mod 8, \\ \alpha^4 &\equiv 1 \text{ or } 1 + 4\sqrt{-2} \mod 8. \end{aligned}$$

Proof. Since $\sqrt{-2}$ does not divide α, we must have that a is odd. We have that $\alpha^2 = a^2 - 2b^2 + 2ab\sqrt{-2}$ and $\alpha^4 = a^4 + 4a^3b\sqrt{-2} - 12a^2b^2 - 8ab^3\sqrt{-2} + 4b^4$. Hence, if b is even, we have that $\alpha^2 \equiv 1 \bmod 4$, $-2\alpha^2 \equiv -2 \bmod 8$ and $\alpha^4 \equiv 1 \bmod 8$. If b is odd, then $\alpha^2 \equiv -1 + 2\sqrt{-2} \bmod 4$, $-2\alpha^2 \equiv 2 + 4\sqrt{-2} \bmod 8$ and $\alpha^4 \equiv 1 + 4\sqrt{-2} \bmod 8$. □

To check whether an elliptic curve $y^2 = x^3 + Ax^2 + Bx$ over K has good reduction at $\mathfrak{p}_2$, we will use the following lemma, which is a consequence of lemma 2.8:

Lemma 4.4 *Let $K = \mathbb{Q}(\sqrt{-2})$. The elliptic curve $y^2 = x^3 + Ax^2 + Bx$ has good reduction at π_2 if and only if A and B satisfy the following conditions:*

1) $A \equiv 6$ or $2 + 4\sqrt{-2} \bmod 8$ and $B \equiv 1$ or $1 + 4\sqrt{-2} \bmod 8$, or

2) $A \equiv 1$ *or* $-1+2\sqrt{-2} \bmod 4$ *and* $B \equiv 0 \bmod 16$*, or*

3) $A \equiv 0 \bmod 4\sqrt{-2}$*,* $B \equiv 4+8\sqrt{-2} \bmod 16$ *and either* $2A+B \equiv 4 \bmod 32$ *or* $-2A-B \equiv 12+16\sqrt{-2} \bmod 32$*.*

Proof. We have $\pi_2^2 = -2$, $\pi_2^5 = 4\sqrt{-2}$, $\pi_2^8 = 16$, $\pi_2^{10} = -32$, $\pi_2^4 + 8\pi_2 = 4+8\sqrt{-2}$, $\pi_2^4 + \pi^6 = -4$ and $5\pi_2^4 + 4\pi_2^5 + \pi_6 = 20+16\sqrt{-2}-8 = 12+16\sqrt{-2}$. The lemma then follows from lemma 2.8 and lemma 4.3. □

We now find the elliptic curves of the form $y^2 = x^3+Ax^2+Bx$ that have prime conductor.

Lemma 4.5 *There are no elliptic curves over* K *of the form* $y^2 = x^3+Ax^2+Bx$ *with prime conductor* (π) *not dividing* 2 *or* 3*, with* $(A, B, \pi_2) = 1$ *and* $B^2(A^2-4B) = 2^8\pi^{2r}$*.*

Proof. Suppose $y^2 = x^3 + Ax^2 + Bx$ is an elliptic curve with prime conductor (π) not dividing 2 or 3, such that $(A, B, \pi_2) = 1$ and $B^2(A^2-4B) = 2^8\pi^{2r}$. Then A^2-4B is a square, so that $X^3+AX^2+BX = 0$ has its three roots in $\mathcal{O}_K$, say $0, a, b$ with $a, b \not\equiv 0 \bmod \pi$ and $a \equiv b \bmod \pi$. We then have $B = ab$ and $A = -a-b$, and $a^2b^2(a-b)^2 = 2^8\pi^{2r}$. By hypothesis, π does not divide a and b. Furthermore, π_2 divides one and only one of a and b. Let say it divides a. Then $a = 16v$ and $b = w$, where v and w are units. The equation then becomes, after simplification, $(16v-w)^2 = \pi^{2r}$, which has no solutions. Indeed, the possible values for $16v-w$ are ± 15 and ± 17 which are not powers of primes in K. The result then follows. □

Lemma 4.6 *The equation* $A^2+1 = 64u\pi^s$ *has no solutions* $A \in \mathcal{O}_K$*.*

Proof. Write $A = x+y\sqrt{-2}$, with x and y rational integers. We deduce that $x^2-2y^2+1 \equiv 0 \bmod 64$ and $2xy \equiv 0 \bmod 64$. The first congruence implies that $x \equiv 1 \bmod 2$. Then, the second congruence implies that $y \equiv 0 \bmod 32$. Using the first congruence again, we get $x^2+1 \equiv 0 \bmod 64$, which is impossible, since a square cannot be -1 modulo 4. □

Lemma 4.7 *The elliptic curves over K of the form $y^2 = x^3+Ax^2+Bx$ with prime conductor (π) not dividing 2 or 3 such that $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ are the elliptic curves of the form (4.1)*

Proof. We know that π cannot divide B. If π_2 divides B, then it does not divide A. Hence $B = 16v$. The equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ becomes, after simplification, $A^2 - 64v = \pi^{2r+1}$. If $v = 1$, we have $(A - 8)(A + 8) = \pi^{2r+1}$. Since π cannot divide simultaneously $A + 8$ and $A - 8$, we have $A - 8 = w$ or $A + 8 = w$, with w a unit. If $A - 8 = w$, then $(A - 8)(A + 8) = w(16 + w)$. But $16 + w = 15$ or 17, which are not odd powers of primes in K. Hence, $w(16 + w)$ cannot be of the form $w(16 + w) = \pi^{2r+1}$. There are no solutions as well for the case $A + 8 = w$, a unit. If $v = -1$, then the equation is $A^2 + 64 = \pi^{2r+1}$. Whenever there is a solution, the corresponding elliptic curve is of the form (4.1).

If π_2 does not divide B, then $B = v$, a unit. The equation becomes, after simplication, $A^2-4v = 2^8\pi^{2r+1}$, and writing $A = 2C$, we get $C^2-v = 64\pi^{2r+1}$. If $v = 1$, we can rewrite the equation as $(C-1)(C+1) = 64\pi^{2r+1}$. Since π cannot divide $C-1$ and $C+1$ simultaneously, we have $C - 1 = 2w$, $C - 1 = 32w$, $C + 1 = 2w$ or $C + 1 = 32w$. If $C - 1 = 2w$, we get $(C - 1)(C + 1) = 2w(2w + 2) = 4w(1 + w)$, which cannot possibly be a multiple of 64. Similarly, we get that in the other cases too, there are no solutions. If $v = -1$, the equation becomes $C^2 + 1 = 64\pi^{2r+1}$. By lemma 4.6, it has no solutions. □

Lemma 4.8 *The elliptic curves over K of the form $y^2 = x^3+Ax^2+Bx$ with prime conductor (π) not dividing 2 and 3, with $(A, B, \pi_2) = 1$ and $B^2(A^2 - 4B) = -2^8\pi^{2r}$, are the elliptic curves of the form (4.2).*

Proof. There are four cases, depending on whether π and π_2 divide B. If π_2 and π divide B, then $B = 16v\pi^r$. The equation becomes $A^2 - 64v\pi^r = -1$, after simplification. This can be rewritten as $A^2 + 1 = 64v\pi^r$. However, this has no solutions, by lemma 4.6.

If $B = v\pi^r$, then the equation becomes $A^2 - 4v\pi^r = -2^8$. We can see that A must then be a multiple of 2. Write $A = 2C$. Then $C^2 - v\pi^r = -64$ i.e., $C^2 + 64 = v\pi^r$. If

$r = 2t + 1$, then we can assume that $v = 1$, since v can be absorbed in π^{2r+1}. The equation becomes $C^2 + 64 = \pi^{2t+1}$. If there are solutions, then the corresponding elliptic curves are $y^2 = x^3 + 2Cx^2 + \pi^{2t+1}x$, which are of the form (4.2).

Assume now that $r = 2t$ is even. If $v = 1$, the equation becomes $C^2 + 64 = \pi^{2t}$. If there are solutions, then the corresponding elliptic curves are $y^2 = x^3 + 2Cx^2 + \pi^{2t}x$. These curves are 2-isogenous to $y^2 = x^3 - Cx^2 - 16x$. But, by lemma 4.5, there is no curve of the form $y^2 = x^3 - Cx^2 - 16x$ with prime conductor. For $v = -1$, the equation is $C^2 + 64 = -\pi^{2t}$. Writing $C = x + y\sqrt{-2}$ and $\pi^t = u + v\sqrt{-2}$, we get $x^2 - 2y^2 + 64 = -u^2 + 2v^2$ and $xy = uv$. Since π is a prime of $\mathbb{Q}(\sqrt{-2})$ above an odd rational prime, u must be odd. The first equation then implies that u and x must both be odd. The second equation implies then that y and v must have same parity. But this is incompatible with the first equation. We conclude that the equation $C^2 + 64 = -\pi^{2t}$ has no solutions.

If $B = 16v$, the equation becomes $A^2 - 64v = -\pi^{2r}$. If $v = 1$, the equation can be rewritten as $(A - 8)(A + 8) = -\pi^{2r}$. Since π cannot divide both $A - 8$ and $A + 8$, we have $A - 8 = w$ or $A + 8 = w$, where $w = \pm 1$. If $A - 8 = w$, we get $(A - 8)(A + 8) = w(16 + w)$. But this has no solutions. Similarly, in the other case, there are no solutions as well. For $v = -1$, the equation is $A^2 + 64 = -\pi^{2r}$, which has no solutions, as already seen.

If $B = v$, the equation becomes $A^2 - 4v = -2^8\pi^{2r}$. We can see then that A must be of the form $A = 2C$ for some C in $\mathcal{O}_K$. The equation becomes $C^2 - v = -64\pi^{2r}$. If $v = -1$, there are no solutions by lemma 4.6. If $v = 1$, the equation can be rewritten in the form $(C - 1)(C + 1) = -64\pi^{2r}$, which can easily be seen to have no solutions. □

When $\mathrm{ord}_{\pi_2}(a_1) = 1$, then, as for the case of $K = \mathbb{Q}(i)$, the Newton polygon of $f(x) = x^3 + b_2x^2 + 8b_4x + 16b_6$ has two segments, one of length 2 and slope -3, the other of length one and slope -2. Hence, a root in $\mathcal{O}_K$ either has valuation 2 or valuation 3. We show here too that it cannot have valuation 3.

Lemma 4.9 *In $K = \mathbb{Q}(\sqrt{-2})$, an element $x + y\sqrt{-2}$ is divisible (resp. exactly divisible) by $\sqrt{-2}$ if and only if x is even (resp. x is even and y is odd).*

Proof. The element $x + y\sqrt{-2}$ is divisible by $\sqrt{-2}$ if and only if there exist integers a, b such that $x + y\sqrt{-2} = (a + b\sqrt{-2})\sqrt{-2} = -2b + a\sqrt{-2}$. Thus, $x + y\sqrt{-2}$ is divisible by $\sqrt{-2}$ if and only if x is even. It is exactly divisible by $\sqrt{-2}$ if and only if it is divisible by $\sqrt{-2}$ but not by 2, i.e., if and only if x is even and y is odd. □

Lemma 4.10 *Let $f(x) = x^3 + b_2x^2 + 8b_4x + 16b_6$. It t is in $\mathcal{O}_K$ and such that $f(t) = 0$, then* $\mathrm{ord}_{\pi_2}(t) = 2$.

Proof. We only have to show that $\mathrm{ord}_{\pi_2}(t)$ cannot be 3. Suppose that $\mathrm{ord}_{\pi_2}(t) = 3$. We have that $t^3 + b_2t^2 + 8b_4t + 16b_6 = 0$. Also $\mathrm{ord}_{\pi_2}(t^3 + 8b_4t) = 9$, hence, we must also have that $\mathrm{ord}_{\pi_2}(b_2t^2 + 16b_6) = 9$. We show that this cannot happen, thus proving that $\mathrm{ord}_{\pi_2}(t)$ cannot be equal 3. Using the facts that $\mathrm{ord}_{\pi_2}(a_1) = 1$, $\mathrm{ord}_{\pi_2}(a_3) = 0$ and $\mathrm{ord}_{\pi_2}(t) = 3$, we can see that $b_2 = 2(\alpha + \beta\sqrt{-2})$, $t^2 = 8(\gamma + \zeta\sqrt{-2})$ and $b_6 = \epsilon + \delta\sqrt{-2}$, where α, γ and ϵ are odd, β, ζ, δ are even. We have that $b_2t^2 + 16b_6 = 16(\alpha\gamma - 2\beta\zeta + \epsilon) + (\alpha\zeta + \beta\gamma + \delta)\sqrt{-2})$. But $\alpha\gamma - \beta\zeta + \epsilon$ and $\alpha\zeta + \beta\gamma + \delta$ are both even, so that $b_2t^2 + 16b_6$ has valuation greater than or equal to 10, and so cannot be equal to 9. □

We thus have that $\mathrm{ord}_{\pi_2}(t) = 2$ and thus, $\mathrm{ord}_{\pi_2}(A) > 4$ and $\mathrm{ord}_{\pi_2}(B) = 4$. Only the fact that $\mathrm{ord}_{\pi_2}(A) > 4$ is not obvious. Since $\mathrm{ord}_{\pi_2}(B) = 4$ and $B^2(A^2 - 4B) = u2^8\pi^s$, we have $\mathrm{ord}_{\pi_2}(A^2 - 4B) = 8$, so that $\mathrm{ord}_{\pi_2}(A) \geq 4$. If $\mathrm{ord}_{\pi_2}(A) = 4$, we can write $A = 4(\alpha + \beta\sqrt{-2})$, with α odd, by lemma 4.9. By the same lemma, we can write $B = 4(\epsilon + \delta\sqrt{-2})$, with ϵ odd. We then have $A^2 - 4B = 16(\alpha^2 - 2\beta^2 - \epsilon + (2\alpha\beta + \delta)\sqrt{-2})$. Since $\alpha^2 - 2\beta^2 - \epsilon$ is even, we have $\mathrm{ord}_{\pi_2}(A^2 - 4B) > 4$, contradiction. Thus, we must have $\mathrm{ord}_{\pi_2}(A) > 4$.

Lemma 4.11 *Any elliptic curve $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Q}(\sqrt{-2})$ with* $\mathrm{ord}_{\pi_2}(A) > 4$ *and* $\mathrm{ord}_{\pi_2}(B) = 4$ *does not have good reduction at π_2.*

Proof. Dividing by 8, we get a new equation $y^2 = x^3 + ax^2 + bx$ with $\mathrm{ord}_{\pi_2}(a) > 2$ and $\mathrm{ord}_{\pi_2}(b) = 0$. By lemma 4.4, such an elliptic curve does not have good reduction at π_2. Indeed, b does not satisfy the conditions on B in lemma 4.4 *b*) or *c*). In addition, since $\mathrm{ord}_{\pi_2}(a) = 2$, we cannot have $a \equiv 6$ or $2 + 4\sqrt{-2} \bmod 8$. Hence a does not satisfy the conditions on A of lemma 4.4 *a*). We thus have that the elliptic curve $y^2 = x^3 + ax^2 + bx$ does not have good reduction at π_2. □

Lemma 4.12 *The elliptic curves over K with prime conductor (π) not dividing 2 or 3 and K-rational 2-torsion points are the elliptic curves of the form (4.1) and (4.2) that have good reduction at π_2.*

Proof. Let E/K be an elliptic curve over K with prime conductor (π) not dividing 2 or 3, admitting a K-rational 2-torsion point. Consider a global minimal equation of the form (2.2) for E/K. Then, by lemma 2.5, we must have $\mathrm{ord}_{\pi_2}(a_1) = 0$, or $\mathrm{ord}_{\pi_2}(a_1) = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$. By the comments just before lemma 4.11, if $\mathrm{ord}_{\pi_2} = 1$ and $\mathrm{ord}_{\pi_2}(a_3) = 0$, then E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $\mathrm{ord}_{\pi_2}(A) > 4$ and $\mathrm{ord}_{\pi_2}(B) = 4$. But such an elliptic curve does not have good reduction at π_2, by lemma 4.11. Now, if $\mathrm{ord}_{\pi_2}(a_1) = 0$, then E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $(A, B, \pi_2) = 1$, by lemma 2.7. By lemma 4.5, 4.7 and 4.8, the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with $(A, B, \pi_2) = 1$ that have prime conductor (π) not dividing 2 or 3 are the elliptic curves of the form (4.1) and (4.2). □

4.3 The equation $x^2 + 64 = \pi^{2r+1}$.

From the previous section, any elliptic curve with prime conductor (π) not dividing 2 or 3 and having a K-rational 2-torsion point is of the form $y^2 = x^3 + Ax^2 - 16x$ or $y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x$, with $A \in \mathcal{O}_K$ such that $A^2 + 64 = \pi^{2r+1}$. We now study the equation $x^2 + 64 = \pi^{2r+1}$. We find conditions on π such that the equation has no solutions.

Lemma 4.13 *Let p be a prime such that $p \equiv 3 \bmod 8$. Let (π) be a prime in K above p. Then the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions (A, r) with $A \in \mathcal{O}_K$ and $r \in \mathbb{N}$.*

Proof. Indeed, by lemma 3.19, we know that a prime q splits completely in $L = K(i)$ if and only if $q \equiv 1 \bmod 8$. On the other hand, we know that a prime q splits in K if and only if $(\frac{-2}{q}) = 1$, i.e., if and only if $q \equiv 1 \bmod 8$ or $q \equiv 3 \bmod 8$. Thus, the prime $\mathfrak{p}$ must be inert in L, since otherwise, the prime p would split completely in L. Then rewriting the equation in the form $(A - 8i)(A + 8i) = \pi^{2r+1}$ and taking norms, we get to a contradiction. □

Lemma 4.14 *Let p be a prime such that $p \equiv 5, 7 \bmod 8$. Then the equation $A^2+64 = \pm p^{2r+1}$ has no solutions (A, r) with $A \in \mathcal{O}_K$, and $r \in \mathbb{N}$.*

Proof. Such primes p remain prime in K. Writing $A = x + y\sqrt{-2}$, the equation implies $x^2 - 2y^2 + 64 = \pm p^{2r+1}$ and $2xy = 0$. If $x = 0$, the first equation implies $-2y^2 + 64 = \pm p^{2r+1}$, which is impossible, since p is odd. If $y = 0$, the first equation implies $x^2 + 64 = p^{2r+1}$, and this is known to have solutions only for $r = 0$(see [42]), so that then $p \equiv 1 \bmod 8$, contradicting the hypothesis on p. □

Lemma 4.15 *For each prime π not dividing 2 or 3 and fixed $r \in \mathbb{N}$, at most one of the equation $A^2 + 64 = \pi^{2r+1}$ and $A^2 + 64 = -\pi^{2r+1}$ have solutions $A \in \mathcal{O}_K$.*

Proof. Suppose there exist A and B in $\mathcal{O}_K$ such that $A^2 + 64 = \pi^{2r+1}$ and $B^2 + 64 = -\pi^{2r+1}$. Then $A^2 + B^2 = -128$. Write $A = x + y\sqrt{-2}$, $B = s + t\sqrt{-2}$ and $\pi^{2r+1} = u + v\sqrt{-2}$. Since π does not divide 2, u must be odd. We have $x^2 - 2y^2 + 2xy\sqrt{-2} = u + v\sqrt{-2} = -s^2 + 2t^2 - 2st\sqrt{-2}$. Hence, x and s must be odd. The equation $A^2 + B^2 = -128$ gives $x^2 - 2y^2 + s^2 - 2t^2 + 2(xy + st)\sqrt{-2} = -128$, so that $xy = -yt$. Thus, $y \equiv t \bmod 2$. Looking at the equation modulo 4, we get $x^2 - 2y^2 + s^2 - 2t^2 \equiv 0 \bmod 4$, i.e., $2 \equiv 2(y^2 + t^2) \bmod 4$, which is impossible, since y and t have same parity. This gives the result. □

4.4 Proof of the main theorem

Lemma 4.16 *If A is such that $A^2 + 64 = \pi^{2r+1}$, with π dividing a prime $p \equiv 1 \bmod 16$, then A can be chosen so that $A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$. In that case, the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has prime conductor (π). If π divides a prime $p \equiv 9 \bmod 16$, the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ always has bad reduction at π_2.*

Proof. Let π be a prime in K above the rational prime p. By lemma 4.13 and lemma 4.14, the equation $A^2 + 64 = \pi^{2r+1}$ has a solution only when $p \equiv 1 \bmod 8$. The elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has good reduction at π_2 if and only if $A \equiv 1$ or $-1 + 2\sqrt{-2} \bmod 4$, by lemma 4.4 and lemma 4.3. Writing $A = x + y\sqrt{-2}$ and $\pi^{2r+1} = u + v\sqrt{-2}$, with x, y, u and v in $\mathbb{Z}$, we have $x^2 - 2y^2 + 64 + 2xy\sqrt{-2} = u + v\sqrt{-2}$. Since π does not divide 2, u must be odd, and hence x must be odd. Taking norms, we get

$$(x^2 - 2y^2 + 64)^2 + 8x^2y^2 = p^{2r+1}. \tag{4.3}$$

Assume first that $p \equiv 1 \bmod 16$. Then $p^{2r+1} \equiv 1 \bmod 16$. Looking at the equation (4.3) modulo 16, we get $x^4 + 4y^4 + 4x^2y^2 \equiv 1 \bmod 16$. Since x is odd, we have $x^4 \equiv 1 \bmod 16$. Thus, $4y^2(y^2 + x^2) \equiv 0 \bmod 16$ and y must be even. If $y \equiv 0 \bmod 4$, then replacing A by $-A$ if necessary, we have $A \equiv 1 \bmod 4$. If $y \equiv 2 \bmod 4$, then replacing A by $-A$ if necessary, we have $A \equiv -1 + 2\sqrt{-2} \bmod 4$. Thus, by lemma 4.4, the elliptic curve $y^2 = x^2 + Ax^2 - 16x$ has good reduction at π_2. Hence, it has conductor (π).

