JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jerson CARO

Watkins's conjecture for quadratic twists of Elliptic Curves with Prime Power Conductor

Tome 37, nº 2 (2025), p. 647-663.

https://doi.org/10.5802/jtnb.1335

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **37** (2025), 647–663

Watkins's conjecture for quadratic twists of Elliptic Curves with Prime Power Conductor

par Jerson CARO

Dedicated to the memory of my father

Résumé. La conjecture de Watkins affirme que le rang d'une courbe elliptique est borné par la valuation 2-adique de son degré modulaire. Nous montrons que cette conjecture est vraie lorsque E est une tordue quadratique d'une courbe elliptique avec un point rationnel d'ordre 2 et de conducteur une puissance de nombre premier, en particulier pour les courbes elliptiques associées aux nombres congruents. De plus, nous donnons une borne inférieure pour le *congruence number* des courbes elliptiques de la forme $y^2 = x^3 - dx$, où d est un entier sans facteur biquadratique.

Abstract. Watkins's conjecture asserts that the rank of an elliptic curve is upper bounded by the 2-adic valuation of its modular degree. We show that this conjecture is satisfied when E is any quadratic twist of an elliptic curve with a rational point of order 2 and prime power conductor, in particular, for the congruent number elliptic curves. Furthermore, we give a lower bound for the congruence number for elliptic curves of the form $y^2 = x^3 - dx$, with d a fourth power free integer.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. The modularity theorem [4, 27, 29] ensures the existence of a non-constant morphism $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$. Denote by ϕ_E the morphism, up to sign, which has minimal degree and which sends the cusp $i\infty$ to the neutral point of E. *The modular degree* m_E of E is the degree of ϕ_E. There are many relevant conjectures in number theory about this invariant. One of them, equivalent to ABC conjecture [12], is to give polynomial bounds of its size in terms of the conductor. The following conjecture is the main topic of this paper.

Conjecture 1.1 (Watkins [28])**.** For every elliptic curve E over $\mathbb{Q}$ we have $r \leq \nu_2(m_E)$, where ν_p denotes the p-adic valuation and $r := \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$.

Manuscrit reçu le 29 mars 2024, révisé le 13 août 2024, accepté le 20 septembre 2024.
2020 *Mathematics Subject Classification.* 11G05, 11G18, 11G40.
Mots-clefs. Watkins's conjecture, elliptic curves, modular degree, Mordell–Weil rank.
This research was supported by ANID Doctorado Nacional 21190304.

One particular case of this conjecture is to prove that when m_E is odd, then $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0$. In this direction, there is great progress. For example, Kazalicki and Kohen [14, 15] proved that if the congruence number δ_E of E (which is a multiple of the modular degree m_E) is odd, then $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0$. From this, it may be deduced (see Proposition 4.3) that Watkins's conjecture holds for elliptic curves with conductor a prime power and nontrivial rational 2-torsion, (cf. Section 4).

When the elliptic curves has a rational point of order 2, using Selmer groups an upper bound for r can be given in terms of $\omega(N)$. Here, N is the conductor of E, and $\omega(N)$ is the number of distinct prime factors of N (cf. Section 2.3). This upper bound allowed Esparza-Lozano & Pasten [11] to prove that Watkins's conjecture holds for a quadratic twist $E^{(D)}$ by D with $\omega(D)$ large enough, whenever E has a rational point of order 2.

A natural question emerges: When do all the quadratic twists of an elliptic curve E satisfy Watkins's conjecture? In this paper we prove that this conjecture holds for any quadratic twist of an elliptic curve with a rational point of order 2 and prime power conductor.

Theorem 1.2. *Let E be an elliptic curve with a rational point of order 2. Assume that E is a quadratic twist of an elliptic curve with prime power conductor. Then E satisfies Watkins's conjecture.*

To prove that if $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) > 0$ then $2 \mid m_E$, because of Theorem 1 in [5], the only missing case is when E has conductor N divisible by at most two odd primes, additive reduction at 2 and a rational point of order 2. Thus, the previous Theorem covers many of those cases.

Another application of this theorem is the following: An integer D is a *congruent number* if there exists a right triangle such that its sides are rational and its area equals D. An important problem in number theory is to know when an integer number D is a congruent number, which is equivalent to know if the elliptic curve $y^2 = x^3 - D^2x$ has positive Mordell–Weil rank r, see [16]. A crucial observation is that for an integer D, $E^{(D)} : y^2 = x^3 - D^2x$ is the quadratic twist by D of the elliptic curve $E : y^2 = x^3 - x$, which has conductor 32. Applying [11, Theorem 1.2], we have that for a positive squarefree integer D, with $\omega(D) \geq 12$, Watkins's conjecture holds for $E^{(D)}$. Thanks to Theorem 1.2, we show this conjecture unconditionally. More precisely:

Corollary 1.3. *Watkins's conjecture holds for all congruent curves $E^{(D)} : y^2 = x^3 - D^2x$.*

Since the elliptic curve $y^2 = x^3 - x$ has complex multiplication by $\mathbb{Z}[i]$ we may consider its quartic twists. However, the process we use to prove Theorem 1.2 seems not useful for quartic twists, since we need to find a lower bound of the 2-adic valuation of an infinite product. Although we

cannot give an applicable lower bound for $\nu_2(m_E)$, we found an alternative process that provides us a lower bound of $\nu_2(\delta_E)$.

Theorem 1.4. *Let d be an odd squarefree integer and D any divisor of d. For the elliptic curve $E : y^2 = x^3 - dD^2x$ we have that*

$$2\left\lfloor \frac{\omega(d)+1}{2} \right\rfloor + 1 \leq \nu_2(\delta_E).$$

This theorem allows us to prove that for some elliptic curves $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq \nu_2(\delta_E)$. This result goes into the direction of Watkins's conjecture since $m_E \mid \delta_E$ as we mentioned before.

Corollary 1.5. *Let p be an odd prime. Then for E an elliptic curve $y^2 = x^3 - px$ or $y^2 = x^3 - p^3x$, we have that* $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) < \nu_2(\delta_E)$.

2. Preliminaries

2.1. 2-adic valuation of the modular degree. [11, Lemma 3.1] gives an equation that relates the modular degree of an elliptic curve E with that of its quadratic twist $E^{(D)}$ by D, where D is any fundamental discriminant. We denote by N and $N^{(D)}$ the conductors of E and $E^{(D)}$, respectively. Before showing this equation, we have to define some invariants which appear on it.

2.1.1. *Petersson Norm.* Let $S_2(\Gamma_0(N))$ be the space of weight 2 cuspidal holomorphic modular forms; over this space, we have an inner product that allows us to define the following norm.

Definition 2.1. The Petersson norm of $f \in S_2(\Gamma_0(N))$ is defined by

$$\|f\|_N = \left(\int_{\Gamma_0(N)\backslash \mathfrak{h}} |f(z)|^2 \mathrm{d}x \wedge \mathrm{d}y \right)^{1/2}, \qquad z = x + iy \text{ and } y > 0.$$

Observation 2.2. Although this definition depends on the level N, we know that if $N \mid M$ and $f \in S_2(\Gamma_0(N))$, then $f \in S_2(\Gamma_0(M))$ and $\|f\|_M^2 = [\Gamma_0(N) : \Gamma_0(M)]\|f\|_N^2$.

2.1.2. *Manin Constant.* Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and let ω_E be its Néron differential. We have that $\phi_E^*\omega_E$ is a regular differential on $X_0(N)$, which implies the following formula:

$$\phi_E^*\omega_E = 2\pi i c_E f_E(z)\mathrm{d}z$$

where c_E is a rational number and f_E denotes the Hecke newform attached to E. Due to [10, Proposition 2], c_E, which we call the Manin constant, is an integer uniquely defined up to sign.

The mentioned equation given by [11, Lemma 3.1] is the following:

$$\frac{m_{E^{(D)}}}{c^2_{E^{(D)}}} = \frac{m_E}{c_E^2} \times \frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N} \left|\frac{\Delta_{E^{(D)}}}{\Delta_E}\right|^{1/6}, \tag{2.1}$$

where Δ_E denotes the global minimal discriminant of E. Equation (2.1) implies the following lemma:

Lemma 2.3. *Let E be an elliptic curve and $E^{(D)}$ its quadratic twist by D. Then*

$$\nu_2(m_{E^{(D)}}) \geq \nu_2\left(\frac{m_E}{c_E^2}\right) + \nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) + \frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right). \tag{2.2}$$

2.2. Elliptic curves with a rational point of order 2 and prime power conductor. In this section, we classify all the elliptic curves defined over $\mathbb{Q}$ with nontrivial rational 2-torsion and conductor a power of a prime.

Remark 2.4. Suppose that E is an elliptic curve with conductor a power of a prime p^α. Then we have that $\alpha \leq 2$ for $p > 3$, $\alpha \leq 5$ for $p = 3$ and $\alpha \leq 8$ for $p = 2$ (see [25, IV.10]).

We shall write $[a_1, a_2, a_3, a_4, a_6]$ for the elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We begin with the elliptic curves with prime conductor. Setzer [23] proved that for $p \neq 17$ there exists an elliptic curve with prime conductor p and a rational point of 2 if and only if $p = u^2+64$ for some integer u, in which case there are two nonisomorphic elliptic curves with conductor p. The minimal models of these elliptic curves are:

TABLE 2.1. Elliptic curves with prime conductor $p > 17$ and nontrivial rational 2-torsion

LMFDB label	Weierstrass coefficients	Δ	2-Torsion
$p.a1$	$[1, (u-1)/4, 0, -1, 0]$	p	$\mathbb{Z}/2\mathbb{Z}$
$p.a2$	$[1, (u-1)/4, 0, 4, u]$	$-p^2$	$\mathbb{Z}/2\mathbb{Z}$

A 2-isogeny connects these two elliptic curves. Moreover, the work of Mestre & Oesterlé [19] implies that the curve $p.a2$ is the $X_0(p)$-optimal, where an elliptic curve E is called $X_0(N)$-optimal if it has the minimal modular degree m_E in its isogeny class. Additionally, every other modular parametrization of a curve in the isogeny class factors through the minimal-degree modular parametrization of the optimal curve.