Assume now that $p \equiv 9 \bmod 16$. Then $p^{2r+1} \equiv 9 \bmod 16$. Looking at the equation (4.3) modulo 16, we get $4y^2(y^2 + x^2) \equiv 8 \bmod 16$. Thus, y must be odd. But in that case, $\pm A \not\equiv 1 \bmod 4$ and $\pm A \not\equiv -1 + 2\sqrt{-2} \bmod 4$. This proves that the curves $y^2 = x^3 \pm Ax^2 - 16x$ do not have good reduction at π_2 when $p \equiv 9 \bmod 16$. □

Let us now give the proof of Theorem 4.1:

Proof of Theorem 4.1.

a) By lemma 2.6, the elliptic curves with prime conductor not dividing 2 or 3 having a K-rational 2-torsion point are of the form $y^2 = x^3 + Ax^2 + Bx$, with $B^2(A^2 - 4B) = u2^8\pi^s$. By lemma 4.12 all of them are of the form (4.1) and (4.2), where A satisfies the equation $A^2 + 64 = \pi^{2r+1}$. By lemma 4.13 and 4.14, the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions when $p \not\equiv 1 \bmod 8$. By lemma 4.16, when the equation $A^2 + 64 = \pi^{2r+1}$ has a solution $A \in \mathcal{O}_K$ with $p \equiv 1 \bmod 16$, then A can be chosen so that the elliptic curve (4.1) has good reduction at π_2. When $p \equiv 9 \bmod 16$, then any elliptic curve of the form $y^2 = x^3 + Ax^2 - 16x$ corresponding to a solution A of $A^2 + 64 = \pi^{2r+1}$ has bad reduction at π_2.

b) By remark 2.12, the hypotheses of theorem 2.11 are satisfied here with $K = \mathbb{Q}(\sqrt{-2})$. The result then follows from theorem 2.11

c) By remark 2.25, the hypotheses of theorem 2.23 and corollary 2.24 are satisfied for $K = \mathbb{Q}(\sqrt{-2})$. The result then follows from corollary 2.24.

4.5 Tables of values A such that $y^2 = x^3 + Ax^2 - 16x$ is an elliptic curve with prime conductor

The tables below give some values of A such that the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ is an elliptic curve with prime conductor (π). Such A must be such that $A^2 + 64 = \pi^{2r+1}$ and A is a square modulo 4.

A	$\pi = A^2 + 64$	p
$-1 + 6\sqrt{-2}$	$-7 - 12\sqrt{-2}$	337
$1 + 4\sqrt{-2}$	$33 + 8\sqrt{-2}$	1217
$3 + 6\sqrt{-2}$	$1 + 36\sqrt{-2}$	2593
$-3 + 4\sqrt{-2}$	$41 - 24\sqrt{-2}$	2833
$1 + 8\sqrt{-2}$	$-63 + 16\sqrt{-2}$	4481
$3 + 2\sqrt{-2}$	$65 + 12\sqrt{-2}$	4513
$5 + 4\sqrt{-2}$	$57 + 40\sqrt{-2}$	6449
$-5 + 6\sqrt{-2}$	$17 - 60\sqrt{-2}$	7489
$5 + 8\sqrt{-2}$	$-39 + 80\sqrt{-2}$	14321
$-9 + 6\sqrt{-2}$	$73 - 108\sqrt{-2}$	28657
$-5 + 10\sqrt{-2}$	$-111 - 100\sqrt{-2}$	32321
$11 + 2\sqrt{-2}$	$177 + 44\sqrt{-2}$	35201
$9 + 8\sqrt{-2}$	$17 + 144\sqrt{-2}$	41761
$7 + 10\sqrt{-2}$	$-87 + 140\sqrt{-2}$	46769
$15 + 2\sqrt{-2}$	$281 + 60\sqrt{-2}$	86161
$-15 + 4\sqrt{-2}$	$257 - 120\sqrt{-2}$	94849
$13 + 8\sqrt{-2}$	$105 + 208\sqrt{-2}$	97553
$-1 + 14\sqrt{-2}$	$-327 - 28\sqrt{-2}$	108497
$9 + 12\sqrt{-2}$	$-143 + 216\sqrt{-2}$	113761
$3 + 14\sqrt{-2}$	$-319 + 84\sqrt{-2}$	115873
$-17 + 2\sqrt{-2}$	$345 - 68\sqrt{-2}$	128273
$-5 + 14\sqrt{-2}$	$-303 - 140\sqrt{-2}$	131009
$-15 + 8\sqrt{-2}$	$161 - 240\sqrt{-2}$	141121
$-11 + 12\sqrt{-2}$	$-103 - 264\sqrt{-2}$	150001
$19 + 2\sqrt{-2}$	$417 + 76\sqrt{-2}$	185441
$15 + 10\sqrt{-2}$	$89 + 300\sqrt{-2}$	187921
$-9 + 14\sqrt{-2}$	$-247 - 252\sqrt{-2}$	188017

A	$\pi = A^2 + 64i$	p
$13 + 12\sqrt{-2}$	$-55 + 312\sqrt{-2}$	197713
$17 + 8\sqrt{-2}$	$225 + 272\sqrt{-2}$	198593
$-19 + 4\sqrt{-2}$	$393 - 152\sqrt{-2}$	200657
$-3 + 16\sqrt{-2}$	$-439 - 96\sqrt{-2}$	211153
$19 + 6\sqrt{-2}$	$353 + 228\sqrt{-2}$	228577
$-15 + 12\sqrt{-2}$	$1 - 360\sqrt{-2}$	259201
$-21 + 6\sqrt{-2}$	$433 - 252\sqrt{-2}$	314497
$17 + 12\sqrt{-2}$	$65 + 408\sqrt{-2}$	337153
$-1 + 18\sqrt{-2}$	$-583 - 36\sqrt{-2}$	342481
$-11 + 16\sqrt{-2}$	$-327 - 352\sqrt{-2}$	354737
$23 + 2\sqrt{-2}$	$585 + 92\sqrt{-2}$	359153
$7 + 18\sqrt{-2}$	$-535 + 252\sqrt{-2}$	413233
$-17 + 14\sqrt{-2}$	$-39 - 476\sqrt{-2}$	454673
$-25 + 2\sqrt{-2}$	$681 - 100\sqrt{-2}$	483761
$-23 + 8\sqrt{-2}$	$465 - 368\sqrt{-2}$	487073
$-15 + 16\sqrt{-2}$	$-223 - 480\sqrt{-2}$	510529
$11 + 18\sqrt{-2}$	$-463 + 396\sqrt{-2}$	528001
$-3 + 20\sqrt{-2}$	$-727 - 120\sqrt{-2}$	557329
$-25 + 6\sqrt{-2}$	$617 - 300\sqrt{-2}$	560689
$17 + 16\sqrt{-2}$	$-159 + 544\sqrt{-2}$	617153
$-23 + 12\sqrt{-2}$	$305 - 552\sqrt{-2}$	702433
$-25 + 10\sqrt{-2}$	$489 - 500\sqrt{-2}$	739121
$13 + 20\sqrt{-2}$	$-567 + 520\sqrt{-2}$	862289
$29 + 4\sqrt{-2}$	$873 + 232\sqrt{-2}$	869777
$25 + 12\sqrt{-2}$	$401 + 600\sqrt{-2}$	880801
$7 + 22\sqrt{-2}$	$-855 + 308\sqrt{-2}$	920753
$-29 + 6\sqrt{-2}$	$,833 - 348\sqrt{-2}$	936097
$-9 + 22\sqrt{-2}$	$-823 - 396\sqrt{-2}$	990961

Chapter 5

Elliptic curves over $\mathbb{Q}(\sqrt{-3})$

5.1 Main theorem

Let $K = \mathbb{Q}(\sqrt{-3})$. We are interested in finding all the elliptic curves whose conductor is a prime ideal not dividing 2 or 3. Let $\theta = \frac{1+\sqrt{-3}}{2}$. Then the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\theta]$.

The main theorem of this chapter is the following:

Theorem 5.1 *a) Let p be a prime distinct from 2, 3, 17 and 241. Let $\mathfrak{p}$ be a prime in K above p. Then there is an elliptic curve with prime conductor $\mathfrak{p}$ and K-rational two-torsion points if and only if, for some generator π of $\mathfrak{p}$, the equation $x^2 + 64 = w\pi^{2r+1}$, with w a non-square unit in $\mathcal{O}_K$, has solutions (A, r), $A \in \mathcal{O}_K$, $r \in \mathbb{N}$, with $A \equiv \alpha^2 \bmod 4$. The corresponding elliptic curves are*

$$y^2 = x^3 + Ax^2 - 16x, \qquad \Delta = 2^{12} w\pi^{2r+1} \tag{5.1}$$

$$y^2 = x^3 - 2Ax^2 + w\pi^{2r+1}x, \qquad \Delta = -2^{12} w^2\pi^{4r+2}. \tag{5.2}$$

b) The equation $x^2 + 64 = w\pi^{2r+1}$ has no solutions if $p \equiv 1 \bmod 3$ and $p \equiv 3 \bmod 4$. Thus any elliptic curve with conductor $\mathfrak{p}$ has no K-rational 2-torsion points when $p \equiv 1 \bmod 3$ and $p \equiv 3 \bmod 4$.

If p is prime in K, then there are solutions only for $r = 0$. Thus, if p is not of the form $p = x^2 + 64$, any elliptic curve with conductor (p) has no K-rational 2-torsion points.

c) Let π be a prime not dividing 2 or 3. If for all the extensions of the form $N = K(\sqrt{\pm\pi})$, the ray class number $h_{(2)}(N)$ is coprime to 3, then any elliptic curve with prime conductor (π) must have a K-rational 2-torsion point.

Theorem 5.2 *The elliptic curves with conductor* 17 *having* K*-rational* 2*-torsion points are the curves over* $\mathbb{Q}$ *with conductor* 17 *found by Setzer ((1.3), (1.4), (1.5) and (1.6) in the introduction).*

The elliptic curves with prime conductor a prime dividing 241 *having* K*-rational* 2*-torsion points are*

$$y^2 = x^3 + (8+\theta^4)x^2 + 16x, \qquad \Delta = 2^{12}\theta^4(16-\theta), \tag{5.3}$$

$$y^2 = x^3 - (1-17\theta)x^2 - 16x, \qquad \Delta = 2^{12}\theta^2(16-\theta)^2, \tag{5.4}$$

$$y^2 = x^3 + 2(32\theta^5 - 1)x^2 + x, \qquad \Delta = 2^{12}\theta^4(16-\theta), \tag{5.5}$$

$$y^2 = x^3 + 2(1-17\theta)x^2 + \theta^2(16-\theta)^2x, \qquad \Delta = -2^{12}\theta^4(16-\theta)^4, \tag{5.6}$$

and their conjugates.

We have found only one field K and one prime p such that the equation $A^2+64 = u\pi^{2r+1}$ with π a prime in K above p, has a solution $A \in \mathcal{O}_K$, with u a unit in K and $r > 0$, namely when $K = \mathbb{Q}(\sqrt{-3})$, $p = 73$, $\pi = 8+\theta$ and $r = 1$. Since in this case, $A^2 + 64 = \pi$ also has a solution, we obtain 4 distinct elliptic curves with conductor (π):

$$y^2 = x^3 + (4-9\theta)x^2 - 16x, \qquad \Delta = 2^{12}\theta(8+\theta), \tag{5.7}$$

$$y^2 = x^3 - 2(4-9\theta)x^2 + \theta(8+\theta)x, \qquad \Delta = -2^{12}\theta^2(8+\theta)^2, \tag{5.8}$$

$$y^2 = x^3 + (-9-19\theta)x^2 - 16x, \qquad \Delta = 2^{12}\theta(8+\theta)^3, \tag{5.9}$$

$$y^2 = x^3 + 2(9+19\theta)x^2 + \theta(8+\theta)^3x, \qquad \Delta = -2^{12}\theta^2(8+\theta)^6. \tag{5.10}$$

Corollary 5.3 *a) There are no elliptic curves over* $\mathbb{Q}(\sqrt{-3})$ *with prime conductor dividing* $p =$ 2, 3, 5, 7, 19, 31, 43, 67, 71, 79, 127, 139, 149, 151, 163, 167, 199, 211, 223, 263, 271, 307, 317, 331, 367, 463, 487, 499, 571, 607, 619, 631, 643, 691, 727, 739, 751, 811, 823, 859, 883, 911, 941, 967, *and* 991.

b) Any elliptic curve with conductor (π) *dividing* $p =$ 13, 37, 61, 73, 97, 109, 157, 181, 193, 229, 277, 313, 337, 349, 373, 397, 409, 421, 457, 541, 601, 661, 709, 733, 769,

829, 877, 937 *and* 997 *must have a* K*-rational* 2*-torsion point and discriminant* Δ *such that* $\mathrm{ord}_\pi(\Delta) > 1$.

c) There are at least 4 *elliptic curves with prime conductor dividing* 73. *Any such elliptic curve must have a* K*-rational* 2*-torsion point.*

Proof.

a) Let p be a prime in the list a). We note first that there are no elliptic curves defined over K with prime conductor (2) or $(\sqrt{-3})$ (see Table 4 in [37] and Table 2 in [39]). If $p \neq 2, 3$, then it satisfies the condition c) of theorem 5.1. If p is prime in K, then it is not of the form $p = x^2 + 64$. Thus there are no elliptic curves with conductor (p). If p splits in K, and π is inert in $K(i)$, then by b), the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions. Thus by b) and c) of theorem 5.1, there are no elliptic curves with conductor (π).

b) Let p be a prime appearing in the list b). Then it satisfies the conditions of theorem 5.1, c). The first statement follows from this. The second statement follows from the tables at the end this chapter.

c) The prime 73 satisfies the conditions c) of theorem 5.1, c). Thus, any elliptic curve with prime conductor dividing 73 must have a K-rational 2-torsion point. The tables at the end show 2 elliptic curves with prime conductor dividing 73. The 2-isogenies of those elliptic curves also have prime conductor dividing 73. □

5.2 Elliptic curves $y^2 = x^3 + Ax^2 + Bx$

We are now going to find the elliptic curves over K with prime conductor (π) not dividing 2 or 3, admitting a K-rational 2-torsion point. Any such elliptic curve has an equation of the form $y^2 = x^3 + Ax^2 + Bx$ with $B^2(A^2 - 4B) = 2^8 u\pi^s$, where u is a unit in K and $s \in \mathbb{N}$.

We will use the following lemmas several times:

Lemma 5.4 *a) If $v^3 = 1$, then $y^2 = x^3 + av^{-1}x^2 + bvx$ and $y^2 = x^3 + avx^2 + bv^2x$ are isomophirc to $y^2 = x^3 + ax^2 + bx$.*

b) If $v^3 = -1$, then $y^2 = x^3 + av^{-1}x^2 + bvx$ is isomorphic to $y^2 = x^3 - ax^2 - bx$.

c) If $v^3 = -1$, then $y^2 = x^3 + avx^2 + bv^2x$ is isomorphic to $y^2 = x^3 - ax^2 + bx$.

Proof.

a) Since $v^3 = 1$, we have $v^{-1} = v^2$ and $v = v^4$. We have $y^2 = x^3 + av^{-1}x^2 + bvx = x^3 + av^2x^2 + bvx$. Putting $X = vx$, $Y = y$, we get $Y^2 = X^3 + aX^2 + bX$. For the second equation, we have $y^2 = x^3 + avx^2 + bv^2x = x^3 + av^4x^2 + bv^2x$. Putting $X = v^2x$, $Y = y$, we get $Y^2 = X^3 + aX^2 + bX$.

b) Since $v^3 = -1$, we have $v^{-1} = -v^8$ and $v = -v^4$. We have $y^2 = x^3 + av^{-1}x^2 + bvx = x^3 - av^8x^2 - bv^4x$. Putting $X = v^4x$ and $Y = y$, we get $Y^2 = X^3 - aX^2 - bX$.

c) We have $y^2 = x^3 + avx^2 + bv^2x = x^3 - av^4x^2 + bv^2x$. Putting $X = v^2x$, $Y = y$, we get $Y^2 = X^3 - aX^2 + bX$.

The next three lemmas are diophantine lemmas that we will use to find the elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with prime conductor.

Lemma 5.5 *a) Let π be a prime of K. If v and w are units in K, then $16v + w = u\pi^n$ only when $v\bar{w}$ is an even power s of θ. When s is 2 or 4, there are solutions only for $n = 1$, and the prime π is a prime above 241. When $s = 0$, there are solutions only when $n = 1$, and the prime π is 17.*

b) The equation $16v - w = u\pi^n$ has a solution only when $v\bar{w}$ is an odd power of θ.

Proof. We prove only part *a*). The norm of $16v + w$ is $(16v + w)(16\bar{v} + \bar{w}) = 16^2 + 1 + 16(v\bar{w} + \bar{v}w)$. The possible values for $v\bar{w} + \bar{v}w$ are ± 1 and ± 2. Thus, the possible values for

the norm are 241, 273, 225, 289. There are solutions only when the norm is 241 or $289 = 17^2$. The norm is 241 when $v\bar{w} = \theta^2$ or $v\bar{w} = \theta^4$. In that case, $16v + w$ is itself a prime, so that $n = 1$. The norm is 289 when $v\bar{w} = 1$. In that case, $16v + w = 17\epsilon$, for some unit ϵ. Since 17 is a rational prime which remains prime in K, we have $n = 1$ in this case as well. □

Lemma 5.6 *The equation $A^2 - u \equiv 0 \bmod 64$ has no solutions $A \in \mathcal{O}_K$ when u is an odd power of θ.*

Proof. Write $A = x + y\theta$. Then $A^2 = x^2 - y^2 + (2xy + y^2)\theta$. If $u = \theta$, we have $A^2 - u = x^2 - y^2 + (2xy + y^2 - 1)\theta$. Hence, $x^2 - y^2 \equiv 0 \bmod 64$ and $2xy + y^2 - 1 \equiv 0 \bmod 64$. But this is easily seen to be impossible.

If $u = -1$, then we have $A^2 + 1 = x^2 - y^2 + 1 + (2xy + y^2)\theta$. Hence, $x^2 - y^2 + 1 \equiv 0 \bmod 4$ and $2xy + y^2 \equiv 0 \bmod 64$. This has no solutions as well.

If $u = \theta^5 = 1 - \theta$, then $A^2 - u = x^2 - y^2 - 1 + (2xy + y^2 + 1)\theta$. Hence, $x^2 - y^2 + 1 \equiv 0 \bmod 64$ and $2xy + y^2 + 1 \equiv 0 \bmod 64$. But this has no solutions. □

Lemma 5.7 *The equation $\alpha^2 - 64w = u\pi^{2r}$, where u and w are odd powers of θ, and π is coprime to 2, has no solutions.*

Proof. Write $w = \theta^{2s+3}$ and $u = \theta^{2t+1}$. Let $\beta = \theta^{-s}\alpha$. Then $\beta^2 + 64 = \theta^{2(t-s)+1}\pi^{2r}$. Thus, it suffices to prove that the equation $\alpha^2 + 64 = u\pi^{2r}$, with u an odd power of θ, has no solutions. Let us write $\alpha = a + b\theta$ and $\pi^r = s + t\theta$. The norm of π^r is then $s^2 + st + t^2$. Since π is coprime to 2, $s^2 + st + t^2$ must be an odd number, and hence, either s is even, in which case t must be odd, or s is odd, which imposes no conditions on t. First, consider the case when $u = \theta^3$; then the equation is $\alpha^2 + 64 = -\pi^{2r}$. This implies $a^2 - b^2 + 64 = -s^2 + t^2$ and $2ab + b^2 = -2st - t^2$. These equations can be rewritten as $a^2 + s^2 + 64 = b^2 + t^2$ and $b^2 + t^2 = -2(st + ab)$. From the second equation, we can deduce that $b \equiv t \bmod 2$. If $b \equiv t \equiv 1 \bmod 2$, then the second equation implies that $st + ab \equiv 1 \bmod 2$, and hence that $s \not\equiv a \bmod 2$. But this condition is not compatible with the first equation. If $b \equiv t \equiv 0 \bmod 2$, then $b^2 + t^2 \equiv 0 \bmod 4$, and the first equation implies that $a^2 + s^2 \equiv 0 \bmod 4$, so that $a \equiv s \equiv 0 \bmod 2$. But again

this is impossible, since when s is even, t must be odd. We conclude that the equation $\alpha^2 + 64 = -\pi^{2r}$ has no solutions.

Suppose now that $u = \theta$. Then, the equation becomes $\alpha^2 + 64 = \theta\pi^{2r}$, which implies $a^2 - b^2 + 64 = -2st - t^2$ and $2ab + b^2 = s^2 + 2st$. From the second equation, we can see that we must have $s \equiv b \bmod 2$. If $s \equiv b \equiv 1 \bmod 2$, then looking at the second equation modulo 4, we can see that $2ab \equiv 2st \bmod 4$, and hence $ab \equiv st \bmod 2$, so that $a \equiv t \bmod 2$. But this is incompatible with the first equation. Now, if $s \equiv b \equiv 0 \bmod 2$, looking at the first equation modulo 4, we see that $a^2 + t^2 \equiv 0 \bmod 4$, so that $a \equiv t \equiv 0 \bmod 2$, which again contradicts the hypothesis on s and t. We conclude that there are no solutions in this case too.

Lastly, suppose that $u = \theta^5$. Then the equation becomes $\alpha^2 + 64 = \theta^5\pi^{2r}$, which implies that $a^2 - b^2 + 64 = s^2 + 2st$ and $2ab + b^2 = -s^2 + t^2$. Adding the two equations, we get $a^2+2ab+64 = 2st+t^2$, from which we can deduce that $a \equiv t \bmod 2$. If $a \equiv t \equiv 1 \bmod 2$, then looking this last equation modulo 8, we deduce that $ab \equiv st \bmod 4$, so that $b \equiv s \bmod 2$. But this is incompatible with the second equation. Now, if $a \equiv t \equiv 0 \bmod 2$, looking at the third equation modulo 8, we deduce that $b \equiv s \equiv 0 \bmod 2$, which again contradicts the hypothesis on s and t.