For $p = 17$ Setzer [23] shows that there are four nonisomorphic elliptic curves. From now on, $(*)$ indicates which elliptic curve is the $X_0(N)$-optimal.

TABLE 2.2. Elliptic curves with conductor 17

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ	2-Torsion
$17.a1$	$[1,-1,1,-91,-310]$	4	2	17	$\mathbb{Z}/2\mathbb{Z}$
$17.a2$	$[1,-1,1,-6,-4]$	2	2	17^2	$(\mathbb{Z}/2\mathbb{Z})^2$
$17.a3(*)$	$[1,-1,1,-1,-14]$	1	1	-17^4	$\mathbb{Z}/2\mathbb{Z}$
$17.a4$	$[1,-1,1,-1,0]$	4	4	17	$\mathbb{Z}/2\mathbb{Z}$

On the other hand, Mulholland [20] proved that for $p > 3$ the elliptic curves with a rational point of order 2 and conductor p^2 are the quadratic twist by p of the elliptic curves in Tables 2.1 and 2.2 by p, together with the ones with conductor 49 listed below:

TABLE 2.3. Elliptic curves with conductor 49

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ	2-Torsion
$49.a1$	$[1,-1,0,-1822,30393]$	14	1	7^9	$\mathbb{Z}/2\mathbb{Z}$
$49.a2$	$[1,-1,0,-107,552]$	7	1	7^9	$\mathbb{Z}/2\mathbb{Z}$
$49.a3$	$[1,-1,0,-37,-78]$	2	1	7^3	$\mathbb{Z}/2\mathbb{Z}$
$49.a4(*)$	$[1,-1,0,-2,-1]$	1	1	7^2	$\mathbb{Z}/2\mathbb{Z}$

By Remark 2.4 we have classified the elliptic curves whose conductor is a power of a prime for $p > 3$ and nontrivial rational 2-torsion. Using the database [17], we can classify the elliptic curves with a rational point of order 2 and conductor a power of 2 or 3. We noticed that there are no elliptic curves with a rational point of order 2 of conductor 3^m for any integer m. Thus, by Remark 2.4 we only need to list the ones with conductor 2^m with $m \in \{5,6,7,8\}$.

The following table shows the elliptic curves with conductor 2^5:

TABLE 2.4. Elliptic curves with conductor 32

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ	2-Torsion
$32.a1$	$[0,0,0,-11,-14]$	4	2	2^9	$\mathbb{Z}/2\mathbb{Z}$
$32.a2$	$[0,0,0,-11,14]$	4	2	2^9	$\mathbb{Z}/2\mathbb{Z}$
$32.a3$	$[0,0,0,-1,0]$	2	2	2^6	$(\mathbb{Z}/2\mathbb{Z})^2$
$32.a4(*)$	$[0,0,0,4,0]$	1	1	-2^{12}	$\mathbb{Z}/2\mathbb{Z}$

Let us mention that 32.a3 is called the *congruent number* curve. Meanwhile, the elliptic curves of conductor 2^6 are the quadratic twists of the previous ones by 2. Finally, the elliptic curves with conductor 2^7 are listed in the following table and again the elliptic curves of conductor 2^8 are the quadratic twists of the previous ones by 2.

Table 2.5. Elliptic curves with conductor 128

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ	2-Torsion
$128.a1$	$[0,1,0,-9,7]$	8	1	2^{13}	$\mathbb{Z}/2\mathbb{Z}$
$128.a2(*)$	$[0,1,0,1,1]$	4	1	-2^8	$\mathbb{Z}/2\mathbb{Z}$
$128.b1$	$[0,1,0,-2,-2]$	16	2	2^7	$\mathbb{Z}/2\mathbb{Z}$
$128.b2(*)$	$[0,1,0,3,-5]$	8	1	-2^{14}	$\mathbb{Z}/2\mathbb{Z}$
$128.c1$	$[0,-1,0,-9,-7]$	8	1	2^{13}	$\mathbb{Z}/2\mathbb{Z}$
$128.c2(*)$	$[0,-1,0,1,-1]$	4	1	-2^8	$\mathbb{Z}/2\mathbb{Z}$
$128.d1$	$[0,-1,0,-2,2]$	16	2	2^7	$\mathbb{Z}/2\mathbb{Z}$
$128.d2(*)$	$[0,-1,0,3,5]$	8	1	-2^{14}	$\mathbb{Z}/2\mathbb{Z}$

2.3. The Mordell–Weil Rank. [26, Section X.4] gives a bound for a 2-isogeny Selmer rank. This work allows Caro & Pasten [6] to find an upper bound for the Mordell–Weil rank of an elliptic curve with nontrivial rational 2-torsion

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2\omega(N) - 1. \tag{2.3}$$

Furthermore, [3, Proposition 1.1] shows that if the elliptic curve has minimal Weierstrass equation $y^2 = x^3 + Ax^2 + Bx$, we obtain that

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq \omega(A^2 - 4B) + \omega(B) - 1. \tag{2.4}$$

We define the function $\delta_2(D)$ on the set of integers as follows:

$$\delta_2(D) = \begin{cases} 1 & \text{if } 2 \mid D \\ 0 & \text{otherwise.} \end{cases}$$

Using inequality (2.4) we have the following lemma:

Lemma 2.5. *Let E be an elliptic curve with a rational point of order 2 and prime power conductor $N = p^\alpha$, and let $E^{(D)}$ its quadratic twist by D, with D a fundamental discriminant. Then we have*

$$\operatorname{rank}_{\mathbb{Z}}(E^{(D)}(\mathbb{Q})) \leq 2\omega(D) + 1 - 2\nu_p(D).$$

Even sharper, if E is $32.a3$ we have

$$\operatorname{rank}_{\mathbb{Z}}(E^{(D)}(\mathbb{Q})) \leq 2\omega(D) - \delta_2(D).$$

Proof. We know that $E^{(D)}[2] \cong E[2]$ as Galois modules because one is the other multiplied by the character χ_D and χ_D takes values congruent to 1 (mod 2). Then $E^{(D)}$ also has nontrivial rational 2-torsion, so applying the inequality (2.3) we have

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}}(E^{(D)}(\mathbb{Q})) &\leq 2\omega(N^{(D)}) - 1 \leq 2(\omega(D) + (1 - \nu_p(D))) - 1 \\ &= 2\omega(D) + 1 - 2\nu_p(D). \end{aligned}$$

The second inequality is derived from the observation that the primes dividing $N^{(D)}$ are exactly those primes that divide D and p. If E is $32.a3$ its quadratic twist $E^{(D)}$ is $y^2 = x^3 - D^2x$, in particular, we can apply inequality (2.4), so we obtain

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) &\leq \omega(4D^2) + \omega(-D^2) - 1 \\ &= \omega(D) + (1 - \delta_2(D)) + \omega(D) - 1 \\ &= 2\omega(D) - \delta_2(D),\end{aligned}$$

which ends the proof. □

Remark 2.6. Note that we can also apply the inequality (2.4) to $y^2 = x^3 - dx$, for any integer d, and again, we obtain that $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2\omega(d) - \delta_2(d)$.

3. Lower bounds for some 2-adic valuations

This section aims to give lower bounds for the 2-adic valuation of the invariants in Lemma 2.3.

3.1. Minimal discriminants. We start by finding a lower bound for

$$\nu_2\left(\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right)^{1/6}\right) = \frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right). \tag{3.1}$$

Definition 3.1. Let p be a prime. The p-adic signature of an elliptic curve E is the triple $(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta(E)))$, where c_4, c_6 are the usual Weierstrass invariants of a minimal model of E and $\Delta(E)$ denotes the minimal discriminant of E.

Pal [21] classifies the valuation (3.1) in terms of the 2-adic signature of E. To begin with, we compute the 2-adic signature of an elliptic curve with odd discriminant and a rational point of order 2.

Lemma 3.2. *Let E be an elliptic curve with a rational point of order 2 and odd discriminant. Then the 2-adic signature of E is $(0, 0, 0)$.*

Proof. Assume that the minimal model of E is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Since E has good reduction at 2, then either a_1 or a_3 must be odd. Furthermore, because $E(\mathbb{Q})[2] \neq \{0\}$, there exists $x_0 \in \mathbb{Q}$ such that

$$x_0^3 + b_2x_0^2 + 8b_4x_0 + 16b_6 = 0, \tag{3.2}$$

where b_2, b_4 and b_6 are the usual Weierstrass invariants. We first suppose for a contradiction that a_1 is even. Then $\nu_2(b_2) = \nu_2(a_1^2+4a_2) \geq 2$, $\nu_2(b_4) = \nu_2(a_1a_3 + 2a_4) \geq 1$, and a_3 must be odd, hence $b_6 = a_3^2 + 4a_6$ is odd too. Consequently, the Newton polygon (as it is noticed in Section 2 of [23])

attached to (3.2) is a line with slope $-4/3$, so, by Dumas's irreducibility criterion (cf. the corollary in p. 55 of [22]) this polynomial has no rational solutions, which is a contradiction. Hence b_2 is odd, and therefore $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ are odd too. □

Corollary 3.3. *Let E be an elliptic curve with a rational point of order 2 and odd discriminant. Then we have*

$$\frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right) \geq \begin{cases} 0 & \text{if } D \equiv 1 \pmod 4 \\ 2 & \text{if } 2 \mid D. \end{cases}$$