We can thus conclude that the equation $\alpha^2 + 64 = u\pi^{2r}$, where u is an odd power of θ, has no solutions. □

Let us now find the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ over K that have prime conductor (π) not dividing 2 or 3. Considering an equation of the form (2.2), we must have $\mathrm{ord}_{\pi_2}(a_1) = 1$ by lemma 2.5. Then, by lemma 2.7, A and B cannot be simultaneously divisible by π_2. Hence, from now on in this section, we consider equation $y^2 = x^3 + Ax^2 + Bx$ such that A and B are not simultaneously divisible by 2. Any elliptic curve over K with prime conductor not dividing 2 or 3 has an equation of this type.

Lemma 5.8 *The elliptic curves of the form* $y^2 = x^3 + Ax^2 + Bx$ *with prime conductor* (π) *not dividing* 2 *or* 3*, such that* $B^2(A^2-4B) = 2^8 u\pi^{2r+1}$ *are the curves (1.4), (1.5), (5.3), (5.5) and the curves of the form (5.1).*

Proof. B cannot be divisible by π. If 2 divides B, then $B = 16v$, where v is a unit. If 2 does not divide B, then $B = v$ is a unit v.

If $B = 16v$, the equation becomes, after simplification, $(Av)^2 - 64v^3 = u\pi^{2r+1}$. Let $\alpha = Av$. The values that v^3 can take are ± 1.

If $v^3 = 1$, the equation is $\alpha^2 - 64 = u\pi^{2r+1}$, which can be rewritten as $(\alpha - 8)(\alpha + 8) = u\pi^{2r+1}$. Since π cannot divide $\alpha - 8$ and $\alpha + 8$ simultaneously, $\alpha - 8$ or $\alpha + 8$ must be units. If $\alpha - 8 = w$, with w a unit, we get $(\alpha - 8)(\alpha + 8) = w(16 + w) = \pi^{2r+1}$. By lemma 5.5, there are solutions only when $w = 1, \theta^2$ or θ^4. If $w = 1$, we get $\alpha = 9$, and the corresponding elliptic curve is $y^2 = x^3 + 9v^{-1}x^2 + 16vx$, which is isomorphic to the curve (1.5), by lemma 5.4. Now, if $w = \theta^4$, we get $\alpha = 8 + \theta^4$ and the corresponding elliptic curve is $y^2 = x^3 + (8 + \theta^4)v^{-1}x^2 + 16vx$, which is isomorphic to (5.3). If $w = \theta^2$, we get the conjugate curve. Now, if $\alpha + 8 = w$, with w a unit, all the curves that we get from this case do not have good reduction at 2.

If $v^3 = -1$, the equation is $\alpha^2 + 64 = u\pi^{2r+1}$, and the corresponding elliptic curve is $y^2 = x^3 - \alpha v^{-1}x^2 + 16vx$, which is isomorphic to $y^2 = x^3 + \alpha x^2 - 16x$. This is a curve of the form (5.1).

When $B = v$, the equation becomes $(Av)^2 - 4v^3 = u2^8\pi^{2r+1}$. Let $\alpha = Av$. We can see that α must be of the form $\alpha = 2C$, and the equation becomes $C^2 - v^3 = 64u\pi^{2r+1}$. If $v^3 = -1$, then there are no solutions, by lemma 5.6.

Now, if $v^3 = 1$, then the equation becomes $(C - 1)(C + 1) = 64u\pi^{2r+1}$. Since π cannot divide simultaneously $C + 1$ and $C - 1$, we have $C + 1 = 2w$, $C + 1 = 32w$, $C - 1 = 2w$ or $C - 1 = 32w$. If $C + 1 = 2w$, we get $(C + 1)(C - 1) = 2w(2w - 2) = 4w(w - 1)$, which cannot be a multiple of 64. If $C + 1 = 32w$, we get $(C + 1)(C - 1) = 32w(32w - 2) = 64w(16w - 1) = 64u\pi^{2r+1}$. By lemma 5.5, this has a solution only when w is an odd power of θ. If $w = \theta^5$,

then $C = 32\theta^5 - 1$, and the corresponding curve is $y^2 = x^3 + 2(32\theta^5 - 1)v^{-1}x^2 + vx$, which is isomorphic to the curve (5.5), by lemma 5.4. If $w = \theta$, we get the conjugate curve. If $w = -1$, we get $C = -33$, and the corresponding curve is $y^2 = x^3 - 66v^{-1}x^2 + vx$, which is isomorphic to the curve (1.4). The cases $C - 1 = 2w$ or $C - 1 = 32w$ can be solved similarly. However, the corresponding elliptic curves have bad reduction at 2. □

Lemma 5.9 *The elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3, such that $B^2(A^2 - 4B) = u2^8\pi^{2r}$, with u a square unit, are the curves (5.4) and its conjugate, and (1.3).*

Proof. In this case, u is an even power of θ. Then $A^2 - 4B$ is a square, so that $X^3 + AX^2 + BX = 0$ has its three roots in $\mathcal{O}_K$, say $0, a, b$ with $a, b \not\equiv 0 \bmod \pi$ and $a \equiv b \bmod \pi$. We then have $B = ab$ and $A = -a - b$, and $a^2b^2(a - b)^2 = u2^8\pi^{2r}$. By hypothesis, π does not divide a and b. In addition, π_2 divides one and only one of a and b. Let say it divides a. Then $a = 16v$ and $b = w$, where v and w are units. The equation then becomes, after simplification, $(vw)^2(16v - w)^2 = u\pi^{2r}$. This has a solution only if $16v - w$ is of the form $16v - w = \epsilon\pi^n$, where ϵ is a unit. Let β be such that $\bar{\beta} = v\bar{w}$. By lemma 5.5, $\bar{\beta}$ must be an odd power of θ, i.e., $\bar{\beta} = -1$, θ or θ^5. If $\bar{\beta}$ is an odd power of θ, so is β. Solving for w, we get that $w = \beta v$. Thus, $A = -(16 + \beta)v$ and $B = 16v^2\beta$. If $v^3 = 1$, the corresponding elliptic curves are $y^2 = x^3 - (16 + \theta)vx^2 + 16\theta v^2x$, $y^2 = x^3 - 15vx^2 - 16v^2x$ and $y^2 = x^3 - (16 + \theta^5)vx^2 + 16\theta^5v^2x$, with v an odd power of θ, which are isomorphic to $y^2 = x^3 - (1 - 17\theta)x^2 - 16x$, $y^2 = x^3 - 15x - 16x$ and $y^2 = x^3 - (1 - 17\theta^5)x^2 - 16x$. They all have good reduction at 2. The first is the curve (5.4), the third is its conjugate, and the second is the curve (1.3).

When $v^3 = -1$, all the corresponding elliptic curves have bad reduction at 2. □

Remark 5.10 The curves in lemma 5.9 are of the form $y^2 = x^3 + Ax^2 + Bx$, with $B = -16$ and $A^2 + 64 = \pi^2$. Let u be a square unit. From the lemma above, we can deduce that the only elliptic curves of the form $y^2 = x^3 + Ax^2 - 16x$ with prime conductor (π) not dividing 2 or 3 such that $A^2 + 64 = u\pi^{2r}$ are the curves (5.4) and its conjugate, and the curve (1.3).

Lemma 5.11 *The curves of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3, such that $B^2(A^2 - 4B) = u2^8\pi^{2r}$ with u a unit that is not a square, are the curves (1.6), (5.6) and its conjugate, (5.2) and its conjugate.*

Proof. In this case, u is an odd power of θ. Note that $\theta^3 = -1$ and $\theta^5 = 1 - \theta$. There are four cases, depending on whether π and $\pi_2 = 2$ divide B.

If 2 and π divide B, we have $B = 16v\pi^r$. The equation becomes, after simplification, $(Av)^2 - 64v^3\pi^r = u$, i.e. $\alpha^2 - u = \pm 64\pi^r$, where $\alpha = Av$. But this equation has no solutions, by lemma 5.6.

If 2 divides B, but π does not, then $B = 16v$. The equation becomes, after simplification, $\alpha^2 - 64v^3 = u\pi^{2r}$, where $\alpha = Av$. If $v^3 = 1$, the equation is $\alpha^2 - 64 = u\pi^{2r}$, which can be rewritten as $(\alpha - 8)(\alpha + 8) = u\pi^{2r}$. Since π cannot divide simultaneously $\alpha - 8$ and $\alpha + 8$, either $\alpha - 8$ or $\alpha + 8$ is a unit. If $\alpha - 8 = w$, with w a unit, we get $(\alpha - 8)(\alpha + 8) = w(16 + w)$. The equation becomes $w(16+w) = u\pi^{2r}$. By lemma 5.5, this has no solutions. Similarly, there are no solutions with $\alpha + 8 = w$ a unit. If $v^3 = -1$, the equation becomes $\alpha^2 + 64 = u\pi^{2r}$, which has no solutions, by lemma 5.7.

If π divides B, but 2 does not, then $B = v\pi^r$. The equation becomes, after simplification, $(Av)^2 - 4v^3\pi^r = 2^8u$, or $\alpha^2 - 4v^3\pi^r = 2^8u$. We must have that $\alpha = 2C$, so that $C^2 - v^3\pi^r = 64u$. The corresponding curve is $y^2 = x^3 + 2Cv^{-1}x^2 + v\pi^r x$. If r is odd, write $r = 2t + 1$. Since $v^3 = \pm 1$, it can be absorbed in π^{2t+1}, and the equation can simply be written in the form $C^2 - 64u = \pi^{2t+1}$. Multiplying by u^2, we get $(uC)^2 + 64 = u^2\pi^{2t+1}$. Let $\gamma = uC$. Thus, $\gamma^2 + 64 = u^2\pi^{2t+1}$. Then, the corresponding elliptic curve is $y^2 = x^3 + 2\gamma u^{-1}x^2 + \pi^{2t+1}x$. This curve is isomorphic to $y^2 = x^3 - 2\gamma x^2 + u^2\pi^{2t+1}x$, by lemma 5.4. This is a curve of the form (5.2).

If $r = 2t$ even and $v^3 = 1$, the equation becomes $C^2 - 64u = \pi^{2t}$. Multiplying by u^2, we get $(uC)^2 + 64 = u^2\pi^{2t}$. Let $\gamma = uC$. Then $\gamma^2 + 64 = u^2\pi^{2t}$. The corresponding elliptic curves are of the form $y^2 = x^3 + 2\gamma u^{-1}x^2 + \pi^{2t}x$ which are isomorphic to

$$y^2 = x^3 - 2\gamma x^2 + u^2\pi^{2t}x, \tag{5.11}$$

by lemma 5.4. These curves (5.11) are the 2-isogenies of the curves $y^2 = x^3 + \gamma x^2 - 16x$, with $\gamma^2 + 64 = u^2\pi^{2t}$. Thus, by the remark 5.10, they are $y^2 = x^3 + 2(1 - 17\theta)x^2 + \theta^2(16 - \theta)^2 x$ and its conjugate, which are the curve (5.6) and its conjugate, and $y^2 = x^3 + 30x^2 + 89x$, which is the curve (1.6).

If $r = 2t$ even and $v^3 = -1$, the equation becomes $C^2 + \pi^{2t} = 64u$, i.e., $C^2 - 64u = -\pi^{2t}$. This equation has no solutions, by lemma 5.7

Finally, if neither 2 nor π divides B, then $B = v$, with v a unit. The equation becomes $v^2(A^2 - 4v) = 2^8\pi^{2r}u$, or $\alpha^2 - 4v^3 = 2^8\pi^{2r}u$ where $\alpha = Av$. We can see that $\alpha = 2C$ for some C in $\mathcal{O}_K$. We then get the equation $C^2 - v^3 = 64\pi^{2r}u$. If $v^3 = 1$, we get $(C-1)(C+1) = 64\pi^{2r}u$. Since π cannot divide simultaneously $C-1$ and $C+1$, we must have $C-1 = 2w$, $C-1 = 32w$, $C + 1 = 2w$ or $C + 1 = 32w$, with w a unit. If $C - 1 = w$, we get $(C - 1)(C + w) = 2w(2w + 2) = 4w(w + 1)$, which cannot possibly be a multiple of 64. If $C - 1 = 32w$, then $(C-1)(C+1) = 32w(32w+2) = 64w(16+w) = 64\pi^{2r}u$. By lemma 5.5, $16+w$ cannot possibly be of the form π^{2r}, with π a prime. If $v^3 = 1$, then the equation becomes $C^2 + 1 = 64\pi^{2r}u$. This has no solutions, by lemma 5.6. □

Lemma 5.12 *The elliptic curves over K of prime conductor with prime conductor (π) not dividing 2, 3, 17 or 241 are the elliptic curves of the form (5.1) and (5.2).*

Proof. Let E/K be an elliptic curve over K with prime conductor (π) not dividing 2 or 3, admitting a K-rational 2-torsion point. Consider a global minimal equation of the form (2.2) for E/K. Then, by lemma 2.5, we must have $\mathrm{ord}_{\pi_2}(a_1) = 0$. In that case, the elliptic curve E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, by lemma 2.7. By lemma 5.9, 5.8 and 5.11, the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ that have prime conductor (π) not dividing 2, 3, 17 or 241 are the elliptic curves of the form (5.1) and (5.2). □

5.3 The equation $x^2 + 64 = w\pi^{2r+1}$.

As seen in the previous section, any elliptic curve with prime conductor (π) not dividing 2, 3, 17 or 241 having a K-rational 2-torsion point is of the form $y^2 = x^3 + Ax^2 - 16x$ or

$y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x$, with $A^2 + 64 = w\pi^{2r+1}$, w a unit in K. We now study the equation $x^2 + 64 = w\pi^{2r+1}$.

Lemma 5.13 *Let $L = K(i)$. Let p be a prime of $\mathbb{Q}$. It splits completely in L if and only if $(\frac{-1}{p}) = 1$ and $(\frac{-3}{p}) = 1$ if and only if $p \equiv 1 \bmod 12$.*

Proof. The field L is a compositum of the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Thus a prime p splits completely in L if and only if it splits in both of the above quadratic fields, which is equivalent to say that $(\frac{-1}{p}) = 1$ and $(\frac{-3}{p}) = 1$ which is equivalent to $p \equiv 1 \bmod 12$. □

Lemma 5.14 *If p is a prime such that $p \equiv 1 \bmod 3$ and $p \equiv 3 \bmod 4$, and if $\mathfrak{p} = (\pi)$ is a prime above p, then the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions (A, r) with $A \in \mathcal{O}_K$, and $r \in \mathbb{N}$.*

Proof. We know that a prime q of $\mathbb{Q}$ splits completely in L if and only if $q \equiv 1 \bmod 3$ and $q \equiv 1 \bmod 4$. A prime q splits in K if and only if $q \equiv 1 \bmod 3$. Thus, if $\mathfrak{p} = (\pi)$ is a prime above satisfying the hypotheses of the lemma, it must be inert in L. Then writing the equation in the form $(A - 8i)(A + 8i) = \pi^{2r+1}$, we have that $A \pm 8i = \epsilon\pi^{2r+1}$, and taking norms leads to a contradiction. □

Lemma 5.15 *Let p be a rational prime that remains prime in K. Then $A^2 + 64 = up^{2r+1}$ only if $r = 0$, $u = 1$ and $p = 37$ or p is of the form $p = a^2 + 64$ with $a \in \mathbb{Z}$. We have $37 = (\pm 3\sqrt{-3})^2 + 64$.*

Proof. This follows from lemma 2.28. □

Remark 5.16 Note that the solutions $A = \pm 3\sqrt{-3}$ do not correspond to elliptic curves with prime conductor. Indeed, the corresponding curves are $y^2 = x^3 \pm 3\sqrt{-3}x^2 - 16x$. To check whether these elliptic curves have good reduction at 2, we use lemma 2.8. Using the notations of lemma 7.4, when $d = -3$, we have $\theta = (1 + \sqrt{-3})/2$, $\gamma = -1$. We must check whether $A \equiv 1, 3\theta,$ or $-1 + \theta \bmod 4$. If $A = 3\sqrt{-3}$, we get $A = 3 - 6\theta \equiv 3 + 2\theta \bmod 4$. If $A = -3\sqrt{-3}$, we get $A = -3 + 6\theta \equiv 1 + 2\theta \bmod 4$. Hence $A \not\equiv 1, 3\theta$ or $-1 + \theta \bmod 4$. We conclude that the elliptic curves $y^2 = x^3 \pm 3\sqrt{-3}x^2 - 16x$ do not have prime conductor.

5.4 Proof of the Main Theorem

Proof of Theorem 5.1.

a) By lemma 5.12, any elliptic curve with prime conductor not dividing 2, 3, 17 and 241, having a K-rational 2-torsion point is of the form (5.1) or (5.2) where A satisfies $A^2 + 64 = w\pi^{2r+1}$. Conversely, if A is such that $A^2 + 64 = w\pi^{2r+1}$ and A is a square modulo 4, then the corresponding curve (5.1) has discriminant $\Delta = 2^{12}w\pi^{2r+1}$, $c_4 = 16(A^2 + 48)$. Thus, this elliptic curve has good reduction everywhere outside 2 and π and multiplicative reduction at π. By lemma 2.8, it has good reduction at 2 as well. Hence, its conductor is (π).

b) By lemma 5.14, the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions. Then, from part a), any elliptic curve with conductor (π) does not have K-rational 2-torsion points.

c) By remark 2.12, the hypotheses of theorem 2.11 are satisfied here with $K = \mathbb{Q}(\sqrt{-3})$. The result then follows from theorem 2.11 □

5.5 Tables of values A such that $y^2 = x^3 + Ax^2 - 16x$ is an elliptic with prime conductor

We give below values of $A \in \mathcal{O}_K$ such that $A \equiv \alpha^2 \bmod 4$ and $A^2 + 64$ is a prime π of $\mathcal{O}_K$ above a prime p of $\mathbb{Q}$. For each such value A, the elliptic curve $y^2 = x^3 - Ax^2 - 16x$ is an elliptic curve with conductor $\mathfrak{f} = (\pi)$. Note that in the third line (with a $*$ sign), the value $A^2 + 64$ is really $A^2 + 64 = \theta\pi^3$ and not $A^2 + 64 = \pi$. This is the only case where we find A such that $A^2 + 64 = w\pi^{2r+1}$ with $r > 0$. All the other values of A are such that $A^2 + 64 = \pi$.

A	$\pi = A^2 + 64$	p
$-1/2 + 9/2\sqrt{-3}$	$7/2 - 9/2\sqrt{-3}$	73
$-37/2 + 19/2\sqrt{-3}$	$271/2 - 703/2\sqrt{-3}$	73 $*$
5	89	89
-7	113	113
13	233	233
17	353	353
-23	593	593
-35	1289	1289
37	1433	1433
-43	1913	1913
-47	2273	2273
$-1 + 6\sqrt{-3}$	$-43 - 12\sqrt{-3}$	2281
$-5/2 + 11/2\sqrt{-3}$	$-41/2 - 55/2\sqrt{-3}$	2689
$-1 + 2\sqrt{-3}$	$53 - 4\sqrt{-3}$	2857
-55	3089	3089
$-5/2 + 5/2\sqrt{-3}$	$103/2 - 25/2\sqrt{-3}$	3121
$7/2 + 9/2\sqrt{-3}$	$31/2 + 63/2\sqrt{-3}$	3217
$7/2 + 7/2\sqrt{-3}$	$79/2 + 49/2\sqrt{-3}$	3361
$3 + 2\sqrt{-3}$	$61 + 12\sqrt{-3}$	4153
$-5/2 + 3/2\sqrt{-3}$	$127/2 - 15/2\sqrt{-3}$	4201
65	4289	4289
$3/2 + 13/2\sqrt{-3}$	$-121/2 + 39/2\sqrt{-3}$	4801
$3 + 6\sqrt{-3}$	$-35 + 36\sqrt{-3}$	5113
$-9/2 + 7/2\sqrt{-3}$	$95/2 - 63/2\sqrt{-3}$	5233
73	5393	5393

A	$\pi = A^2 + 64$	p
$7/2 + 1/2\sqrt{-3}$	$151/2 + 7/2\sqrt{-3}$	5737
$-5/2 + 13/2\sqrt{-3}$	$-113/2 - 65/2\sqrt{-3}$	6361
$5 + 4\sqrt{-3}$	$41 + 40\sqrt{-3}$	6481
$-5 + 2\sqrt{-3}$	$77 - 20\sqrt{-3}$	7129
97	9473	9473
$11/2 + 11/2\sqrt{-3}$	$7/2 + 121/2\sqrt{-3}$	10993
$-5 + 6\sqrt{-3}$	$-19 - 60\sqrt{-3}$	11161
$7 + 2\sqrt{-3}$	$101 + 28\sqrt{-3}$	12553
$-7 + 4\sqrt{-3}$	$65 - 56\sqrt{-3}$	13633
$15/2 + 1/2\sqrt{-3}$	$239/2 + 15/2\sqrt{-3}$	14449
$15/2 + 7/2\sqrt{-3}$	$167/2 + 105/2\sqrt{-3}$	15241
-127	16193	16193
$15/2 + 9/2\sqrt{-3}$	$119/2 + 135/2\sqrt{-3}$	17209
$-17/2 + 7/2\sqrt{-3}$	$199/2 - 119/2\sqrt{-3}$	20521
$-9/2 + 15/2\sqrt{-3}$	$-169/2 - 135/2\sqrt{-3}$	20809
145	21089	21089
$7 + 6\sqrt{-3}$	$5 + 84\sqrt{-3}$	21193
$-9 + 2\sqrt{-3}$	$133 - 36\sqrt{-3}$	21577
$-13/2 + 13/2\sqrt{-3}$	$-41/2 - 169/2\sqrt{-3}$	21841
$-1/2 + 17/2\sqrt{-3}$	$-305/2 - 17/2\sqrt{-3}$	23473
-163	26633	26633
-167	27953	27953
-175	30689	30689
$-21/2 + 3/2\sqrt{-3}$	$335/2 - 63/2\sqrt{-3}$	31033
$19/2 + 11/2\sqrt{-3}$	$127/2 + 209/2\sqrt{-3}$	36793