Proof. By [21, Proposition 2.4.2.(a)] if $D \equiv 1 \pmod 4$, $\nu_2(\Delta_E) = \nu_2(\Delta_{E^{(D)}})$. On the other hand, if $2 \mid D$ the associated squarefree integer D^* to D is congruent to -1 or 2 modulo 4. Lemma 3.2 implies that the 2-adic signatue of E is $(0, 0, 0)$. By [21, Proposition 2.4.2.(b).i] when $D^* \equiv -1 \pmod 4$, $\nu_2(\Delta_E) = \nu_2(\Delta_{E^{(D)}}) = 12$. Finally, by [21, Proposition 2.4.2.(c).i] when $D^* \equiv 2 \pmod 4$, $\nu_2(\Delta_E) = \nu_2(\Delta_{E^{(D)}}) = 18$. □

Finally, we list the 2-adic signature of the elliptic curves with conductor 2^5 and 2^7. Analogously to the proof of Corollary 3.3, Table 3.1 and [21, Proposition 2.4.2] imply the following lemma:

TABLE 3.1. 2-adic signature

LMFDB label	$(c_4(E), c_6(E))$	2-adic signature
32.a1	$(528, 12096)$	$(4, 6, 9)$
32.a2	$(528, -12096)$	$(4, 6, 9)$
32.a3	$(48, 0)$	$(4, \infty, 6)$
32.a4	$(-192, 0)$	$(6, \infty, 12)$
128.a1	$(448, -8704)$	$(6, 9, 13)$
128.a2	$(-32, -640)$	$(5, 7, 8)$
128.b1	$(112, 1088)$	$(4, 6, 7)$
128.b2	$(-128, 5120)$	$(7, 10, 14)$
128.c1	$(448, 3392)$	$(6, 6, 13)$
128.c2	$(-32, 1088)$	$(5, 6, 8)$
128.d1	$(112, -2368)$	$(4, 6, 7)$
128.d2	$(-128, -3520)$	$(7, 6, 14)$

Lemma 3.4. *Let E be an elliptic curve with conductor 2^5 or 2^7. Then we have*

$$\frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right) \geq -\delta_2(D)$$

3.2. Petersson norms. Now we want to relate the 2-adic valuation of the Petersson norms of $f_{E^{(D)}}$ and f_E.

Proposition 3.5. *Let E be an elliptic curve with a rational point of order 2 and minimal conductor N among all its quadratic twists.*

(i) *Assume that N is a power of an odd prime, and if $N = p^2$, we only consider D such that $p \nmid D$. Then, we have*

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3\omega(D).$$

(ii) *Furthermore, if E is 17.a4 in Table 2.2 we have*

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4\omega(D).$$

(iii) *If N is 2^5 or 2^7 we have*

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3\omega(D) - 2\delta_2(D).$$

(iv) *Furthermore, if E is 32.a3 in Table 2.4 we have*

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4\omega(D) - 3\delta_2(D).$$

Proof. The Rankin–Selberg method (cf. [24]) shows that

$$\|f_E\|^2_N = \frac{N}{8\pi^3} L(\operatorname{Sym} f, 2),$$

where $L(\operatorname{Sym} f, 2)$ denotes the symmetric square L-function associated to f (see [9, Equation 2] for its definition). Delaunay [9] compares the local factors of $L(\operatorname{Sym} f, 2)$ and $L(\operatorname{Sym} f^{(D)}, 2)$ gives an equation relating $\|f_E\|^2_N$ to $\|f_{E^{(D)}}\|^2_{N^{(D)}}$ (see [9, Theorem 1]). To state this equation, let us fix some notation. For a prime number q we define $V(q) = (q-1)(q+1-a_q)(q+1+a_q)$, and $U(q) = (q-1)(q+1)$, where a_q is the Fourier coefficient of f_E. Finally, we define $U_2 = 2(3-a_2)(3+a_2)$. Assume that N is a power of an odd prime p. Since $p \mid D$ only if $N = p$, then according to the notation of Delaunay in [9], $D_1 = p$. Thus, taking 2-adic valuations [9, Theorem 1] implies that

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq \nu_p(D)\nu_2(U(p)) + \nu_2(D)\nu_2(U_2) + \sum_{\substack{q \mid D \\ q \neq 2,p}} \nu_2(V(q)).$$

In view of the fact that $E(\mathbb{Q})[2]$ reduces injectively into $E(\mathbb{F}_q)$ for $q \notin \{2, p\}$, we have $q + 1 \equiv a_q(E) \pmod 2$, in particular, $\nu_2(V(q)) \geq 3$. Furthermore, the database [17] tells us that $2 \mid 3 - a_2, 3 + a_2$ for elliptic curves with conductor 17 or 49, and an inspection of the reduction modulo 2 of $p.a1$

and $p.a2$ for $p > 17$ shows that $2 \mid \#E(\mathbb{F}_2)$, which shows that $\nu_2(U_2) \geq 3$. Finally, it is clear that $\nu_2(U(p)) \geq 3$, then

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3\left(\nu_p(D) + \delta_2(D) + \sum_{\substack{q|D \\ q\neq 2,p}} 1\right) = 3\omega(D),$$

which proves (i).