A	$\pi = A^2 + 64$	p
193	37313	37313
197	38873	38873
205	42089	42089
$3/2 + 19/2\sqrt{-3}$	$-409/2 + 57/2\sqrt{-3}$	44257
$-21/2 + 11/2\sqrt{-3}$	$167/2 - 231/2\sqrt{-3}$	46993
$-25/2 + 1/2\sqrt{-3}$	$439/2 - 25/2\sqrt{-3}$	48649
$23/2 + 9/2\sqrt{-3}$	$271/2 + 207/2\sqrt{-3}$	50497
-227	51593	51593
$-21/2 + 13/2\sqrt{-3}$	$95/2 - 273/2\sqrt{-3}$	58153
245	60089	60089
$-25/2 + 9/2\sqrt{-3}$	$319/2 - 225/2\sqrt{-3}$	63409
$11/2 + 19/2\sqrt{-3}$	$-353/2 + 209/2\sqrt{-3}$	63913
-263	69233	69233
265	70289	70289
$-13/2 + 19/2\sqrt{-3}$	$-329/2 - 247/2\sqrt{-3}$	72817
$3/2 + 21/2\sqrt{-3}$	$-529/2 + 63/2\sqrt{-3}$	72937
$-5 + 10\sqrt{-3}$	$-211 - 100\sqrt{-3}$	74521
-275	75689	75689
$-5/2 + 21/2\sqrt{-3}$	$-521/2 - 105/2\sqrt{-3}$	76129
-283	80153	80153
$-29/2 + 5/2\sqrt{-3}$	$511/2 - 145/2\sqrt{-3}$	81049
305	93089	93089
$-15 + 4\sqrt{-3}$	$241 - 120\sqrt{-3}$	101281
-323	104393	104393
$-13/2 + 21/2\sqrt{-3}$	$-449/2 - 273/2\sqrt{-3}$	106297

A	$\pi = A^2 + 64$	p
$27/2 + 13/2\sqrt{-3}$	$239/2 + 351/2\sqrt{-3}$	106681
-335	112289	112289
$31/2 + 9/2\sqrt{-3}$	$487/2 + 279/2\sqrt{-3}$	117673
-347	120473	120473
353	124673	124673
$-9/2 + 23/2\sqrt{-3}$	$-625/2 - 207/2\sqrt{-3}$	129793
-367	134753	134753
$1 + 12\sqrt{-3}$	$-367 + 24\sqrt{-3}$	136417
$35/2 + 3/2\sqrt{-3}$	$727/2 + 105/2\sqrt{-3}$	140401
$-33/2 + 9/2\sqrt{-3}$	$551/2 - 297/2\sqrt{-3}$	142057
377	142193	142193
$35/2 + 5/2\sqrt{-3}$	$703/2 + 175/2\sqrt{-3}$	146521
$17 + 4\sqrt{-3}$	$305 + 136\sqrt{-3}$	148513
-395	156089	156089
-403	162473	162473
$-1/2 + 25/2\sqrt{-3}$	$-809/2 - 25/2\sqrt{-3}$	164089
-407	165713	165713
$15/2 + 23/2\sqrt{-3}$	$-553/2 + 345/2\sqrt{-3}$	165721
$-21/2 + 21/2\sqrt{-3}$	$-313/2 - 441/2\sqrt{-3}$	170353
413	170633	170633
$-15 + 8\sqrt{-3}$	$97 - 240\sqrt{-3}$	182209
$19 + 2\sqrt{-3}$	$413 + 76\sqrt{-3}$	187897
437	191033	191033
$-19 + 4\sqrt{-3}$	$377 - 152\sqrt{-3}$	211441
-463	214433	214433

A	$\pi = A^2 + 64$	p
$35/2 + 13/2\sqrt{-3}$	$487/2 + 455/2\sqrt{-3}$	214561
$31/2 + 17/2\sqrt{-3}$	$175/2 + 527/2\sqrt{-3}$	215953
$39/2 + 7/2\sqrt{-3}$	$815/2 + 273/2\sqrt{-3}$	221953
$9 + 12\sqrt{-3}$	$-287 + 216\sqrt{-3}$	222337
-475	225689	225689
485	235289	235289
-487	237233	237233
497	247073	247073
$17 + 8\sqrt{-3}$	$161 + 272\sqrt{-3}$	247873
$27/2 + 21/2\sqrt{-3}$	$-169/2 + 567/2\sqrt{-3}$	248257
$19 + 6\sqrt{-3}$	$317 + 228\sqrt{-3}$	256441
517	267353	267353
$-11 + 12\sqrt{-3}$	$-247 - 264\sqrt{-3}$	270097
$15 + 10\sqrt{-3}$	$-11 + 300\sqrt{-3}$	270121
$11/2 + 27/2\sqrt{-3}$	$-905/2 + 297/2\sqrt{-3}$	270913
$-1 + 14\sqrt{-3}$	$-523 - 28\sqrt{-3}$	275881
-527	277793	277793
$-25/2 + 23/2\sqrt{-3}$	$-353/2 - 575/2\sqrt{-3}$	279121
$-29/2 + 21/2\sqrt{-3}$	$-113/2 - 609/2\sqrt{-3}$	281353
533	284153	284153
-535	286289	286289
$3 + 14\sqrt{-3}$	$-515 + 84\sqrt{-3}$	286393
553	305873	305873
557	310313	310313
565	319289	319289

A	$\pi = A^2 + 64$	p
-575	330689	330689
$-19 + 8\sqrt{-3}$	$233 - 304\sqrt{-3}$	331537
$39/2 + 15/2\sqrt{-3}$	$551/2 + 585/2\sqrt{-3}$	332569
577	332993	332993
$35/2 + 19/2\sqrt{-3}$	$199/2 + 665/2\sqrt{-3}$	341569
$23 + 2\sqrt{-3}$	$581 + 92\sqrt{-3}$	362953
-607	368513	368513
613	375833	375833
617	380753	380753
$-13/2 + 29/2\sqrt{-3}$	$-1049/2 - 377/2\sqrt{-3}$	381697
$43/2 + 13/2\sqrt{-3}$	$799/2 + 559/2\sqrt{-3}$	393961
-635	403289	403289
$35/2 + 21/2\sqrt{-3}$	$79/2 + 735/2\sqrt{-3}$	406729
$-45/2 + 11/2\sqrt{-3}$	$959/2 - 495/2\sqrt{-3}$	413689
$-41/2 + 17/2\sqrt{-3}$	$535/2 - 697/2\sqrt{-3}$	435913
$-49/2 + 1/2\sqrt{-3}$	$1327/2 - 49/2\sqrt{-3}$	442033
$47/2 + 9/2\sqrt{-3}$	$1111/2 + 423/2\sqrt{-3}$	442777
-667	444953	444953
$11 + 14\sqrt{-3}$	$-403 + 308\sqrt{-3}$	447001
$-9/2 + 31/2\sqrt{-3}$	$-1273/2 - 279/2\sqrt{-3}$	463513
$23 + 6\sqrt{-3}$	$485 + 276\sqrt{-3}$	463753
-683	466553	466553
$-25 + 2\sqrt{-3}$	$677 - 100\sqrt{-3}$	488329
$1 + 16\sqrt{-3}$	$-703 + 32\sqrt{-3}$	497281
$17 + 12\sqrt{-3}$	$-79 + 408\sqrt{-3}$	505633

A	$\pi = A^2 + 64$	p
713	508433	508433
$-49/2 + 9/2\sqrt{-3}$	$1207/2 - 441/2\sqrt{-3}$	510073
-715	511289	511289
$51/2 + 3/2\sqrt{-3}$	$1415/2 + 153/2\sqrt{-3}$	518113
$51/2 + 5/2\sqrt{-3}$	$1391/2 + 255/2\sqrt{-3}$	532489
$-29/2 + 27/2\sqrt{-3}$	$-545/2 - 783/2\sqrt{-3}$	534073
$5 + 16\sqrt{-3}$	$-679 + 160\sqrt{-3}$	537841
737	543233	543233
$-17/2 + 31/2\sqrt{-3}$	$-1169/2 - 527/2\sqrt{-3}$	549937
-743	552113	552113
$7/2 + 33/2\sqrt{-3}$	$-1481/2 + 231/2\sqrt{-3}$	588361
$-53/2 + 3/2\sqrt{-3}$	$1519/2 - 159/2\sqrt{-3}$	595801
773	597593	597593
-775	600689	600689
$-9/2 + 33/2\sqrt{-3}$	$-1465/2 - 297/2\sqrt{-3}$	602713
785	616289	616289
793	628913	628913
$43/2 + 21/2\sqrt{-3}$	$391/2 + 903/2\sqrt{-3}$	649777
$23/2 + 31/2\sqrt{-3}$	$-1049/2 + 713/2\sqrt{-3}$	656377
-815	664289	664289
817	667553	667553
$51/2 + 13/2\sqrt{-3}$	$1175/2 + 663/2\sqrt{-3}$	674833
$39/2 + 25/2\sqrt{-3}$	$-49/2 + 975/2\sqrt{-3}$	713569
$55/2 + 7/2\sqrt{-3}$	$1567/2 + 385/2\sqrt{-3}$	725041
$25 + 8\sqrt{-3}$	$497 + 400\sqrt{-3}$	727009

A	$\pi = A^2 + 64$	p
853	727673	727673
$-17 + 14\sqrt{-3}$	$-235 - 476\sqrt{-3}$	734953
-863	744833	744833
$-37/2 + 27/2\sqrt{-3}$	$-281/2 - 999/2\sqrt{-3}$	768241
$27 + 6\sqrt{-3}$	$685 + 324\sqrt{-3}$	784153
-887	786833	786833
$-41/2 + 25/2\sqrt{-3}$	$31/2 - 1025/2\sqrt{-3}$	788209
$11/2 + 35/2\sqrt{-3}$	$-1649/2 + 385/2\sqrt{-3}$	790969
$23/2 + 33/2\sqrt{-3}$	$-1241/2 + 759/2\sqrt{-3}$	817081
-907	822713	822713
913	833633	833633
$-29 + 2\sqrt{-3}$	$893 - 116\sqrt{-3}$	837817
$-57/2 + 9/2\sqrt{-3}$	$1631/2 - 513/2\sqrt{-3}$	862417
-943	889313	889313
-955	912089	912089
$19/2 + 35/2\sqrt{-3}$	$-1529/2 + 665/2\sqrt{-3}$	916129
$-15 + 16\sqrt{-3}$	$-479 - 480\sqrt{-3}$	920641
$-27 + 8\sqrt{-3}$	$601 - 432\sqrt{-3}$	921073
$47/2 + 23/2\sqrt{-3}$	$439/2 + 1081/2\sqrt{-3}$	924601
965	931289	931289
$-21/2 + 35/2\sqrt{-3}$	$-1489/2 - 735/2\sqrt{-3}$	959449
-983	966353	966353
$11/2 + 37/2\sqrt{-3}$	$-1865/2 + 407/2\sqrt{-3}$	993793
997	994073	994073
$-9 + 18\sqrt{-3}$	$-827 - 324\sqrt{-3}$	998857

Chapter 6

Elliptic curves over $\mathbb{Q}(\sqrt{-7})$

6.1 Main theorem

Let $K = \mathbb{Q}(\sqrt{-7})$. We are interested in finding all the elliptic curves whose conductor is a prime ideal not dividing 2 or 3. We note first that there are no elliptic curves over K with prime conductor dividing 2 (see Table 2 in [38]). Let $\theta = \frac{1+\sqrt{-7}}{2}$. We have that $\mathcal{O}_K = \mathbb{Z}[\theta]$ and 2 splits as $2\mathcal{O}_K = (\theta)(\bar{\theta})$.

The main theorem of this chapter is the following:

Theorem 6.1 *a) Let p be a prime distinct from 2, 3 and 17. Let $\mathfrak{p}$ be a prime above p. There is an elliptic curve with prime conductor $\mathfrak{p}$ and a K-rational 2-torsion point if and only if, for some generator π, the equation $x^2 + 64 = \pi^{2r+1}$ has a solution (A, r), such that $A \equiv \alpha^2 \bmod 4$, with α coprime to 2. Then the corresponding elliptic curves are*

$$y^2 = x^3 + Ax^2 - 16x, \qquad \Delta = 2^{12}\pi^{2r+1}, \tag{6.1}$$

$$y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x, \qquad \Delta = -2^{12}\pi^{4r+2}. \tag{6.2}$$

b) If $(\frac{-7}{p}) = 1$ and $p \equiv 3 \bmod 4$, then the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions. Then, any elliptic curve with conductor (π) has no K-rational 2-torsion points.

If p is prime in K, then there are solutions only for $r = 0$. Thus, if p is not of the form $p = x^2 + 64$, any elliptic curve with conductor (p) has no K-rational 2-torsion points.

c) Let π be a prime not dividing 2 or 3. If for all the extensions of the form $N = K(\sqrt{\pm\pi})$, the ray class number $h_{(2)}(N)$ is coprime to 3, then any elliptic curve with prime conductor (π) must have a K-rational 2-torsion point.

Theorem 6.2 *The elliptic curves over K with conductor (17) are the elliptic curves over $\mathbb{Q}$ with conductor 17 found by Setzer ((1.3), (1.4), (1.5) and (1.6) in the introduction).*

Corollary 6.3 *a) There are no elliptic curves defined over K with prime conductor (π) dividing $p = 11, 23, 41, 43, 67, 71, 103, 107, 127, 151, 179, 191, 239, 263, 271, 331, 347, 359, 379, 409, 431, 443, 463, 479, 487, 491, 547, 571, 601, 607, 631, 647, 659, 683, 751, 863, 883, 907, 911, 919, 947$ and 967.*

b) The primes $p = 73$ and 353 remain prime in K and are of the form $p = a^2 + 64$ with $a \in \mathbb{Z}$, and the corresponding elliptic curves

$$\begin{aligned} y^2 &= x^3 + ax^2 - 16x, \\ y^2 &= x^3 - 2ax^2 + px, \end{aligned}$$

are the only elliptic curves with conductor (p).

c) Any elliptic curve with conductor (π) dividing $p = 29, 37, 109, 137, 149, 197, 233, 281, 373, 389, 421, 449, 457, 541, 557, 613, 617, 673, 701, 709, 757, 809, 821, 877$ and 953 must have a K-rational 2-torsion point and discriminant Δ such that $\mathrm{ord}_\pi(\Delta) > 1$.

Proof.

a) Let p be a prime appearing in the list a). Then it satisfies the conditions of theorem 6.1 b) and c). Thus, there are no elliptic curves with conductor (p).

b) Let $p = 73$ or 353. Then p satisfies the conditions of theorem 6.1 c). Thus any elliptic curve with conductor (p) must have a K-rational 2-torsion point. By theorem 6.1 b), there are solutions to the equation $x^2 + 64 = p^{2r+1}$ only if $r = 0$. Since p is of the form $p = a^2 + 64$, the result follows from theorem 6.1 a).

c) Let p be a prime appearing in the list c). Then the equation $\pi = x^2 + 64$, with π a prime above p, has no solutions. The prime p satisfies in addition the conditions of theorem 6.1 c). Thus any elliptic curve with conductor (π) must have a K-rational 2-torsion point and discriminant Δ such that $\mathrm{ord}_\pi(\Delta) > 1$. □

6.2 Elliptic curves $y^2 = x^3 + Ax^2 + Bx$ of prime conductor

To find the elliptic curves with prime conductor not dividing 2 and 3, we use lemma 2.5. Hence, all such elliptic curves can be written in the form $y^2 = x^3 + Ax^2 + Bx$, with

$$B^2(A^2 - 4B) = u2^8\pi^s, \tag{6.3}$$

for some prime π not dividing 2 and 3. By lemma 2.7, we know that π (resp. θ, $\bar{\theta}$) cannot divide simultaneously A and B.

Lemma 6.4 *An element $a + b\theta$ of $\mathbb{Z}[\theta]$ is divisible by θ^6 (resp. $\bar{\theta}^6$) if and only if $7a + 10b \equiv 0 \bmod 64$ and $-5a + 2b \equiv 0 \bmod 64$ (resp. $a - 5b \equiv 0 \bmod 32$ and $5a + 7b \equiv 0 \bmod 64$).*

Proof. We have that $\theta^6 = 2 + 5\theta$ so that a multiple of θ^6 is of the form $(2 + 5\theta)(x + y\theta) = 2x - 10y + (5x + 7y)\theta$. Thus $a + b\theta = (2 + 5\theta)(x + y\theta)$, so that $x = \frac{7a+10b}{64}$ and $y = \frac{-5a+2b}{64}$. This implies that $7a + 10b \equiv 0 \bmod 64$ and $-5a + 2b \equiv 0 \bmod 64$. □

Lemma 6.5 *a) The equation $A^2 + 1 \equiv 0 \bmod 64$ has no solutions.*

b) The equation $A^2 + \theta^6 \equiv 0 \bmod \bar{\theta}^6$ has no solutions.

c) The equation $A^2 + \bar{\theta}^6 \equiv 0 \bmod \theta^6$ has no solutions.

Proof. We have $\theta^2 = -2 + \theta$, $\theta^6 = 2 + 5\theta$. Write $A = x + y\theta$ with x, $y \in \mathbb{Z}$. Then $A^2 + 1 = x^2 - 2y^2 + 1 + (2xy + y^2)\theta$ and $A^2 + \theta^6 = x^2 - 2y^2 + 2 + (2xy + y^2 + 5)\theta$.

a) The equation implies $x^2 - 2y^2 + 1 \equiv 0 \bmod 64$ and $2xy + y^2 \equiv 0 \bmod 64$. But this is impossible. The result follows.

b) If $A = x + y\theta$ is a solution of the equation $A^2 + \theta^6 \equiv 0 \bmod \bar{\theta}^6$, then by lemma 6.4, we must have $x^2-2y^2+2-5(2xy+y^2+5) \equiv 0 \bmod 32$ and $5(x^2-2y^2+2)+7(2xy+y^2+5) \equiv 0 \bmod 64$, i.e., $x^2 - 7y^2 - 10xy - 23 \equiv 0 \bmod 32$ and $5x^2 - 3y^2 + 14xy + 45 \equiv 0 \bmod 64$. The first equation implies that $x \equiv y + 1 \bmod 2$, i.e. x and y have distinct parity. If x is even, then we get, using the second equation $y^2 + 1 \equiv 0 \bmod 4$, which is impossible. If x is odd, then using the second equation again, we get $y^2 + 2 \equiv 0 \bmod 4$ which again is impossible. Thus there are no solutions to the equation $A^2 + \theta^6 \equiv 0 \bmod \bar{\theta}^6$.

c) This follows from *b*), by conjugation. □

Lemma 6.6 *a) The equation $A^2 - 1 = 64u\pi^r$ with $u = \pm 1$, π a prime of K not dividing 2, has a solution only when $r = 1$ and $(\pi) = (17)$. The solutions are $A = \pm 33$.*

b) The equation $A^2 - 64 = u\pi^r$ with $u = \pm 1$, π a prime of K not dividing 2, has a solution only when $r = 1$ and $(\pi) = (17)$. The solutions are $A = \pm 9$.

c) The equation $A^2 + 64 = -\pi^{2r}$ where π is a prime not dividing 2, has no solutions.

Proof.

a) The equation can be rewritten as $(A - 1)(A + 1) = 64u\pi^r$. The valuation of $A - 1$ or $A + 1$ at θ or $\bar{\theta}$ is 1 or 5. Furthemore, if π divide one of $A - 1$ or $A + 1$, then it does not divide the other. Thus $A + 1 = \theta^s\bar{\theta}^t w$ or $A - 1 = \theta^s\bar{\theta}^t w$, with $s = 1$ or 5, $t = 1$ or 5 and $w = \pm 1$. Suppose $A + 1 = \theta^s\bar{\theta}^t w$. Then $(A + 1)(A - 1) = \theta^s\bar{\theta}^t w(\theta^s\bar{\theta}^t w - 2) = \theta^{s+1}\bar{\theta}^{t+1} w(\theta^{s-1}\bar{\theta}^{t-1} w - 1) = 64u\pi^r$. Thus, we must have $s = t = 5$. In that case, we get $(A + 1)(A - 1) = 64w(16w - 1) = 64u\pi^r$. There is a solution only when $r = 1$, $w = -1$, since 17 is prime in K, and 15 is composite. When $w = -1$, we get $A = -33$ and $u\pi = 17$. If $A - 1 = \theta^s\bar{\theta}^t w$, we get $r = 1$, $w = 1$, $A = 33$ and $u\pi = 17$.

b) The equation can be rewritten as $(A-8)(A+8) = u\pi^r$. Since π cannot divide $A-8$ and $A + 8$ simultaneously, we have $A - 8 = w$ or $A + 8 = w$, $w = \pm 1$. Suppose $A - 8 = w$.