To prove (ii), we notice that $\#E(\mathbb{Q})[4] = 4$ and due to the fact that $E(\mathbb{Q})[4]$ reduces injectively into $E(\mathbb{F}_q)$ for $q \notin \{2, p\}$, we have $q+1 \equiv a_q(E) \pmod 4$, in particular, $\nu_2(V(q)) \geq 4$. We also know by the database [17] that $a_2 = -1$ then $\nu_2(U_2) = 4$ and $\nu_2(U(17)) = 5$. Putting all together we obtain

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4\left(\nu_p(D) + \delta_2(D) + \sum_{\substack{q|D \\ q\neq 2,p}} 1\right) = 4\omega(D).$$

For (iii), we note that for N equal to 2^5 or 2^7 [9, Theorem 1] says that

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) = \delta_2(D) + \sum_{\substack{q|D \\ q\neq 2}} \nu_2(V(q)).$$

As we saw before $\nu_2(V(q)) \geq 3$ for $q \neq 2$, then

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq \nu_2(D) + 3(\omega(D) - \delta_2(D)) = 3\omega(D) - 2\delta_2(D).$$

Finally, to prove (iv), we only need to notice that for the curve $32.a3$ $\#E(\mathbb{Q})[2] = 4$, then $\nu_2(V(q)) \geq 4$ for $q \neq 2$, which ends the proof. □

Remark 3.6. Notice that if D is prime and $D \equiv 1 \pmod 4$ and relatively prime to N we can improve the bounds given in (i) and (ii), since $\nu_2(V(D))$ is higher. In this case, we have $\nu_2(\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N) \geq 4$ if N is a power of an odd prime, and $\nu_2(\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N) \geq 5$ if E is $17.a4$.

3.3. Manin constant. Now, we compute c_E of the elliptic curves E in Table 2.1.

Proposition 3.7. *Let E be an elliptic curve, $X_0(N)$-optimal with odd squarefree conductor N, and let E' an elliptic curve connected with E by a 2 isogeny $\theta : E \to E'$. Then we have that $c_E = 1$ and $c_{E'} \in \{1, 2\}$.*

Proof. By [18, Corollary 4.2], c_E must be a power of 2, and [1, Theorem A] says that if $p \mid c_E$ then $p \mid N$, which implies that $c_E = 1$. Now, let $\mathcal{E}$ and $\mathcal{E}'$

be the Néron models of E and E', and ω, ω' their respective Néron differentials. Since θ and $\theta^\vee$ define morphisms $\theta^* : H^0(\mathcal{E}', \Omega^1_{\mathcal{E}'/\mathbb{Z}}) \to H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathbb{Z}})$ and $(\theta^\vee)^* : H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathbb{Z}}) \to H^0(\mathcal{E}', \Omega^1_{\mathcal{E}'/\mathbb{Z}})$, there are $a, b \in \mathbb{Z}$ such that $\theta^*\omega' = a\omega$ and $(\theta^\vee)^*\omega = b\omega'$. Due to the optimality of ϕ_E we have that $\phi_{E'} = \theta \circ \phi_E$, which implies that

$$\phi^*_{E'}\omega' = \phi^*_E\theta^*\omega' = a\phi^*_E\omega = 2\pi i a f_E(z)\mathrm{d}z,$$

hence $c_{E'} = a$. On the other hand, we have that $a \mid 2$ since

$$ab\omega = \theta^*(\theta^\vee)^*\omega = [2]^*\omega = 2\omega,$$

which ends the proof. □

Corollary 3.8. *Let E be an elliptic curve with a rational point of order 2 and prime conductor $p > 17$. Then $\nu_2(m_E/c_E^2) \geq -1$.*

Proof. We denote $E_{p,1}$ and $E_{p,2}$ the curves $p.a1$ and $p.a2$ in Table 2.1, respectively. As we discussed before, there is a 2-isogeny θ between these two curves, and the work of [19] shows that $E_{p,2}$ is $X_0(p)$-optimal. Because of Proposition 3.7 $c_{E_{p,1}} \in \{1, 2\}$ and $c_{E_{p,2}} = 1$, in particular, $\nu_2(m_{E_{p,2}}/c^2_{E_{p,2}}) \geq 0$. Since $\phi_{E_{p,1}} = \theta \circ \phi_{E_{p,2}}$, we have that $m_{E_{p,1}} = 2m_{E_{p,2}}$ therefore $\nu_2(m_{E_{p,1}}) \geq 1$, consequently

$$\nu_2(m_{E_{p,1}}/c^2_{E_{p,1}}) \geq \nu_2(m_{E_{p,1}}) - 2 \geq -1,$$

which gives the desired result. □

4. The Main Result

Before proving Theorem 1.2, we need the following definition and proposition:

Definition 4.1. Let E be an elliptic curve defined over $\mathbb{Q}$ and $f_E = \sum_{n=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$ be its Hecke newform. The congruence number δ_E of E is the largest integer such that there is a modular form $g = \sum_{n=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$ with $b_n \in \mathbb{Z}$, such that g and f_E are orthogonal with respect to the Petersson inner product, and $a_n \equiv b_n \pmod{\delta_E}$ for all n.

Remark 4.2. There are some relations between the modular degree and the congruent number. The most relevant is $m_E \mid \delta_E$, whenever E is $X_0(N)$-optimal [7].