Then $(A-8)(A+8) = w(w+16) = u\pi^r$. There is a solution only when $r = 1$ and $w = 1$, since 17 is prime in K, and 15 is composite. When $w = 1$, we get $A = 9$ and $u\pi = 17$. If $A + 8 = w$, we get $r = 1$, $w = -1$, $A = -9$ and $u\pi = 17$.

c) Let us write $A = x + y\theta$ and $\pi^r = u + v\theta$. The norm of π^r is an odd prime power. This norm is $(u + v\theta)(u + v\bar{\theta}) = u^2 + uv + 2v^2$, so that u must be odd and v must be even. Furthemore, we have $x^2 - 2y^2 + 64 = -u^2 + 2v^2$ and $2xy + y^2 = -2uv - v^2$. The first equation implies that x and u have same parity, hence they are both odd. The second equation implies that y and v have same parity, hence they are both even. Now looking at the first equation modulo 8, we get an impossibility: indeed, the lefthand side is $x^2 - 2y^2 + 64 \equiv 1 \bmod 8$, whereas the righthand side is $-u^2 + 2v^2 \equiv -1 \bmod 8$. □

Lemma 6.7 *The elliptic curves over K of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3, such that $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$, are the curves (1.4), (1.5), and the elliptic curves of the form (6.1).*

Proof. In that case, π cannot divide B by lemma 2.7.
If θ and $\bar{\theta}$ divide B, then $B = 16v$, where $v = \pm 1$. Indeed, we know, by lemma 2.7, that θ (and $\bar{\theta}$) cannot divide simultaneously A and B. So, if θ and $\bar{\theta}$ divide B, they do not divide A. Hence, since A and B satisfy equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$, we have $B = 16v$, where v is a unit. The equation $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ becomes, after simplification, $A^2 - 64v = \pi^{2r+1}$. If $v = 1$, then the equation is $A^2 - 64 = \pi^{2r+1}$. By lemma 6.6, the solutions are $A = \pm 9$, $r = 0$ and $\pi = 17$. When $A = 9$, the corresponding curve is $y^2 = x^3 + 9x^2 + 16x$, which is the curve (1.5). If $A = -9$, we get a curve which does not have good reduction at 2.

If neither θ nor $\bar{\theta}$ divide B, then $B = v$, with v a unit. The equation becomes $A^2 - 4v = 2^8\pi^{2r+1}$. Then, we must have that A is a multiple of 2: $A = 2C$, for some C in $\mathcal{O}_K$. Simplifying by 4, the equation becomes $C^2 - v = 64\pi^{2r+1}$.

If $v = -1$, then the equation becomes $C^2 + 1 = 64\pi^{2r+1}$, which has no solutions by lemma 6.5. If $v = 1$, the equation can be rewritten as $C^2 - 1 = 64\pi^{2r+1}$. By lemma 6.6, the solutions are $C = \pm 33$, with $r = 0$ and $\pi = 17$. When $C = -33$, the corresponding curve is the curve (1.4). When $C = 33$, the corresponding curve does not have good reduction at the primes dividing 2.

If θ divides B, but $\bar{\theta}$ does not, then $B = \theta^4 v$, where v is a unit. The equation becomes after simplification $A^2 - 4\theta^4 v = \bar{\theta}^8 \pi^{2r+1}$. We can see that A must then be of the form $A = \bar{\theta} C$. The equation then becomes after simplification $C^2 - \theta^6 v = \bar{\theta}^6 \pi^{2r+1}$. First, if $v = -1$, the equation becomes $C^2 + \theta^6 = \bar{\theta}^6 \pi^{2r+1}$. By lemma 6.5, this has no solutions. Now, if $v = 1$, then the equation becomes $C^2 - \theta^6 = \bar{\theta}^6 \pi^{2r+1}$, which can be rewritten as $(C - \theta^3)(C + \theta^3) = \bar{\theta}^6 \pi^{2r+1}$. If π divides one of $C - \theta^3$ or $C + \theta^3$, then it does not divide the other. Also, the valuations of $C \pm \theta^3$ at $\bar{\theta}$ is either 1 or 5. Thus, $C - \theta^3 = \bar{\theta}^s w$ or $C + \theta^3 = \bar{\theta}^s w$, with $s = 1$ or 5, and $w = \pm 1$. If $C - \theta^3 = \bar{\theta}^s w$, we get $(C - \theta^3)(C + \theta^3) = \bar{\theta}^s w(\bar{\theta}^s w + 2\theta^3) = \bar{\theta}^{s+1} w(\bar{\theta}^{s-1} w + \theta^4) = \bar{\theta}^6 \pi^{2r+1}$. If $s = 1$, since $\theta^4 + 1 = 3\bar{\theta}$ and $\theta^4 - 1 = -\bar{\theta}^4$, there are no solutions. If $s = 5$, since $\bar{\theta}^4 + \theta^4 = 1$ and $\bar{\theta}^4 - \theta^4 = 3(-1 + 2\theta)$, there are no solutions. Similarly, there are no solutions when $C + \theta^3 = \theta^s w$.

If $\bar{\theta}$ divides B, but θ does not, then $B = \bar{\theta}^4 v$ and there are no solutions as well. This can be deduced from the previous case. Indeed, if there were solutions (A, B) of the equation $B^2(A^2 - 4B) = 2^8 \pi^{2r+1}$, with B of the above form, then taking conjugates, we would have $\bar{B}^2(\bar{A}^2 - 4\bar{B}) = 2^8 \bar{\pi}^{2r+1}$. But $\bar{B} = \theta^4 v$, and from the previous case, we know that such a $\bar{B}$ does not exist. □

Lemma 6.8 *The only elliptic curve over K of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3, with $B^2(A^2 - 4B) = 2^8 \pi^{2r}$ is the curve (1.3).*

Proof. The equation is then $B^2(A^2 - 4B) = 2^8 \pi^{2r}$, so that $A^2 - 4B$ must be a square, and hence the equation $x^3 + Ax^2 + Bx = 0$ has all its solutions in $\mathcal{O}_K$, say $0, a, b$, with $a, b \not\equiv 0 \bmod \pi$ and $a \equiv b \bmod \pi$. We then have $a^2 b^2 (a - b)^2 = 2^8 \pi^{2r}$. There are only two cases (by symmetry): θ and $\bar{\theta}$ divide a, or θ divides a but $\bar{\theta}$ does not. If θ and $\bar{\theta}$ divide a, we

have $a = \theta^m\bar{\theta}^n v$ and $b = w$, where v and w are units. It can be seen that m and n must be equal to 4, so that $a = 16v$. The equation then becomes $(16v - w)^2 = \pi^{2r}$. There is a solution only for $v = -w$, since 17 is a prime in $\mathbb{Q}(\sqrt{-7})$. We have $B = ab = -16$. If $v = 1$, then $w = -1$ and the corresponding elliptic curve is $y^2 = x^3 - 15x^2 - 16x$, which is the curve (1.3). If $v = -1$, then $w = 1$ and the corresponding elliptic curve is $y^2 = x^3 + 15x^2 - 16x$ which does not have good reduction at the primes dividing 2. If θ divides a, but $\bar{\theta}$ does not, we have $a = \theta^m v$ and $b = \bar{\theta}^n w$, and we can see that m and n must be equal to 4. The equation then becomes $(\theta^4 v - \bar{\theta}^4 w)^2 = \pi^{2r}$. Computing the lefthand side of this equation, it can be seen that it cannot be a prime power. □

Lemma 6.9 *The elliptic curves over K of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3 with $B^2(A^2 - 4B) = -2^8\pi^{2r}$ are the the curve (1.6) and the elliptic curves of the form (6.2).*

Proof. There are several cases, considering whether θ, $\bar{\theta}$ or π divide B. If θ, $\bar{\theta}$ and π divide B, we have $B = \theta^4\bar{\theta}^4\pi^r v = 16\pi^r v$ and the equation becomes $A^2 - 64\pi^r v = -1$, i.e. $A^2 + 1 = 64\pi^r v$. This equation has no solutions, by lemma 6.5.

If θ and π divide, but $\bar{\theta}$ does not, we have $B = \theta^4\pi^r v$ and the equation becomes $A^2 - 4\theta^4\pi^r v = -\bar{\theta}^8$, i.e. $A^2 + \bar{\theta}^8 = 4\theta^4\pi^r v$. We can see that A must be of the form $A = \bar{\theta}C$. After simplification, the equation becomes $C^2 + \bar{\theta}^6 = \theta^6\pi^r$. But this equation has no solutions by lemma 6.5.

The case when $\bar{\theta}$ and π divides B, but θ does not is symmetric to the previous, and there are no solutions here as well.

If θ and $\bar{\theta}$ divide B, but π does not, we have $B = \theta^4\bar{\theta}^4 v = 16v$. The equation becomes $A^2 - 64v = -\pi^{2r}$ which has no solutions by lemma 6.6.

If only θ (resp. $\bar{\theta}$) divides B, then $B = \theta^4 v$ (resp. $B = \bar{\theta}^4 v$). In the case of $B = \theta^4 v$, the equation becomes $A^2 - 4\theta^4 v = -\bar{\theta}^8\pi^{2r}$. But then A must be of the form $A = \bar{\theta}C$. Since $v = \pm 1$, the equation becomes $C^2 \pm \theta^6 = -\bar{\theta}^6\pi^{2r}$. In the proof of lemma 6.7, we showed that

the equation $C^2 \pm \theta^6 = \bar{\theta}^6 \pi^{2r+1}$ has no solutions. Similar arguments show that the equation $C^2 \pm \theta^6 = -\bar{\theta}^6 \pi^{2r}$ has no solutions as well.

If only π divides B, we have $B = \pi^r v$. The equation becomes $A^2 - 4\pi^r v = -2^8$. We can see that A must be of the form $A = 2C$, so that the equation can be rewritten as $C^2 - \pi^r v = -64$. If $r = 2t+1$, then v can be absorbed in π^{2t+1}, so that the equation becomes $C^2 + 64 = \pi^{2t+1}$. The corresponding elliptic curves are $y^2 = x^3 + 2Cx^2 + \pi^{2t+1}x$, which are of the form (6.2). If $r = 2t$ and $v = 1$, then we have $B = \pi^{2t}$ and $C^2 - \pi^{2t} = -64$. This can be rewritten as $(C - \pi^t)(C + \pi^t) = -64$. The valuations of $C - \pi^t$ and $C + \pi^t$ at θ or $\bar{\theta}$ are either 1 or 5. Thus $C - \pi^t = \theta^a \bar{\theta}^b w$ or $C + \pi^t = \theta^a \bar{\theta}^b w$, with $a = 1$ or 5, $b = 1$ or 5 and $w = \pm 1$. If $C - \pi^t = \theta^a \bar{\theta}^b w$, then $(C - \pi^t)(C + \pi^t) = \theta^a \bar{\theta}^b w(\theta^a \bar{\theta}^b w + 2\pi^t) = \theta^{a+1} \bar{\theta}^{b+1} w(\theta^{a-1} \bar{\theta}^{b-1} w + \pi^t) = -64$. This is possible only when $a = b = 5$. In that case, we have $(C - \pi^t)(C + \pi^t) = 64w(16w + \pi^t) = -64$. If $w = 1$, we must have $\pi^t = -15$. However, -15 is not a prime power. If $w = -1$, we must have $\pi^t = 17$, hence $t = 1$. This works since 17 is prime in K. In this case, we get $C = -32 + 17 = -15$, $B = \pi^{2t} = 289$, the corresponding curve is the curve (1.6). When $C + \pi^t = \theta^a \bar{\theta}^b w$, the corresponding curve does not have good reduction at the primes that divide 2. If $r = 2t$ and $v = -1$, the equation is $C^2 + 64 = -\pi^{2t}$, which has no solutions, by lemma 6.6.

If $B = v$, with v a unit, the equation becomes $A^2 - 4v = -2^8 \pi^{2r}$. We can see that A must be of the form $A = 2C$, so that $C^2 - v = -64\pi^{2r}$. If $v = -1$, the equation becomes $C^2 + 1 = -64\pi^{2r}$. By lemma 6.5, there are no solutions.

If $v = 1$, then we have $C^2 - 1 = 64\pi^{2r}$. By lemma 6.6, there are no solutions here as well. □

Lemma 6.10 *The elliptic curves over K of prime conductor with prime conductor (π) not dividing 2 or 3 are the elliptic curves of the form (6.1) and (6.2).*

Proof. Let E/K be an elliptic curve over K with prime conductor (π) not dividing 2 or 3, admitting a K-rational 2-torsion point. Consider a global minimal equation of the form (2.2) for E/K. Then, by lemma 2.5, we must have $\mathrm{ord}_{\pi_2}(a_1) = 0$. In that case, the elliptic curve

E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $(A, B, \pi_2) = 1$, by lemma 2.7. By lemma 6.8, 6.7 and 6.9, the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with $(A, B, \pi_2) = 1$ that have prime conductor (π) not dividing 2, 3 or 17 are the elliptic curves of the form (6.1) and (6.2). □

6.3 The equation $x^2 + 64 = \pi^{2r+1}$.

We are now going to study the equation $x^2 + 64 = \pi^{2r+1}$ over K. We know from the previous section that, for given π, solutions $A \in \mathcal{O}_K$ to this equation give rise to elliptic curves $y^2 = x^3 + Ax^2 - 16x$ and $y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x$ with prime conductor (π).

Lemma 6.11 *Let p be a prime of $\mathbb{Q}$. It splits completely in L if and only if $(\frac{-7}{p}) = 1$ and $(\frac{-1}{p}) = 1$.*

Proof. The field L is a compositum of the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-7})$. Thus a prime p splits completely in L if and only if it splits in both of the above quadratic fields, which is equivalent to say that $(\frac{-1}{p}) = 1$ and $(\frac{-7}{p}) = 1$. □

Lemma 6.12 *Let p be a prime such that $(\frac{-7}{p}) = 1$ and $(\frac{-1}{p}) = -1$. Let π be a prime in K above p. Then the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions.*

Proof. Let $L = K(i)$. We know that a prime q of $\mathbb{Q}$ splits completely in L if and only if $(\frac{-7}{p}) = 1$ and $(\frac{-1}{p}) = 1$. A prime q splits in K if and only if $(\frac{-7}{p}) = 1$. Thus, if $\mathfrak{p} = (\pi)$ is a prime above satisfying the hypotheses of the lemma, it must be inert in L. Then writing the equation in the form $(A - 8i)(A + 8i) = \pi^{2r+1}$, we have that $A \pm 8i = \epsilon\pi^{2r+1}$, and taking norms leads to a contradiction. □

Lemma 6.13 *Let p be a rational prime that remains prime in $\mathbb{Q}(\sqrt{-7})$. Then the equation $A^2 + 64 = up^{2r+1}$ has a solution only when $u = 1$ and $r = 0$. In that case A must be a rational integer.*

Proof. This follows from lemma 2.28. □

6.4 Proof of the Main Theorem

Proof of Theorem 6.1

a) By lemma 6.10, any elliptic curve with prime conductor (π) not dividing 2, 3 and 17 is of the form (6.1) or (6.2), with A such that $A^2 + 64 = \pi^{2r+1}$. Conversely, if A satisfies $A^2 + 64 = \pi^{2r+1}$ and A is a square modulo 4, then the corresponding elliptic curves (6.1) and (6.2) have prime conductor (π).

b) By lemma 6.12, if $(\frac{-7}{p}) = 1$ and $(\frac{-1}{p}) = -1$, the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions. Thus, by part a), any elliptic curve with prime conductor (π) does not have a K-rational 2-torsion point.

By lemma 6.13, if p is prime in K and the equation $x^2 + 64 = up^{2r+1}$, with $u = \pm 1$, has a solution, then $u = 1$ and $r = 0$. Thus, if p is not of the form $p = a^2 + 64$, then by part a), any elliptic curve with conductor (p) has no K-rational 2-torsion point.

c) By remark 2.12, the hypotheses of theorem 2.11 are satisfied here with $K = \mathbb{Q}(\sqrt{-7})$. The result then follows from theorem 2.11

6.5 Tables of values A such that $y^2 = x^3 + Ax^2 - 16x$ is an elliptic curve with prime conductor

We give below some values for A such that $A \equiv \alpha^2 \bmod 4$ and $A^2 + 64$ is a prime π of $\mathbb{Q}(\sqrt{-7})$. For each such value A the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has prime conductor $\mathfrak{f} = (\pi)$.

A	$\pi = A^2 + 64$	p
-3	73	73
5	89	89
17	353	353
-23	593	593
33	1153	1153
37	1433	1433
$-1 + 2\sqrt{-7}$	$37 - 4\sqrt{-7}$	1481
45	2089	2089
-47	2273	2273
$1 + 4\sqrt{-7}$	$-47 + 8\sqrt{-7}$	2657
65	4289	4289
73	5393	5393
-75	5689	5689
$-5 + 2\sqrt{-7}$	$61 - 20\sqrt{-7}$	6521
93	8713	8713
$7 + 2\sqrt{-7}$	$85 + 28\sqrt{-7}$	12713
-123	15193	15193
-135	18289	18289
145	21089	21089
-163	26633	26633
177	31393	31393
$-1 + 6\sqrt{-7}$	$-187 - 12\sqrt{-7}$	35977
193	37313	37313
$11 + 2\sqrt{-7}$	$157 + 44\sqrt{-7}$	38201
$3 + 6\sqrt{-7}$	$-179 + 36\sqrt{-7}$	41113

A	$\pi = A^2 + 64$	p
205	42089	42089
213	45433	45433
-227	51593	51593
$-5 + 6\sqrt{-7}$	$-163 - 60\sqrt{-7}$	51769
-243	59113	59113
$-13 + 2\sqrt{-7}$	$205 - 52\sqrt{-7}$	60953
-255	65089	65089
$7 + 6\sqrt{-7}$	$-139 + 84\sqrt{-7}$	68713
-263	69233	69233
-275	75689	75689
-283	80153	80153
$13 + 4\sqrt{-7}$	$121 + 104\sqrt{-7}$	90353
-303	91873	91873
305	93089	93089
$-9 + 6\sqrt{-7}$	$-107 - 108\sqrt{-7}$	93097
-327	106993	106993
345	119089	119089
-347	120473	120473
353	124673	124673
$11 + 6\sqrt{-7}$	$-67 + 132\sqrt{-7}$	126457
-367	134753	134753
$-17 + 2\sqrt{-7}$	$325 - 68\sqrt{-7}$	137993
-375	140689	140689
-395	156089	156089

A	$\pi = A^2 + 64$	p
-403	162473	162473
437	191033	191033
$-7 + 8\sqrt{-7}$	$-335 - 112\sqrt{-7}$	200033
465	216289	216289
485	235289	235289
-487	237233	237233
$-19 + 4\sqrt{-7}$	$313 - 152\sqrt{-7}$	259697
-527	277793	277793
$-11 + 8\sqrt{-7}$	$-263 - 176\sqrt{-7}$	286001
-535	286289	286289
537	288433	288433
557	310313	310313
565	319289	319289
577	332993	332993
-607	368513	368513
613	375833	375833
633	400753	400753
-635	403289	403289
-667	444953	444953
-683	466553	466553
$-23 + 4\sqrt{-7}$	$481 - 184\sqrt{-7}$	468353
$7 + 10\sqrt{-7}$	$-587 + 140\sqrt{-7}$	481769
$17 + 8\sqrt{-7}$	$-95 + 272\sqrt{-7}$	526913
737	543233	543233
765	585289	585289

A	$\pi = A^2 + 64$	p
773	597593	597593
-775	600689	600689
$25 + 4\sqrt{-7}$	$577 + 200\sqrt{-7}$	612929
793	628913	628913
-795	632089	632089
$-19 + 8\sqrt{-7}$	$-23 - 304\sqrt{-7}$	647441
-815	664289	664289
817	667553	667553
$-13 + 10\sqrt{-7}$	$-467 - 260\sqrt{-7}$	691289
837	700633	700633
-843	710713	710713
-863	744833	744833
-887	786833	786833
$-25 + 6\sqrt{-7}$	$437 - 300\sqrt{-7}$	820969
-907	822713	822713
913	833633	833633
-927	859393	859393
-943	889313	889313
$1 + 12\sqrt{-7}$	$-943 + 24\sqrt{-7}$	893281
-955	912089	912089
$-17 + 10\sqrt{-7}$	$-347 - 340\sqrt{-7}$	929609
-975	950689	950689
-983	966353	966353
997	994073	994073

Chapter 7

Elliptic curves over imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ of class number one, with $d = -11,\ -19,\ -43,\ -67,\ -163$

7.1 Main theorem

Let $K = \mathbb{Q}(\sqrt{d})$, where $d = -11,\ -19,\ -43,\ -67$ or -163. In this case, $d \equiv 1 \bmod 4$ and so the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Let $\theta = (1+\sqrt{d})/2$ and let $\gamma = (1-d)/4$.

The main result of this chapter is the following theorem:

Theorem 7.1 *a) Let p be a prime distinct from 2 and 3,(and 17 in the case $d = -11$ and -163). Let $\mathfrak{p}$ be a prime in K above p. Then, there is an elliptic curve with conductor $\mathfrak{p}$ and a K-rational 2-torsion point if and only if, for some generator π of $\mathfrak{p}$, the equation $x^2 + 64 = \pi^{2r+1}$ has a solution (A, r) with $A \equiv \alpha^2 \bmod 4$ for some algebraic integer α coprime to 2. When the equation has a solution, the corresponding elliptic curves are*

$$y^2 = x^3 + Ax^2 - 16x, \qquad \Delta = 2^{12}\pi^{2r+1}, \tag{7.1}$$

$$y^2 = x^3 - 2Ax^2 + \pi^{2r+1}x, \qquad \Delta = 2^{12}\pi^{4r+2}. \tag{7.2}$$

b) If $(\frac{d}{p}) = 1$ and $p \equiv 3 \bmod 4$, then the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions. Then, any elliptic curve with conductor (π) has no K-rational 2-torsion points.

If p is prime in K, then there are solutions only for $r = 0$. Thus, if p is not of the form $p = x^2 + 64$, any elliptic curve with conductor (p) has no K-rational 2-torsion points.

c) Let π be a prime in $\mathbb{Q}(\sqrt{-11})$ such that $(\pi) \neq (3)$ and (19). If for any extension of the form $N = K(\pi^{\epsilon/3})$, with $\epsilon = 1$ or 2, the ray class number $h_{(3)}(N)$ is not divisible by 4, then, there are no elliptic curves over K with conductor (π).

Corollary 7.2 *Let $K = \mathbb{Q}(\sqrt{-11})$. Then, there are no elliptic over K, with prime conductor dividing $p =$ 5, 7, 13, 23, 29, 31, 37, 53, 67, 71, 103, 113, 137, 163, 167, 173, 179, 181, 191, 193, 199, 227, 229, 239, 251, 257, 263, 269, 283, 311, 317, 353, 367, 389, 419, 433, 443, 461, 463, 487, 499, 509, 521, 569, 577 and 599.*

Proof. All these primes satisfy condition *c*) of the above theorem. □

Theorem 7.3 *The elliptic curves over $K = \mathbb{Q}(\sqrt{-11})$ or $\mathbb{Q}(\sqrt{-163})$ of conductor 17 having a K-rational 2-torsion point are the elliptic curves over $\mathbb{Q}$ given by Setzer's ((1.3), (1.4), (1.5) and (1.6)).*

7.2 Elliptic curves $y^2 = x^3 + Ax^2 + Bx$ with prime conductor

To use lemma 2.8, which gives criterion for an elliptic curve to have good reduction, we will need the following lemma:

Lemma 7.4 *Let $d = -3, -7, -11, -19, -43, -67$ or -163. Let $\theta = (1 + \sqrt{d})/2$ and $\gamma = (d-1)/4$. Let $\alpha = a + b\theta$ be an algebraic integer in $K = \mathbb{Q}(\sqrt{d})$ coprime to the prime in K above 2. Then $\alpha^2 \equiv 1$ or $1 + \gamma + 3\theta$ or $\gamma + \theta \bmod 4$, $-2\alpha^2 \equiv -2$ or $-2(1 + \gamma - \theta)$ or $-2(\gamma + \theta) \bmod 8$, and $\alpha^4 \equiv 1$ or $1 + 3\gamma + \gamma^2 + (7 + 6\gamma)\theta$ or $\gamma + \gamma^2 + (1 + 2\gamma)\theta \bmod 8$.*

Proof. Since α is coprime to the prime in K above 2, a and b cannot both be even. We have that $\alpha^2 = a^2 + \gamma b^2 + (b^2 + 2ab)\theta$ and $\alpha^4 = a^4 + b^4\gamma + 4ab^3\gamma + b^4\gamma^2 + 6a^2b^2\gamma + (4a^3b + 4ab^3\gamma + 2b^4\gamma + 6a^2b^2 + b^4 + 4ab^3)\theta$. If a is odd and b is even, then $\alpha^2 \equiv 1 \bmod 4$, $-2\alpha^2 \equiv -2 \bmod 8$ and $\alpha^4 \equiv 1 \bmod 8$. If a is odd and b is odd, then $\alpha^2 \equiv 1 + \gamma + 3\theta \bmod 4$, $-2\alpha^2 \equiv -2(1 + \gamma - \theta) \bmod 8$ and $\alpha^4 \equiv 1 + 3\gamma + \gamma^2 + (7 + 6\gamma)\theta \bmod 8$. If a is even and b is odd, then $\alpha^2 \equiv \gamma + \theta \bmod 4$, $-2\alpha^2 \equiv -2(\gamma + \theta) \bmod 8$ and $\alpha^4 \equiv \gamma + \gamma^2 + (1 + 2\gamma)\theta \bmod 8$. □

Lemma 7.5 *a) The equation $A^2 - 64 = u\pi^s$, with $u = \pm 1$, π a prime not dividing 2 has a solution $A \in \mathcal{O}_K$ only when $s = 1$ and 17 is prime in K. The solutions are $A = \pm 9$, with $s = 1$, and $u\pi = 17$.*

b) The equation $A^2 - 1 = 64u\pi^s$, with $u = \pm 1$ and π a prime not dividing 2 has a solution only when $s = 1$ and 17 is prime in K. The solutions are $A = \pm 33$.

c) The equation $A^2 + 1 \equiv 0 \bmod 64$ has no solutions $A \in \mathcal{O}_K$.

d) The equation $A^2 + 64v = -\pi^{2r}$, where $v = \pm 1$, has no solutions $A \in \mathcal{O}_K$ when π is a prime not dividing 2.

e) The equation $A^2 - \pi^{2r} = -64$, with π a prime not dividing 2, has a solution only when $r = 1$ and 17 is prime in K. The solutions are $A = \pm 15$, $\pi = \mp 17$.

Proof.

a) The equation can be rewritten as $(A-8)(A+8) = u\pi^s$. Since π cannot divide $A-8$ and $A+8$ simultaneously, we have $A - 8 = w$ or $A + 8 = w$, where $w = \pm 1$. If $A - 8 = w$, we get $(A - 8)(A + 8) = w(16 + w) = u\pi^s$. This has a solution only when $w = 1$ and 17 is prime in K. In that case, we have $A = 9$, $s = 1$ and $u\pi = 17$. If $A + 8 = w$, we get $(A+8)(A-8) = w(w - 16) = u\pi^s$. This has a solution only when $w = -1$ and 17 is prime in K. In that case, we have $A = -9$, $s = 1$ and $u\pi = -17$.

b) The equation can be rewritten as $(A-1)(A+1) = 64u\pi^s$. Since π cannot divide $A-1$ and $A+1$ simultaneously, then $A-1 = 2w$, $A-1 = 32w$, $A+1 = 2w$ or $A+1 = 32w$. If $A - 1 = 2w$, we have $(A - 1)(A + 1) = 2w(2w + 2) = 4w(w + 1)$ which cannot possibly be a multiple of 64. If $A - 1 = 32w$, we get $(A-1)(A+1) = 32w(32w+2) = 64w(16w + 1) = 64u\pi^s$. Hence, there is a solution only when $w = 1$ and $s = 1$. In that case $A = 33$, $s = 1$ and $u\pi = 17$. If $A+1 = 2w$, there are no solutions. If $A+1 = 32w$, the solution is $A = -33$ with $s = 1$, $u\pi = 17$.

c) Let $\theta = \frac{1+\sqrt{d}}{2}$ and $\gamma = \frac{d-1}{4}$. Then $\theta^2 = \theta + \gamma$. Writing $A = x + y\theta$, with $x, y \in \mathbb{Z}$, we have $x^2 + \gamma y^2 + 1 \equiv 0 \bmod 64$ and $2xy + y^2 \equiv 0 \bmod 64$. But this has no solutions.

d) Write $A = x + y\theta$ and $\pi^r = m + n\theta$. We have $\theta^2 = \gamma + \theta$, where $\gamma = (d-1)/4$. Since the norm of π^r is an odd prime power, and the norm is $m^2 + mn + \gamma n^2$, we must have that either m is odd, or m is even and n is odd. The equation $A^2 + 64v = -\pi^{2r}$ implies $x^2 + \gamma y^2 + 64v = -m^2 - \gamma n^2$ and $2xy + y^2 = -2mn - n^2$. The second equation implies that y and n must have same parity, and then the first equation implies that m and x must also have same parity. Suppose first that m is odd. Then x is also odd. Looking at the first equation modulo 4, we see that y and n must then be odd, which is incompatible with the second equation. If m is even and n is odd, then looking at the first equation modulo 4, we deduce that y and n must also be even, a contradiction. Thus the equation $A^2 + 64v = -\pi^{2r}$ has no solutions.

e) The equation can be rewritten in the form $(A - \pi^r)(A + \pi^r) = -64$. Thus $A - \pi^r = 2w$, $A - \pi^r = 32w$, $A + \pi^r = 2w$ or $A + \pi^r = 32w$, where w is a unit. If $A - \pi^r = 2w$, we get $(A - \pi^r)(A + \pi^r) = 2w(2w + 2)$ which cannot possibly be -64. If $A - \pi^r = 32w$, we get $(A - \pi^r)(A + \pi^r) = 32w(32w + 2\pi^r) = 64w(16w + \pi^r) = -64$. If $w = 1$, we must have $\pi^r = -17$. In that case we get $A = 32 - 17 = 15$. If $w = -1$, we must have $\pi^r = 17$. In that case $A = -32 + 17 = -15$. Similarly, there are no solutions if $A + \pi^r = 2w$, and $A = \pm 15$ when $A + \pi^r = 32w$. □

Lemma 7.6 *The elliptic curves over K of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3 and such that $B^2(A^2 - 4B) = 2^8\pi^{2r+1}$ are the curve (1.4), (1.5) and (7.1).*

Proof. We have that π cannot divide B. If 2 divides B, we have $B = 16v$. The equation becomes, after simplification, $A^2 - 64v = \pi^{2r+1}$. If $v = 1$, by lemma 7.5, there are solutions only when 17 is a prime in K, which is the case for $d = -11$ and $d = -163$. In those cases, we have $A = \pm 9$. When $A = 9$, the corresponding curve is the curve (1.5). If $A = -9$,

the corresponding elliptic curve has bad reduction at 2. If $v = -1$, then the equation is $A^2 + 64 = \pi^{2r+1}$, and the corresponding elliptic curves are the curves (7.1).

If 2 does not divide B, then $B = v$, with $v = \pm 1$. The equation becomes $A^2 - 4v = 2^8\pi^{2r+1}$. Then, we must have $A = 2C$, so that $C^2 - v = 64\pi^{2r+1}$. If $v = -1$, there are no solutions, by lemma 7.5. When $v = 1$, we have $B = 1$ and $C^2 - 1 = 64\pi^{2r+1}$. By lemma 7.5, there are solutions only when 17 is prime in K. In that case, the solutions are $C = \pm 33$. When $C = -33$, the corresponding elliptic curve is the curve (1.4). When $C = 33$, the corresponding elliptic curve has bad reduction at 2. □

Lemma 7.7 *The only elliptic curve of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor not dividing 2 or 3, such that $B^2(A^2 - 4B) = 2^8\pi^{2r}$ is the curve (1.3).*

Proof. We have that $A^2 - 4B$ is a square, so that $X^3 + AX^2 + BX = 0$ has its three roots in $\mathcal{O}_K$, say $0, a, b$ with $a, b \not\equiv 0 \bmod \pi$ and $a \equiv b \bmod \pi$. We then have $B = ab$ and $A = -a - b$, and $a^2b^2(a - b)^2 = 2^8\pi^{2r}$. By hypothesis, π does not divide a and b. Furthermore, π_2 divides one and only one of a and b. Let say it divides a. Then $a = 16v$ and $b = w$, where v and w are units. The equation then becomes, after simplification, $(16v - w)^2 = \pi^{2r}$, which admits solutions for $d = -11$ and $d = -163$. The solutions are $(a, b, A, B) = (16, -1, -15, -16)$ and $(a, b, A, B) = (-16, 1, 15, -16)$. The corresponding elliptic curves are $y^2 = x^3 - 15x^2 - 16x$ and $y^2 = x^3 + 15x^2 - 16x$. The first is the curve (1.3), while the other does not have good reduction at 2. □

Lemma 7.8 *The elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with prime conductor (π) not dividing 2 or 3, such that $B^2(A^2 - 4b) = -2^8\pi^{2r}$, are the curves (1.6) and (7.2).*

Proof. There are four cases, depending on whether π and 2 divide B. If 2 and π divide B, then $B = 16v\pi^r$. The equation becomes $A^2 - 64v\pi^r = -1$, after simplification. This can be rewritten as $A^2 + 1 = 64v\pi^r$. By lemma 7.5, this has no solutions.

If only 2 divides B, then $B = 16v$. The equation becomes $A^2 - 64v = -\pi^{2r}$. This has no solutions, by lemma 7.5.

If only π divides B, we have $B = v\pi^r$. The equation becomes $A^2 - 4v\pi^r = -2^8$. We can see that A must then be a multiple of 2. Write $A = 2C$. Then $C^2 - v\pi^r = -64$ i.e. $C^2 + 64 = v\pi^r$. If $r = 2t + 1$ is odd, v can be absorbed in π^{2t+1}, so that the equation is $C^2 + 64 = \pi^{2r+1}$. Whenever there is a solution, the corresponding elliptic curve is of the form (7.2). If $v = -1$ and $r = 2t$, the equation becomes $C^2 + 64 = -\pi^{2t}$, which has no solutions by lemma 7.5. If $v = 1$ and $r = 2t$, the equation becomes $C^2 - \pi^{2t} = -64$. By lemma 7.5, there are solutions only when 17 is prime in K. In that case, the solutions are $C = \pm 15$, $\pi = \mp 17$. When $C = 15$, the corresponding elliptic curve is the curve (1.6). When $C = -15$, the corresponding elliptic curve does not have good reduction at 2.

If $B = v$, with v a unit, then the equation becomes $A^2 - 4v = -2^8\pi^{2r}$. We can see that A must be of the form $A = 2C$ for some C in $\mathcal{O}_K$. The equation becomes $C^2 - v = -64\pi^{2r}$. By lemma 7.5, this equation has no solutions. □

Lemma 7.9 *The elliptic curves over K with prime conductor (π) not dividing 2, 3 (and 17 when 17 is prime in K) and K-rational 2-torsion points, are the elliptic curves of the form (7.1) and (7.2).*

Proof. Let E/K be an elliptic curve over K with prime conductor (π) not dividing 2, 3 (or 17 when 17 is prime in K), admitting a K-rational 2-torsion point. Consider a global minimal equation of the form (2.2) for E/K. Then, by lemma 2.5, we must have $\mathrm{ord}_{\pi_2}(a_1) = 0$. In that case, the elliptic curve E/K has an equation of the form $y^2 = x^3 + Ax^2 + Bx$, with $(A, B, \pi_2) = 1$, by lemma 2.7. By lemma 7.7, 7.6 and 7.8, the elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ with $(A, B, \pi_2) = 1$ that have prime conductor (π) not dividing 2, 3 or 17 are the elliptic curves of the form (7.1) and (7.2). □

7.3 The equation $x^2 + 64 = \pi^{2r+1}$.

We now study the equation $x^2 + 64 = \pi^{2r+1}$ over the fields $K = \mathbb{Q}(\sqrt{d})$ with $d = -11$, -19, -43, -67 and -163.

Lemma 7.10 *Let $L = K(i)$ with K as in the previous lemma. Let p be a prime of $\mathbb{Q}$. It splits completely in L if and only if $(\frac{d}{p}) = 1$ and $(\frac{-1}{p}) = 1$.*

Proof. The field L is a compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{d})$. Thus a prime splits completely in L if and only if it splits each of those two fields, i.e., if and only if $(\frac{-1}{p}) = 1$ and $(\frac{d}{p}) = 1$. □

Lemma 7.11 *Suppose p is a rational prime such that $(\frac{d}{p}) = 1$ but $(\frac{-1}{p}) = -1$, and that $\mathfrak{p} = (\pi)$ is a prime in $\mathcal{O}_K$ above p. Then the equation $A^2 + 64 = \pi^{2r+1}$ has no solutions (A, π, r) with $A \in \mathcal{O}_K$ and $r \in \mathbb{N}$.*

Proof. Indeed, from the previous lemma, we can deduce that the prime $\mathfrak{p}$ is inert in $L = K(i)$. Rewriting the equation $A^2 + 64 = \pi^{2r+1}$ as $(A + 8i)(A - 8i) = \pi^{2r+1}$, we can see that either $A+8i = \epsilon\pi^{2r+1}$ or $A-8i = \epsilon\pi^{2r+1}$, where ϵ is a unit in L. Suppose $A+8i = \epsilon\pi^{2r+1}$, then taking norms, we get $\pi^{2r+1} = N(\epsilon)\pi^{4r+2}$, which is impossible. □

Lemma 7.12 *Let p be an odd rational prime that remains prime in $\mathbb{Q}(\sqrt{d})$, with $d = -11$, -19, -43, -67 or -163. If $d \neq -11$, then the equation $A^2 + 64 = up^{2r+1}$ has a solution only when $u = 1$ and $r = 0$, in which case A must be a rational integer. In $\mathbb{Q}(\sqrt{-11})$, the equation $A^2 + 64 = up^{2r+1}$ has solutions only when $p = 53$, for which the solutions are $A = \pm 2\sqrt{-11}$, $u = 1$, $r = 0$, or when p is of the form $p = a^2 + 64$.*

Proof. This follows from lemma 2.28 □

Remark 7.13 The solution $A = \pm\sqrt{-11}$ obtained in lemma 7.12 does not produce an elliptic curve $y^2 = x^3 + Ax^2 - 16x$ that has prime conductor. Indeed, this curve does not have good reduction at 2. To check this, we use lemma 2.8 and lemma 7.4. Using the notations of lemma 7.4, when $d = -11$, we have $\theta = (1 + \sqrt{-11})/2$, $\gamma = -3$. Thus to check whether the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has good reduction at 2, we must check whether $A \equiv 1, 2 + 3\theta$ or $1 + \theta \bmod 4$. If $A = \pm\sqrt{-11} = \pm(-1 + 2\theta)$, we get $A \equiv 2 \bmod 4$. Hence the elliptic curve $y^2 = x^3 \pm \sqrt{-11}x^2 - 16x$ does not have good reduction at 2.

7.4 Proof of the main theorem

We can now prove theorem 7.1.

Proof of theorem 7.1

a) By lemma 2.6, the elliptic curves with prime conductor not dividing 2 or 3 having a K-rational 2-torsion point are of the form $y^2 = x^3 + Ax^2 + Bx$, with $B^2(A^2 - 4B) = u2^8\pi^s$. By lemma 7.9, all of them are of the form the form (7.1) and (7.2), where A satisfies the equation $A^2 + 64 = \pi^{2r+1}$, except for those that have prime conductor (17). By lemma 2.8, we must necessarily have $A \equiv \pm\alpha^2 \bmod 4$, with α coprime to $\mathfrak{p}_2$. Conversely, if A is such that $A^2 + 64 = \pi^{2r+1}$ and A is a square modulo 4, then by lemma 2.8, the elliptic curves (7.1) and (7.2) have conductor (π).

b) By lemma 7.11, if $(\frac{d}{p}) = 1$ and $(\frac{-1}{p}) = -1$, the equation $x^2 + 64 = \pi^{2r+1}$ has no solutions. Thus, by part *a*), any elliptic curve with prime conductor (π) does not have a K-rational 2-torsion point.

By lemma 7.12, if p is prime in K, if the equation $x^2 + 64 = up^{2r+1}$, with $u = \pm 1$, has a solution, then $u = 1$ and $r = 0$. Thus, if p is not of the form $p = a^2 + 64$, then by part *a*), any elliptic curve with conductor (p) has no K-rational 2-torsion point.

c) By remark 2.25, the hypotheses of theorem 2.23 and corollary 2.24 are satisfied here with $K = \mathbb{Q}(\sqrt{-11})$. The result then follows from corollary 2.24

7.5 Tables of values A such that $y^2 = x^3 + Ax^2 - 16x$ is an elliptic curve with prime conductor

We give below some values for A such that $A \equiv \alpha^2 \bmod 4$ and $A^2 + 64$ is a prime π of $\mathbb{Q}(\sqrt{d})$ with $d = -11$, -19, -43, -67 and -163. For each such value A, the elliptic curve $y^2 = x^3 + Ax^2 - 16x$ has conductor (π).

A	$\pi = A^2 + 64$	p
-3	73	73
$-1/2 + 5/2\sqrt{-11}$	$-9/2 - 5/2\sqrt{-11}$	89
13	233	233
-23	593	593
$-1 + 2\sqrt{-11}$	$21 - 4\sqrt{-11}$	617
-35	1289	1289
-43	1913	1913
45	2089	2089
-47	2273	2273
57	3313	3313
$3/2 + 1/2\sqrt{-11}$	$127/2 + 3/2\sqrt{-11}$	4057
65	4289	4289
-75	5689	5689
$-5/2 + 7/2\sqrt{-11}$	$-129/2 - 35/2\sqrt{-11}$	7529
97	9473	9473
$-13/2 + 1/2\sqrt{-11}$	$207/2 - 13/2\sqrt{-11}$	11177
-123	15193	15193
$15/2 + 5/2\sqrt{-11}$	$103/2 + 75/2\sqrt{-11}$	18121
-135	18289	18289
145	21089	21089
153	23473	23473
$5 + 4\sqrt{-11}$	$-87 + 40\sqrt{-11}$	25169
$3/2 + 9/2\sqrt{-11}$	$-313/2 + 27/2\sqrt{-11}$	26497
-163	26633	26633
-167	27953	27953

A	$\pi = A^2 + 64$	p
-175	30689	30689
177	31393	31393
197	38873	38873
$11 + 2\sqrt{-11}$	$141 + 44\sqrt{-11}$	41177
$-13/2 + 9/2\sqrt{-11}$	$-233/2 - 117/2\sqrt{-11}$	51217
-243	59113	59113
245	60089	60089
$27/2 + 1/2\sqrt{-11}$	$487/2 + 27/2\sqrt{-11}$	61297
-255	65089	65089
$-25/2 + 5/2\sqrt{-11}$	$303/2 - 125/2\sqrt{-11}$	65921
-263	69233	69233
265	70289	70289
-267	71353	71353
-283	80153	80153
305	93089	93089
-327	106993	106993
353	124673	124673
$-17/2 + 11/2\sqrt{-11}$	$-393/2 - 187/2\sqrt{-11}$	134777
-375	140689	140689
377	142193	142193
-395	156089	156089
$27/2 + 9/2\sqrt{-11}$	$47/2 + 243/2\sqrt{-11}$	162937
405	164089	164089
$-15 + 4\sqrt{-11}$	$113 - 120\sqrt{-11}$	171169

A	$\pi = A^2 + 64$	p
437	191033	191033
$19 + 2\sqrt{-11}$	$381 + 76\sqrt{-11}$	208697
-463	214433	214433
465	216289	216289
$35/2 + 7/2\sqrt{-11}$	$471/2 + 245/2\sqrt{-11}$	220529
-475	225689	225689
-483	233353	233353
485	235289	235289
-487	237233	237233
497	247073	247073
-527	277793	277793
$43/2 + 1/2\sqrt{-11}$	$1047/2 + 43/2\sqrt{-11}$	279137
$-41/2 + 5/2\sqrt{-11}$	$831/2 - 205/2\sqrt{-11}$	288209
537	288433	288433
$-21 + 2\sqrt{-11}$	$461 - 84\sqrt{-11}$	290137
553	305873	305873
$-5/2 + 15/2\sqrt{-11}$	$-1097/2 - 75/2\sqrt{-11}$	316321
-575	330689	330689
$-25/2 + 13/2\sqrt{-11}$	$-489/2 - 325/2\sqrt{-11}$	350249
$-33/2 + 11/2\sqrt{-11}$	$7/2 - 363/2\sqrt{-11}$	362377
$15 + 6\sqrt{-11}$	$-107 + 180\sqrt{-11}$	367849
-607	368513	368513
613	375833	375833
-615	378289	378289
617	380753	380753