The following proposition will play a key role in the proof of Theorem 1.2 when the prime p, dividing both the conductor and the fundamental discriminant D, is considered.

Proposition 4.3. *Watkins's conjecture holds for every elliptic curve E of prime power conductor and a rational point of order 2.*

Proof. Watkins's conjecture is known for elliptic curves of conductor $N < 10000$. In particular, this includes all the elliptic curves with conductor a power of 2. Then, we assume that the conductor is odd. By (2.3), $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 1$. Thus, it is enough to prove that if m_E is odd, $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0$. [2, Theorem 2.2] says that if a prime p divides the ratio δ_E/m_E, then $p^2 \mid N$, consequently, δ_E is odd. Finally, [14, Theorem 1.1], as corrected in [15], implies that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0$. □

Proof of Theorem 1.2. Note that the quadratic twists of $E^{(D)}$ are E itself, or quadratic twists of E. Because of the classification of Section 2 it is enough to prove the theorem for elliptic curves with conductor 2^5, 2^6, 17, 49 and prime numbers of the form $u^2 + 64$ for some integer u.

Suppose that E has conductor $N = 49$, $E^{(7)}$ has conductor $N^{(7)} = 49$ and a rational point of order 2. Notice that if $7 \nmid D'$, $E^{(7D')} = (E^{(7)})^{(D')}$, so, we can assume that $7 \nmid D$, and we can then use Proposition 3.5 (i), freely.

To begin with, we assume that N is odd and E is different to 17.a4. By Corollary 3.8 and Section 2.2 we have that $\nu_2(m_E/c_E^2) \geq -1$. Applying Corollary 3.3 and Proposition 3.5 (i) to Lemma 2.3, (2.2) turns into

$$\nu_2(m_{E^{(D)}}) \geq -1 + 3\omega(D).$$

In the case of 17.a4, we have that $\nu_2(m_E/c_E^2) = -2$ and therefore applying Proposition 3.5 (ii) and Corollary 3.3 to Lemma 2.3 we obtain

$$\nu_2(m_{E^{(D)}}) \geq -2 + 4\omega(D).$$

Meanwhile, Lemma 2.5 implies that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2\omega(D) + 1$, hence in both cases Watkins's conjecture holds for $\omega(D) \geq 2$.

Now, assume D is the fundamental discriminant associated to a prime number. Proposition 4.3 proves the case $D \mid N$. Given Lemma 2.5, we only have to prove that $\nu_2(m_{E^{(D)}}) \geq 3$, then Remark 3.6 proves the case $D \equiv 1 \pmod 4$. For D such that $2 \mid D$, Corollary 3.3 implies that $(1/6)\nu_2\left(\Delta_{E^{(D)}}/\Delta_E\right) \geq 2$, then for E different that 17.a4 we have $\nu_2(m_{E^{(D)}}) \geq -1+3+2 = 4$. Finally, when E is 17.a4 we obtain $\nu_2(m_{E^{(D)}}) \geq -2 + 4 + 2 = 4$.

Now, suppose that E has conductor 2^5 or 2^7, and different to 32.a3, in which case $\nu_2(m_E/c_E^2) \geq 0$. As a consequence, Proposition 3.5 (iii) and Lemma 3.4 applied to Lemma 2.3 imply

$$\nu_2(m_{E^{(D)}}) \geq 3\omega(D) - 3\delta_2(D),$$

and Lemma 2.5 says that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2\omega(D)+1-2\delta_2(D)$, and therefore Watkins's conjecture holds for $\omega(D) \geq 1 + \delta_2(D)$. Thus, the only missing case is $D = 2$, which is covered by Proposition 4.3.

Finally, for E equal to $32.a3$ we have $\nu_2(m_E/c_E^2) = -1$. In this situation, Lemma 2.5 tells us that

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2\omega(D) - \delta_2(D).$$

On the other hand, Applying again Proposition 3.5 (iv) and Lemma 3.4 to Lemma 2.3 we obtain

$$\nu_2(m_{E^{(D)}}) \geq -1 + 4\omega(D) - 4\delta_2(D),$$

and we notice that the inequality $2\omega(D) - \nu_2(D) \leq -1 + 4\omega(D) - 4\delta_2(D)$ is equivalent to

$$\omega(D) \geq \frac{1 + 3\delta_2(D)}{2}.$$

Then, the only missing case is $D = 2$, which again is covered by Proposition 4.3. □

5. Congruence Number of $y^2 = x^3 - dx$

[30, Theorem 2.8] shows that the elliptic curves of the form $y^2 = x^3 - Dx$ have even congruence number, whenever $\omega(D) \geq 1$. The idea of this section is to give a lower bound for $\nu_2(\delta_E)$. First of all, let $p_1, \ldots, p_m$ be a list of distinct odd primes with $m \geq 1$ and define $d = p_1 \cdots p_m > 1$. Let D be a divisor of d. Now, consider the elliptic curves $E : y^2 = x^3 - dx$ and $E^{(D)} : y^2 = x^3 - dD^2x$. Finally, denote by f and $f^{(D)}$ their associated Hecke newforms. Since $E^{(D)}$ is a quadratic twist by D of E, then we have that

$$a_q(f^{(D)}) = \left(\frac{D}{q}\right) a_q(f), \tag{5.1}$$

for every prime number q. Before proving Theorem 1.4 we need the following two lemmas.