A	$\pi = A^2 + 64$	p
-635	403289	403289
$-45/2 + 7/2\sqrt{-11}$	$871/2 - 315/2\sqrt{-11}$	462529
-683	466553	466553
713	508433	508433
$9 + 8\sqrt{-11}$	$-559 + 144\sqrt{-11}$	540577
$-53/2 + 1/2\sqrt{-11}$	$1527/2 - 53/2\sqrt{-11}$	590657
773	597593	597593
-783	613153	613153
793	628913	628913
-795	632089	632089
$-29/2 + 15/2\sqrt{-11}$	$-689/2 - 435/2\sqrt{-11}$	639049
-815	664289	664289
817	667553	667553
837	700633	700633
$25 + 4\sqrt{-11}$	$513 + 200\sqrt{-11}$	703169
$55/2 + 3/2\sqrt{-11}$	$1591/2 + 165/2\sqrt{-11}$	707689
-867	751753	751753
$55/2 + 5/2\sqrt{-11}$	$1503/2 + 275/2\sqrt{-11}$	772721
$47/2 + 11/2\sqrt{-11}$	$567/2 + 517/2\sqrt{-11}$	815417
-927	859393	859393
-943	889313	889313
$-29 + 2\sqrt{-11}$	$861 - 116\sqrt{-11}$	889337
-955	912089	912089
965	931289	931289
993	986113	986113

A	$\pi = A^2 + 64$	p
5	89	89
-7	113	113
$3/2 + 3/2\sqrt{-19}$	$47/2 + 9/2\sqrt{-19}$	937
33	1153	1153
37	1433	1433
-43	1913	1913
45	2089	2089
-47	2273	2273
65	4289	4289
-75	5689	5689
$-13/2 + 3/2\sqrt{-19}$	$127/2 - 39/2\sqrt{-19}$	11257
$11/2 + 5/2\sqrt{-19}$	$-49/2 + 55/2\sqrt{-19}$	14969
-123	15193	15193
145	21089	21089
-147	21673	21673
153	23473	23473
-163	26633	26633
$7/2 + 7/2\sqrt{-19}$	$-313/2 + 49/2\sqrt{-19}$	35897
197	38873	38873
$19/2 + 5/2\sqrt{-19}$	$71/2 + 95/2\sqrt{-19}$	44129
$-25/2 + 1/2\sqrt{-19}$	$431/2 - 25/2\sqrt{-19}$	49409
-227	51593	51593
$1 + 4\sqrt{-19}$	$-239 + 8\sqrt{-19}$	58337
-255	65089	65089
265	70289	70289

A	$\pi = A^2 + 64$	p
-267	71353	71353
$27/2 + 3/2\sqrt{-19}$	$407/2 + 81/2\sqrt{-19}$	72577
-275	75689	75689
-303	91873	91873
305	93089	93089
-315	99289	99289
-335	112289	112289
-347	120473	120473
353	124673	124673
-375	140689	140689
-407	165713	165713
413	170633	170633
$-37/2 + 3/2\sqrt{-19}$	$727/2 - 111/2\sqrt{-19}$	190657
-447	199873	199873
$35/2 + 5/2\sqrt{-19}$	$503/2 + 175/2\sqrt{-19}$	208721
-463	214433	214433
465	216289	216289
-483	233353	233353
485	235289	235289
-487	237233	237233
-527	277793	277793
533	284153	284153
537	288433	288433
565	319289	319289
-575	330689	330689

A	$\pi = A^2 + 64$	p
577	332993	332993
-607	368513	368513
613	375833	375833
-615	378289	378289
617	380753	380753
$-1 + 6\sqrt{-19}$	$-619 - 12\sqrt{-19}$	385897
-635	403289	403289
645	416089	416089
$-19 + 4\sqrt{-19}$	$121 - 152\sqrt{-19}$	453617
-683	466553	466553
713	508433	508433
-715	511289	511289
$-9 + 6\sqrt{-19}$	$-539 - 108\sqrt{-19}$	512137
$-25 + 2\sqrt{-19}$	$613 - 100\sqrt{-19}$	565769
765	585289	585289
$-13/2 + 13/2\sqrt{-19}$	$-1393/2 - 169/2\sqrt{-19}$	620777
793	628913	628913
$47/2 + 7/2\sqrt{-19}$	$767/2 + 329/2\sqrt{-19}$	661217
$55/2 + 1/2\sqrt{-19}$	$1631/2 + 55/2\sqrt{-19}$	679409
837	700633	700633
-843	710713	710713
-863	744833	744833
-867	751753	751753
-907	822713	822713
913	833633	833633
-943	889313	889313
-955	912089	912089
-983	966353	966353
993	986113	986113
997	994073	994073

A	$\pi = A^2 + 64$	p
-3	73	73
5	89	89
-7	113	113
13	233	233
-23	593	593
$-1/2 + 3/2\sqrt{-43}$	$-65/2 - 3/2\sqrt{-43}$	1153
-35	1289	1289
-47	2273	2273
57	3313	3313
65	4289	4289
73	5393	5393
$-9/2 + 3/2\sqrt{-43}$	$-25/2 - 27/2\sqrt{-43}$	7993
$11/2 + 1/2\sqrt{-43}$	$167/2 + 11/2\sqrt{-43}$	8273
93	8713	8713
$-13/2 + 1/2\sqrt{-43}$	$191/2 - 13/2\sqrt{-43}$	10937
145	21089	21089
$19/2 + 1/2\sqrt{-43}$	$287/2 + 19/2\sqrt{-43}$	24473
-167	27953	27953
-175	30689	30689
177	31393	31393
193	37313	37313
$-1/2 + 5/2\sqrt{-43}$	$-409/2 - 5/2\sqrt{-43}$	42089
245	60089	60089
-255	65089	65089

A	$\pi = A^2 + 64$	p
-263	69233	69233
265	70289	70289
$-25/2 + 3/2\sqrt{-43}$	$247/2 - 75/2\sqrt{-43}$	75721
$11 + 2\sqrt{-43}$	$13 + 44\sqrt{-43}$	83417
305	93089	93089
-315	99289	99289
-323	104393	104393
345	119089	119089
$-13 + 2\sqrt{-43}$	$61 - 52\sqrt{-43}$	119993
-347	120473	120473
-367	134753	134753
$31/2 + 3/2\sqrt{-43}$	$415/2 + 93/2\sqrt{-43}$	136033
-395	156089	156089
-403	162473	162473
-407	165713	165713
437	191033	191033
465	216289	216289
477	227593	227593
-487	237233	237233
$11/2 + 7/2\sqrt{-43}$	$-865/2 + 77/2\sqrt{-43}$	250793
$-13/2 + 7/2\sqrt{-43}$	$-841/2 - 91/2\sqrt{-43}$	265841
517	267353	267353
$39/2 + 3/2\sqrt{-43}$	$695/2 + 117/2\sqrt{-43}$	267913

A	$\pi = A^2 + 64$	p
537	288433	288433
-567	321553	321553
-575	330689	330689
-607	368513	368513
-615	378289	378289
-667	444953	444953
-683	466553	466553
$-41/2 + 5/2\sqrt{-43}$	$431/2 - 205/2\sqrt{-43}$	498209
-715	511289	511289
$23 + 2\sqrt{-43}$	$421 + 92\sqrt{-43}$	541193
773	597593	597593
-775	600689	600689
777	603793	603793
-795	632089	632089
837	700633	700633
853	727673	727673
-863	744833	744833
-867	751753	751753
-887	786833	786833
$55/2 + 3/2\sqrt{-43}$	$1447/2 + 165/2\sqrt{-43}$	816121
-907	822713	822713
-943	889313	889313
-975	950689	950689
993	986113	986113
997	994073	994073

A	$\pi = A^2 + 64$	p
-7	113	113
13	233	233
17	353	353
-23	593	593
45	2089	2089
$-1/2 + 1/2\sqrt{-67}$	$95/2 - 1/2\sqrt{-67}$	2273
-55	3089	3089
57	3313	3313
-75	5689	5689
93	8713	8713
-123	15193	15193
-127	16193	16193
$-17/2 + 1/2\sqrt{-67}$	$239/2 - 17/2\sqrt{-67}$	19121
145	21089	21089
$11/2 + 3/2\sqrt{-67}$	$-113/2 + 33/2\sqrt{-67}$	21433
-147	21673	21673
-163	26633	26633
$-13/2 + 3/2\sqrt{-67}$	$-89/2 - 39/2\sqrt{-67}$	27457
-175	30689	30689
193	37313	37313
197	38873	38873
$23/2 + 1/2\sqrt{-67}$	$359/2 + 23/2\sqrt{-67}$	41081
205	42089	42089
$-1 + 2\sqrt{-67}$	$-203 - 4\sqrt{-67}$	42281
213	45433	45433
-227	51593	51593
245	60089	60089
-255	65089	65089

A	$\pi = A^2 + 64$	p
$-21/2 + 3/2\sqrt{-67}$	$47/2 - 63/2\sqrt{-67}$	67033
-275	75689	75689
-323	104393	104393
-327	106993	106993
345	119089	119089
-347	120473	120473
353	124673	124673
$11 + 2\sqrt{-67}$	$-83 + 44\sqrt{-67}$	136601
-395	156089	156089
413	170633	170633
-447	199873	199873
465	216289	216289
477	227593	227593
485	235289	235289
-487	237233	237233
$-41/2 + 1/2\sqrt{-67}$	$935/2 - 41/2\sqrt{-67}$	246713
497	247073	247073
$-37/2 + 3/2\sqrt{-67}$	$511/2 - 111/2\sqrt{-67}$	271657
-527	277793	277793
553	305873	305873
565	319289	319289
-567	321553	321553
-575	330689	330689
577	332993	332993
-607	368513	368513
$-29/2 + 5/2\sqrt{-67}$	$-289/2 - 145/2\sqrt{-67}$	373049
613	375833	375833
-615	378289	378289

A	$\pi = A^2 + 64$	p
$19 + 2\sqrt{-67}$	$157 + 76\sqrt{-67}$	411641
-683	466553	466553
$-45/2 + 3/2\sqrt{-67}$	$839/2 - 135/2\sqrt{-67}$	481249
-715	511289	511289
765	585289	585289
773	597593	597593
-775	600689	600689
793	628913	628913
-795	632089	632089
-815	664289	664289
817	667553	667553
$55/2 + 1/2\sqrt{-67}$	$1607/2 + 55/2\sqrt{-67}$	696281
$-17/2 + 7/2\sqrt{-67}$	$-1369/2 - 119/2\sqrt{-67}$	705737
-843	710713	710713
853	727673	727673
-863	744833	744833
-867	751753	751753
-887	786833	786833
$-53/2 + 3/2\sqrt{-67}$	$1231/2 - 159/2\sqrt{-67}$	802297
-907	822713	822713
-927	859393	859393
$-25/2 + 7/2\sqrt{-67}$	$-1201/2 - 175/2\sqrt{-67}$	873569
-955	912089	912089
-983	966353	966353
993	986113	986113
997	994073	994073

A	$\pi = A^2 + 64$	p
-3	73	73
5	89	89
13	233	233
17	353	353
$-1/2 + 1/2\sqrt{-163}$	$47/2 - 1/2\sqrt{-163}$	593
33	1153	1153
-35	1289	1289
37	1433	1433
-43	1913	1913
-47	2273	2273
$7/2 + 1/2\sqrt{-163}$	$71/2 + 7/2\sqrt{-163}$	3257
-75	5689	5689
97	9473	9473
$-17/2 + 1/2\sqrt{-163}$	$191/2 - 17/2\sqrt{-163}$	20897
-147	21673	21673
-167	27953	27953
-175	30689	30689
193	37313	37313
197	38873	38873
$23/2 + 1/2\sqrt{-163}$	$311/2 + 23/2\sqrt{-163}$	45737
$-25/2 + 1/2\sqrt{-163}$	$359/2 - 25/2\sqrt{-163}$	57689
-243	59113	59113
245	60089	60089
-255	65089	65089
-267	71353	71353
-283	80153	80153

A	$\pi = A^2 + 64$	p
$3/2 + 3/2\sqrt{-163}$	$-601/2 + 9/2\sqrt{-163}$	93601
$-5/2 + 3/2\sqrt{-163}$	$-593/2 - 15/2\sqrt{-163}$	97081
-323	104393	104393
$11/2 + 3/2\sqrt{-163}$	$-545/2 + 33/2\sqrt{-163}$	118633
345	119089	119089
353	124673	124673
$-13/2 + 3/2\sqrt{-163}$	$-521/2 - 39/2\sqrt{-163}$	129841
-375	140689	140689
-395	156089	156089
-403	162473	162473
-407	165713	165713
$19/2 + 3/2\sqrt{-163}$	$-425/2 + 57/2\sqrt{-163}$	177553
477	227593	227593
485	235289	235289
-487	237233	237233
497	247073	247073
$-41/2 + 1/2\sqrt{-163}$	$887/2 - 41/2\sqrt{-163}$	265193
533	284153	284153
537	288433	288433
557	310313	310313
-567	321553	321553
-575	330689	330689
577	332993	332993
$-1 + 2\sqrt{-163}$	$-587 - 4\sqrt{-163}$	347177
-615	378289	378289
617	380753	380753

A	$\pi = A^2 + 64$	p
633	400753	400753
-635	403289	403289
737	543233	543233
-743	552113	552113
-783	613153	613153
785	616289	616289
$-13 + 2\sqrt{-163}$	$-419 - 52\sqrt{-163}$	616313
793	628913	628913
-795	632089	632089
817	667553	667553
837	700633	700633
$43/2 + 3/2\sqrt{-163}$	$319/2 + 129/2\sqrt{-163}$	703561
$55/2 + 1/2\sqrt{-163}$	$1559/2 + 55/2\sqrt{-163}$	730889
-863	744833	744833
$-45/2 + 3/2\sqrt{-163}$	$407/2 - 135/2\sqrt{-163}$	784081
-887	786833	786833
-907	822713	822713
$-17 + 2\sqrt{-163}$	$-299 - 68\sqrt{-163}$	843113
-943	889313	889313
$-5/2 + 5/2\sqrt{-163}$	$-1897/2 - 25/2\sqrt{-163}$	925121
965	931289	931289
-975	950689	950689
-983	966353	966353
997	994073	994073

Appendix A

Programs

A.1 Programs finding primes satisfying conditions of Theorem 2.11 and Theorem 2.23 in the case of $K = \mathbb{Q}(i)$

This program finds the primes π in $K = \mathbb{Q}(i)$ such that if $N = K(\sqrt{\epsilon\pi})$, with $\epsilon = 1$ or i, then the ray class number $h_{(2)}(N)$ is coprime to 3.

```
\p 200;
T(x)=x^2+1;
nff=bnfinit(T(x));
{ forprime(p=3,1000,
     if(kronecker(-1,p)==1,
 P=idealprimedec(nff,p);
 q=P[1];
       r=bnfisprincipal(nff,q);
       u=r[2][1];
       v=r[2][2];
       bnf1=bnfinit(x^4-2*u*x^2+p);
       bnf2=bnfinit(x^4+2*v*x^2+p);
       G=bnrclassno(bnf1,2);
       H=bnrclassno(bnf2,2);
         if(G-floor(G/3)*3<>0,
           if(H-floor(H/3)*3<>0,
 print(p);
 write(clouti2,p)
               )
             )
         );
if(kronecker(-1,p)==-1,
        bng1=bnfinit(x^4-2*(p-1)*x^2+(p+1)^2);
        bng2=bnfinit(x^4+2*(p+1)*x^2+(p-1)^2);
```

```
        M=bnrclassno(bng1,2);
        N=bnrclassno(bng2,2);
          if(M-floor(M/3)*3<>0,
           if(N-floor(N/3)*3<>0,
              print(p);
              write(clouti2,p)
               )
             )
         )
) }
```

This program finds the primes π in $K = \mathbb{Q}(i)$, such that if $N = K(\pi^{\frac{\epsilon}{3}})$, with $\epsilon = 1$ or 2, then the ray class number $h_{(3)}(N)$ is not divisible by 4.

```
\p 400;
T(x)=x^2+1;
nff=bnfinit(T(x));
{ forprime(p=3,1000,
     if(kronecker(-1,p)==1,
 P=idealprimedec(nff,p);
       q=P[1];
       r=bnfisprincipal(nff,q);
       u=r[2][1];
       v=r[2][2];
       bnf1=bnfinit(x^6-2*u*x^3+p);
       bnf2=bnfinit(x^6-2*(u^2-v^2)*x^3+p^2);
       G=bnrclassno(bnf1,3);
       H=bnrclassno(bnf2,3);
         if(G-floor(G/4)*4<>0,
          if(H-floor(H/4)*4<>0,
print(p);
write(clouti3,p)
              )
             )
          );
if(kronecker(-1,p)==-1,
        bng1=bnfinit(x^6+3*x^4-2*p*x^3+3*x^2+6*p*x+p^2+1);
        bng2=bnfinit(x^6+3*x^4-2*p^2*x^3+3*x^2+6*p^2*x+p^4+1);
        M=bnrclassno(bng1,3);
        N=bnrclassno(bng2,3);
          if(M-floor(M/4)*4<>0,
```

```
           if(N-floor(N/4)*4<>0,
              print(p);
              write(clouti3,p)
              )
             )
           )
) }
```

A.2 Programs finding primes satisfying conditions of Theorem 2.11 and Theorem 2.23 in the case of $K = \mathbb{Q}(\sqrt{-2})$.

This program finds the primes π in $K = \mathbb{Q}(\sqrt{-2})$ such that if $N = K(\sqrt{\pm\pi})$, then $h_{(2)}(N)$ is coprime to 3.

```
\p 200;
allocatemem();
T(x)=x^2+2;
nff=bnfinit(T(x));
{ forprime(p=2,1000,
     if(kronecker(-2,p)==1,
 P=idealprimedec(nff,p);
       q=P[1];
 r=bnfisprincipal(nff,q);
       u=r[2][1];
 v=r[2][2];
       bnf1=bnfinit(x^4+(4-2*u)*x^2+8*v*x+p+4+4*u);
       bnf2=bnfinit(x^4+(4+2*u)*x^2+8*v*x+p+4-4*u);
       G=bnrclassno(bnf1,2);
       H=bnrclassno(bnf2,2);
        if(G-floor(G/3)*3<>0,
          if(H-floor(H/3)*3<>0,
print(p);
            write(cloutno22,p)
             )
           )
          );
     if(kronecker(-2,p)==-1,
        bng1=bnfinit(x^4+(4-2*p)*x^2+4+p^2+4*p);
  bng2=bnfinit(x^4+(4+2*p)*x^2+4+p^2-4*p);
       M=bnrclassno(bng1,2);
```

```
        N=bnrclassno(bng2,2);
         if(M-floor(M/3)*3<>0,
           if(N-floor(N/3)*3<>0,
 print(p);
             write(cloutno22,p)
              )
            )
       )
   )  }
```

This program finds the primes in $K = \mathbb{Q}(\sqrt{-2})$, such that if $N = K(\pi^{\frac{\epsilon}{3}})$,with $\epsilon = 1$ or 2, then the ray class number $h_{(3)}(N)$ is not divisible by 4.

```
\p 400;
allocatemem();
T(x)=x^2+2;
nff=bnfinit(T(x));
{ forprime(p=3,1000,
     if(kronecker(-2,p)==1,
        P=idealprimedec(nff,p);
        q=P[1];
  r=bnfisprincipal(nff,q);
        u=r[2][1];
  v=r[2][2];
        bnf1=bnfinit(x^6-2*u*x^3+p);
        bnf2=bnfinit(x^6-2*(u^2-2*v^2)*x^3+p^2);
        G=bnrclassno(bnf1,3);
        H=bnrclassno(bnf2,3);
          if(G-floor(G/4)*4<>0,
            if(H-floor(H/4)*4<>0,
 print(p);
 write(clout23,p)
               )
              )
          );
if(kronecker(-2,p)==-1,
         bng1=bnfinit(x^6+6*x^4-2*p*x^3+12*x^2+12*p*x+p^2+8);
         bng2=bnfinit(x^6+6*x^4-2*p^2*x^3+12*x^2+12*p^2*x+p^4+8);
         M=bnrclassno(bng1,3);
         N=bnrclassno(bng2,3);
           if(M-floor(M/4)*4<>0,
```

```
            if(N-floor(N/4)*4<>0,
   print(p);
              write(clout23,p)
               )
             )
          )
) }
```

A.3 Programs finding primes satisfying conditions of Theorem 2.11 in the case of $K = \mathbb{Q}(\sqrt{d})$ with $d = -3$ or -7.

This program finds the primes π in $K = \mathbb{Q}(\sqrt{d})$, $d = -3$ or -7, such that for the extensions $N = K(\sqrt{\pm\pi})$, the ray class number $h_{(2)}(N)$ is coprime to 3.

```
\p 400;
allocatemem();
d=-3;
T(x)=x^2-x+(1-d)/4;
nff=bnfinit(T(x));
{ forprime(p=3,1000,
     if(kronecker(d,p)==1,
  P=idealprimedec(nff,p);
        q=P[1];
        r=bnfisprincipal(nff,q);
        u=r[2][1];
        v=r[2][2];
        NG=bnfinit(x^4-(2*u+v)*x^2+p);
        G=bnrclassno(NG,2);
        NH=bnfinit(x^4+(2*u+v)*x^2+p);
        H=bnrclassno(NH,2);
    if(G-floor(G/3)*3<>0,
            if(H-floor(H/3)*3<>0,
              print(p);
              write(classoutputneg32,p)
              )
             )
         );
      if(kronecker(d,p)==-1,
   NM=bnfinit(x^4-(2*d+2*p)*x^2+d^2+p^2-2*d*p);
   M=bnrclassno(NM,2);
         NN=bnfinit(x^4+(-2*d+2*p)*x^2+d^2+p^2+2*d*p);
```

```
          N=bnrclassno(NN,2);
           if(M-floor(M/3)*3<>0,
             if(N-floor(N/3)*3<>0,
          print(p);
                write(classoutputneg32,p)
                 )
               )
          )
)
}
```

A.4 Program finding primes satisfying conditions of Theorem 2.23 in the case of $K = \mathbb{Q}(\sqrt{-11})$.

This program finds the primes in $K = \mathbb{Q}(\sqrt{-11})$ such that for $N = K(\pi^{\frac{\epsilon}{3}})$, with $\epsilon = 1$ or 2, the ray class number $h_{(3)}(N)$ is not divisible by 4.

```
\p 400;
allocatemem();d=-11;
T(x)=x^2-x+(1-d)/4;
nff=bnfinit(T(x));
{ forprime(p=3,1000,
     if(kronecker(d,p)==1,
       P=idealprimedec(nff,p);
       q=P[1];
       r=bnfisprincipal(nff,q);
 u=r[2][1];
       v=r[2][2];
       U=u^2+(-1+d)/4*v^2;
       V=2*u*v+v^2;
       NG=bnfinit(x^6-(2*u+v)*x^3+p);
       G=bnrclassno(NG,3);
       NH=bnfinit(x^6-(2*U+V)*x^3+p^2);
       H=bnrclassno(NH,3);
   if(G-floor(G/4)*4<>0,
           if(H-floor(H/4)*4<>0,
             print(p);
             write(classoutputneg11,p)
             )
           )
         );
```

```
    if(kronecker(d,p)==-1,
NM=bnfinit(x^6-3*d*x^4-2*p*x^3+3*d^2*x^2-6*d*p*x+p^2-d^3);
M=bnrclassno(NM,3);
      NN=bnfinit(x^6-3*d*x^4-2*p^2*x^3+3*d^2*x^2-6*d*p^2*x+p^4-d^3);
      N=bnrclassno(NN,3);
        if(M-floor(M/4)*4<>0,
          if(N-floor(N/4)*4<>0,
            print(p);
            write(classoutputneg11,p)
             )
           )
       )
  )
}
```

A.5 Program computing $A^2 + 64i = \pi^{2r+1}$ in $\mathbb{Q}(i)$.

Let $K = \mathbb{Q}(i)$. By Theorem 3.1, to find the elliptic curves with prime conductor not dividing $2, 3$ or 257, and having a K-rational 2-torsion point, it suffices to find the values A such that $A^2 + 64i$ is a prime power π^{2r+1}. When π divides a prime $p \equiv 1 \bmod 16$ and $A \equiv \pm 1 \bmod 4$ (resp. $Ai \equiv \pm 1 \bmod 4$), then the elliptic curve

$$y^2 = x^3 + Ax^2 - 16ix \tag{A.1}$$

resp.

$$y^2 = x^3 + Aix^2 + 16ix \tag{A.2}$$

has conductor (π).

Given a number N, we would like to determine n and m such that all the prime powers of the form $A^2 + 64i = \pi^{2r+1}$, where $A = (a + bi)$ and π is a prime such that $p^{2r+1} \leq N$, are attained if $|a| \leq n, |b| \leq m$. We have

$$N_{K/\mathbb{Q}}(A^2 + 64i) \leq N \Leftrightarrow a^4 + 2b^2a^2 + 2^8ba + b^4 + 2^{12} \leq N. \tag{A.3}$$

Let $\beta(x) = x^4 + 2^{12}$, $f_b(x) = x^4 + 2b^2x^2 + 2^8bx + b^4 + 2^{12}$ and $g_b(x) = x^4 + \alpha(b)x^2 + \beta(b)$ with

$$\alpha(b) = \begin{cases} 2b^2 & \text{if} \quad xb > 0 \\ 2b^2 + 2^8b & \text{if} \quad x > 0, b < 0 \\ 2b^2 - 2^8b & \text{if} \quad x < 0, b > 0. \end{cases}$$

Then $g_b(x) \leq f_b(x)$ and equation A.3 is equivalent to $f_b(a) \leq N$. Hence, if $f_b(x) \leq N$, then $g_b(x) \leq N$. This means that the set $\{(a,b)/f_b(a) \leq N\}$ is included in the set $\{(a,b)/g_b(a) \leq N\}$. Studying the function $g_b(x)$, we get the following:

a) If $N < \beta(b)$, then for all a, we have $g_b(a) > N$.

b) If $N < 2^{12}$, then $N < \beta(b)$ for all b. If $N \geq 2^{12}$, then $\beta(b) \leq N \Leftrightarrow |b| \leq (N - 2^{12})^{\frac{1}{4}}$.

c) If $\beta(b) \leq N$, then $g_b(a) \leq N \Leftrightarrow |a| \leq \sqrt{-\frac{\alpha(b)}{2} + \sqrt{\frac{\alpha(b)^2}{4} + N - \beta(b)}}$.

For given N, the program below finds all values $A \in \mathcal{O}_K$ with the following propreties:

a) $A^2 + 64i$ is a prime power π^{2r+1}.

b) If p is the prime below π, then $p^{2r+1} \leq N$.

c) $A \equiv \pm 1 \bmod 4$.

For each such value, we know that the elliptic curve A.1 has conductor (π).

If A is such that $A^2 + 64i = \pi^{2r+1}$ and $Ai \equiv \pm 1 \bmod 4$, then the elliptic curve A.2 is the one that has prime conductor (π). Its conjugate is $y^2 = x^3 - \bar{A}ix^2 - 16ix$. Put $a = -\bar{A}i$. We have $a \equiv \pm 1 \bmod 4$ and $a^2 + 64i = \pi^{2r+1}$. Thus, the elliptic curve A.2 is the conjugate of an elliptic curve of the form A.1. Therefore, to find the elliptic curves with prime conductor not dividing $2, 3$ or 257 and having K-rational 2-torsion points, it suffices to find the elliptic curves of the form A.1.

```
> restart:

> k:=0;
```

```
> N:=10^6;bf:=x->(x-2^(12))^(1/4);b:=floor(evalf(bf(N)));
> alpha:=(x,y)->piecewise(x*y>0,2*y^2,x<0 and y>0,2*y^2-2^8*y,x>0 and
> y<0,2*y^2-2^8*y);
> s:=alpha(-8,1);evalf(sqrt(-s/2+sqrt(s^2/4+N-2^(12))));
> beta:=x->x^4+2^(12);
> af:=(x,y)->sqrt(-alpha(x,y)/2+sqrt(alpha(x,y)^2/4+N-beta(x)));
> ai:=floor(evalf((N-2^(12))^(1/4)));
> with(numtheory):
> for j from -b to b do
> if j<>0 then
> if modp(j,4)=0 then
> a:=evalf(af(j,1)):
> for i from 1 by 2 to a do
> F:=(i+j*I)^2+64*I:
> Q:=i+j*I:
> M:=ifactors(F*conjugate(F)):
> m:=nops(M[2]):
> if m=1 and M[2]<>[ ] and M[2,1,2]>0 and modp(M[2,1,2],2)=1 and
> M[2,1,1]^M[2,1,2]<=N then
> k:=k+1:
> A[k]:=Q:B[k]:=simplify(F):P[k]:=M[2,1,1]:
> e[k]:=M[2,1,2]:
> end if:end do:end if:end if:end do:
> for i from 1 by 2 to ai do
> K:=(i)^2+64*I:M:=ifactors(K*conjugate(K)):m:=nops(M[2]):
> if m=1 and M[2]<>[ ] and M[2,1,2]>0 and modp(M[2,1,2],2)=1 then
> k:=k+1:
> A[k]:=i:B[k]:=K:P[k]:=M[2,1,1]:e[k]:=M[2,1,2]:
> end if:end do:
```

```
> for i from k-1 to 1 by -1 do
> for j from 1 to i do
> if P[j]>P[j+1] then
> x:=A[j]:y:=B[j]:z:=P[j]:t:=e[j]:A[j]:=A[j+1]:B[j]:=B[j+1]:P[j]:=P[j+1]
> :
> e[j]:=e[j+1]:A[j+1]:=x:B[j+1]:=y:P[j+1]:=z:
> e[j+1]:=t:
> end if:end do:end do:
> for l from 1 to k do
> print(A[l],B[l],P[l]);
> end do;
```

A.6 Program computing $A^2 + 64 = u\pi^{2r+1}$ in $\mathbb{Q}(\sqrt{d})$, with $d = -2, -3, -7, -11, -19, -43, -67, -163$.

A.6.1 Case of $d \neq -2$.

Let $K = \mathbb{Q}(\sqrt{d})$ be one of the quadratic imaginary fields with class number one and $d \neq -1, -2$. Given a number N, we would like to determine n and m such that all the prime powers of the form $A^2 + 64 = \pi^{2r+1}$, where $A = \frac{1}{2}(a + b\sqrt{d})$ and π is a prime such that $p^{2r+1} < N$, are attained if $|a| < n, |b| < m$. We have

$$N_{K/\mathbb{Q}}(A^2 + 64) \leq N \Leftrightarrow a^4 + (2^9 - 2b^2d)a^2 + d^2b^4 + 2^9db^2 + 2^{16} \leq 16N. \tag{A.4}$$

Let $\alpha(x) = 2^9 - 2dx^2$, $\beta(x) = d^2x^4 + 2^9dx^2 + 2^{16}$, and $f_b(x) = x^4 + \alpha(b)x^2 + \beta(b)$. Then equation A.4 is equivalent to $f_b(a) \leq 16N$. Studying the function $f_b(x)$, we get the following:

a) If $16N < \beta(b)$, then for all a, we have $f_b(a) > 16N$.

b) If $N < 2^{12}$, then $\beta(b) \leq 16N \Leftrightarrow \sqrt{\frac{-2^8+4\sqrt{N}}{d}} \leq |b| \leq \sqrt{\frac{-2^8-4\sqrt{N}}{d}}$. If $N \geq 2^{12}$, then $\beta(b) \leq 16N \Leftrightarrow |b| \leq \sqrt{\frac{-2^8-4\sqrt{N}}{d}}$.

c) If $\beta(b) \leq 16N$, then $f_b(a) \leq 16N \Leftrightarrow |a| \leq \sqrt{-\frac{\alpha(b)}{2} + \sqrt{\frac{\alpha(b)^2}{4} + 16N - \beta(b)}}$.

For rational primes p that remain prime in K, we want $a^2 + 64 = p^{2r+1} \leq N$. Hence $|a| \leq \sqrt{N - 64}$.

```
> restart:

> k:=0;d:=-163;th:=(1+sqrt(d))/2;g:=(d-1)/4;
> N:=10^6;bf:=x->sqrt((-2^8-4*sqrt(x))/d);b:=floor(evalf(bf(N)));alpha:
> =x->2^9-2*x^2*d;beta:=x->d^2*x^4+2^9*d*x^2+2^(16);

> af:=x->sqrt(-alpha(x)/2+sqrt(alpha(x)^2/4+16*N-beta(x)));

> ai:=floor(evalf(sqrt(N-64)));

> with(numtheory):
```

```
> for j from 1 to b do
> a:=evalf(af(j));
> for i from 1 to a do
> if modp(j-i,2)=0 then
> for s from 0 to 1 do
> F:=(1/2*(i*(-1)^s+j*sqrt(d)))^2+64:
> Q:=simplify(1/2*(i*(-1)^s+j*sqrt(d))):
> x:=2*Re(Q):y:=2*Im(Q)/sqrt(-d): M:=ifactors(expand(F*conjugate(F))):
> m:=nops(M[2]):
> if m=1 and M[2]<>[ ] then
> if modp(M[2,1,2],2)=1 and ((modp((x-y)/2,4)=modp(1+g,4) and
> modp(y,4)=3) or (modp((x-y)/2,4)=1 and modp(y,4)=0) or
> (modp((x-y)/2,4)=modp(g,4) and modp(y,4)=1)) then
> k:=k+1:
> A[k]:=Q:B[k]:=simplify(F):P[k]:=M[2,1,1]:
> e[k]:=M[2,1,2]:
> end if:end if:end do:end if:end do:end do:
> for i from -ai to ai do
> if modp(i,4)=1 then
> K:=i^2+64:
> M:=ifactors(K):
> m:=nops(M[2]):
> if m=1 and M[2]<>[ ] then
> if legendre(d,M[2,1,1])=-1 then
> if modp(M[2,1,2],2)=1 then
> k:=k+1:
> A[k]:=i:B[k]:=K:P[k]:=M[2,1,1]:e[k]:=M[2,1,2]:
> end if:end if:end if:end if:end do:
```

```
> for i from k-1 to 1 by -1 do
> for j from 1 to i do
> if P[j]>P[j+1] then
> x:=A[j]:y:=B[j]:z:=P[j]:t:=e[j]:A[j]:=A[j+1]:B[j]:=B[j+1]:P[j]:=P[j+1]
> :
> e[j]:=e[j+1]:A[j+1]:=x:B[j+1]:=y:P[j+1]:=z:e[j+1]:=t:
> end if:end do:end do:
> for l from 1 to k do
> print(A[l],B[l],P[l],e[l]);
> od;
```

A.6.2 Case of $d = -2$.

The case of $d = -2$ differs only by the fact that $(1, \sqrt{-2})$ is a basis of $\mathcal{O}_K$. In that case, if $A \in \mathcal{O}_K$, then we can write $A = a + b\sqrt{d}$. Then $A^2 + 64 = a^2 + db^2 + 64 + 2ab\sqrt{d}$ and

$$N_{K/\mathbb{Q}}(A^2 + 64) \leq N \Leftrightarrow a^4 + (2^7 - 2db^2)a^2 + d^2b^4 + 2^7db^2 + 2^{12} \leq N. \tag{A.5}$$

Let $\alpha(x) = 2^7 - 2dx^2$, $\beta(x) = d^2x^4 + 2^7dx^2 + 2^{12}$, and $f_b(x) = x^4 + \alpha(b)x^2 + \beta(b)$. Then equation A.5 is equivalent to $f_b(a) \leq N$. Studying the function $f_b(x)$, we get the following:

a) If $N < \beta(b)$, then for all a, we have $f_b(a) > 16N$.

b) If $N < 2^{12}$, then $\beta(b) \leq N \Leftrightarrow \sqrt{\frac{-2^6+\sqrt{N}}{d}} \leq |b| \leq \sqrt{\frac{-2^6-\sqrt{N}}{d}}$. If $N \geq 2^{12}$, then $\beta(b) \leq N \Leftrightarrow |b| \leq \sqrt{\frac{-2^6-4\sqrt{N}}{d}}$.

c) If $\beta(b) \leq N$, then $f_b(a) \leq N \Leftrightarrow |a| \leq \sqrt{-\frac{\alpha(b)}{2} + \sqrt{\frac{\alpha(b)^2}{4} + N - \beta(b)}}$.

```
> restart:
> k:=0;d:=-2;
> N:=10^6;bf:=x->sqrt((-64-sqrt(N))/(d));b:=floor(evalf(bf(N)));alpha:=
> x->2^7-2*d*x^2;beta:=x->d^2*x^4+2^7*d*x^2+2^(12);
> af:=x->sqrt(-alpha(x)/2+sqrt(alpha(x)^2/4+N-beta(x)));
> with(numtheory):
```

```
> for j from 1 to b do
> a:=evalf(af(j));
> for i from 0 to a do
> if modp(i,2)=1 then
> for s from 0 to 1 do
> F:=(i*(-1)^s+j*sqrt(-2))^2+64: Q:=simplify(i*(-1)^s+j*sqrt(-2)):
> x:=Re(Q):y:=Im(Q)/sqrt(2):
> M:=ifactors(expand(F*conjugate(F))):
> m:=nops(M[2]):
> if m=1 and M[2]<>[ ] then  if modp(M[2,1,2],2)=1 and ((modp(x,4)=3 and
> modp(y,4)=2) or (modp(x,4)=1 and modp(y,4)=0)) then
> k:=k+1:
> A[k]:=Q:
> B[k]:=simplify(F):
> P[k]:=M[2,1,1]:
> e[k]:=M[2,1,2]:
> end if:end if:end do:end if:end do:end do:
> for i from k-1 to 1 by -1 do
> for j from 1 to i do
> if P[j]>P[j+1] then
> x:=A[j]:y:=B[j]:z:=P[j]:t:=e[j]:A[j]:=A[j+1]:B[j]:=B[j+1]:P[j]:=P[j+1]
> :
> e[j]:=e[j+1]:A[j+1]:=x:B[j+1]:=y:P[j+1]:=z:
> e[j+1]:=t:
> end if:end do:end do:
> for l from 1 to k do
> print(A[l],B[l],P[l]);
> od;
```

Bibliography

[1] M. K. Agrawal, J. H. Coates, D.C.Hunt and A. J. van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. **39** (1980), **no. 35**, 991–1002.

[2] A. Beauville, *Le nombre minimum de fibres singulières d'une courbe stable sur* $\mathbb{P}^1$, Astérisque **86** (1981), 97–108.

[3] R. Bölling, *Elliptische Kurven mit Primzahlführer*, Math. Nachr. **80** (1977), 253–278.

[4] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001) **no. 4**, 843–939.

[5] A. Brumer and K. Kramer, *The rank of elliptic curves,* Duke Math. J. **44** (1977), 715–743.

[6] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag New York, Berlin, Heidelberg, 2000.

[7] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), **no. 2**, 237–258

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

[9] J. E. Cremona, *Hyperbolic tesselations, modular symbols and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), 275–323.

[10] J. E. Cremona, *Hyperbolic tesselations, modular symbols and elliptic curves over complex quadratic fields (Addendum and Errata)*, Compositio Math. **63** (1987), 271–272.

[11] J. E. Cremona and E.Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62**, (1994) **no. 205**, 407–429.

[12] B. Edixhoven, A. D. Groot and J. Top, *Elliptic curves over the rationals with bad reduction at only one prime*, Math. Comp. **54**, Issue 189 (Jan., 1990), 413–419.

[13] J. M. Fontaine, *Il n'y pas de variété abeliénne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), **no.3**, 515–538.

[14] E. Herrmann, *Bestimmung aller S-ganzen Lösungen auf elliptischen Kurven*, Dissertation, Universitäte des Saarlandes, 2002.

[15] J. F. Humphreys, *A course in group theory*, Oxford University Press Inc., New York, 1997.

[16] G. J. Janusz, *Algebraic number fields*, Academic Press, New York and London, 1973.

[17] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields*, Arch. Math. **73** (1999), 25–32.

[18] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **83**, (1998), 253–269.

[19] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta Arith. (2001),231–245.

[20] T. Kagawa and M. Kida, *Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields*, J. Number Theory **66** (1997), 201–210.

[21] M. Kida, *Nonexistence of elliptic curves having good reduction everywhere over certain quadratic fields*, Arch. Math. **76** (2001) 436–440.

[22] M. Kida, *Reduction of elliptic curves over certain real quadratic fields*, Math. Comp. **68** (1999), **no. 228**, 1679–1685.

[23] A. Kraus, *Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique*, Acta Arith. **54** (1989) 75–80.

[24] S. Lang, *Algebraic Number Theory*, (2nd ed.). Grad. Texts in Math. 110 (1994)

[25] M. Laska, *Elliptic curves over number fields with prescribed reduction type*, Aspects of Mathematics, vol.4.

[26] J. F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986) **no. 2**, 209–232.

[27] J. F. Mestre and J. Oesterlé, *Courbe de Weil semi-stables de discriminant une puissance m-iéme,* J. Reine Angew. Math. **400** (1989),173–184.

[28] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972) 177–190.

[29] I. Miyawaki, *Elliptic curves of prime power conductor with $\mathbb{Q}$-rational points of finite order*, Osaka J. Math. **10** (1973), 309–323.

[30] P. Morandi, *Field and galois theory*, Springer-Verlag New York, Berlin, Heidelberg (1991).

[31] L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969.

[32] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reductionsverhalten. II*, Math. Nachr. **56** (1973) 269–280.

[33] K. V. Nguyen, *A remark on semi-stable fibrations over $\mathbf{P}^1$ in positive characteristic.* Compositio Math. **112** (1998), **no. 1**, 41–44.

[34] A. P. Ogg, *Abelian curves of 2-power conductor*, Proc. Cambr. Phil. Soc. **62** (1966), 143–148.

[35] A. P. Ogg, *Abelian curves of small conductor*, J. Reine Angew. **226** (1967), 204–215.

[36] I. Papadopoulos, *Sur la classification de Neron des courbes elliptiques en caracteristiques residuelle 2 et 3*, Journal of Number Theory **44**, (1993), 119–152.

[37] R. G. Pinch, *Elliptic curves with good reduction away from* 2, Math. Proc. Camb. Phil. Soc. **96** (1984), 25–36.

[38] R. G. Pinch, *Elliptic curves with good reduction away from* 2*:II*, Math. Proc. Camb. Phil. Soc. **100** (1986), 435–457.

[39] R. G. Pinch, *Elliptic curves with good reduction away from* 3, Math. Proc. Camb. Phil. Soc. **101** (1987) 451–459.

[40] R. Schoof, *Abelian varieties over cyclotomic fields and good reduction everywhere*, Math. Ann. **325** (2003), 413–448.

[41] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent.Math. **15**, (1972) 259–331.

[42] B. Setzer, *Elliptic curves with prime conductor*, J. London Math. Soc. **10** (1975), 367–378.

[43] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math **74** (1978), 235–250.

[44] I. R. Shafarevich, *Algebraic number fields*, Proc. Int. Cong. Stockholm (1962), A. M. S. Translations **31**, 25–39.

[45] J. H. Silverman, *The Arithmetic of elliptic curves*, Springer-Verlag, New York, 1992.

[46] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[47] D. Simon, *Programme de calcul du rang des courbes elliptiques dans les corps de nombres*, Université de Caen. Web: http://www.math.unicaen.fr/∼simon/ell.gp.

[48] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. **108** (1983) **no. 2**, 451–463

[49] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris **273** (1971), 238–241.