Lemma 5.1. *Let n be a positive integer relatively prime to d and $q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ its prime factorization. Then $a_n(f^{(D)}) = \gamma_n(D) a_n(f)$, where*

$$\gamma_n(D) = \left(\frac{D}{q_1}\right)^{\alpha_1} \cdots \left(\frac{D}{q_s}\right)^{\alpha_s}.$$

Proof. Since $\gamma_{nm}(D) = \gamma_n(D)\gamma_m(D)$, it is enough to show this assertion for power of primes. We prove it by induction, taking into account $a_1(f) = 1$ and $a_q(f) = \left(\frac{d}{p}\right) a_q(g)$, as follows

$$\begin{aligned} a_{q^{n+1}}(f^{(D)}) &= a_q(f^{(D)}) a_{q^n}(f^{(D)}) - p a_{q^{n-1}}(f^{(D)}) \\ &= \left(\frac{D}{q}\right) a_q(f) \left(\frac{D}{q}\right)^n a_{q^n}(f) - p \left(\frac{D}{q}\right)^{n-1} a_{q^{n-1}}(f) = \left(\frac{D}{q}\right)^{n+1} a_{q^{n+1}}(f), \end{aligned} \tag{5.2}$$

which gives the desired result. □

Lemma 5.2. *Let m be an odd integer and q be a prime, such that $q \nmid d$. If $\left(\frac{d}{q}\right) = 1$ then $a_{q^m}(f) \equiv 0 \pmod 2$ and if $\left(\frac{d}{q}\right) = -1$ then $a_{q^m}(f) \equiv 0 \pmod 4$.*

Proof. We know that E is a quartic twist of $E_1 : y^2 = x^3 - x$ by d. There is a Grossencharacter χ of $\mathbb{Q}(i)$ (equally $\overline{\chi}$), associated with the CM curve $E_1/\mathbb{Q}$, in the sense that the Hecke eigenform attached to E_1 is a theta series for χ, and $L(E_1/\mathbb{Q}, s) = L(\chi/\mathbb{Q}(i), s)$ (see [25, II. Theorem 10.5]). The conductor of χ is $\mathfrak{p}^3$, where $\mathfrak{p} = (1+i)$, and order 4. By [8, Section 3.2], $\chi\psi$, where $\psi = \left(\frac{\cdot}{d}\right)_4$ is likewise associated with E_d.

First of all, if $q \equiv 3 \pmod 4$ we have $a_q(E) = 0$ since $\#E(\mathbb{F}_q) = q + 1$ by [25, Exercise 2.33(a)]. By induction on (5.2) we obtain that $a_{q^m}(E) = 0$ for m any odd integer.

Finally, assume that $q \equiv 1 \pmod 4$. Since E has a rational 2-torsion point we have that for every prime q such that $(q, 2d) = 1$, $a_q(f) \equiv 0 \pmod 2$. Moreover, if $\left(\frac{d}{q}\right) = -1$ then $(a_q(f)/2)^2 + (a_q(g)/2)^2 = p$, so, $a_q(f) \equiv 0 \pmod 4$. By induction on (5.2), we get the desired result. □

Proof of Theorem 1.4. We define $n_1 = p_1^{\nu_{p_1}(n)} \cdots p_m^{\nu_{p_m}(n)}$ and $n_2 = n/n_1$. Let us also define the cusp form

$$h = \sum_{\substack{D|d \\ D\neq 1}} (-1)^{\omega(D)+1} f^{(D)}.$$

By [13, Table I] $N = N^{(D)}$ for every divisor D of d. Consequently, for every divisor D of d, $f^{(D)}$ and f are orthogonal with respect to the Petersson inner product, since they are different newforms in the same level. Therefore, h and f are also orthogonal. Hence, it is enough to prove that:

$$a_n(f) - a_n(h) = \sum_{D|d} (-1)^{\omega(D)} a_n(f^{(D)}) \equiv 0 \pmod{2^{m+\epsilon}},$$

where $\epsilon = 1$ if m is even and $\epsilon = 2$ if m is odd. Assume that $n_2 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, then by Lemma 5.1 we have $a_{n_2}(f^{(D)}) = \gamma_{n_2}(D) a_{n_2}(f)$. We claim that

$$\sum_{D|d} (-1)^{\omega(D)} a_n(f^{(D)}) = \begin{cases} 2^m a_n(f) & \text{if } \gamma_{n_2}(p) = -1 \text{ for all } p \mid d \\ 0 & \text{otherwise.} \end{cases}$$

Before proving the claim, notice that if $p \mid d$, we have $a_p(f) = 0$ and by (5.1) $a_p(f^{(D)}) = 0$. Therefore, by (5.2) $a_{n_1}(f) = a_{n_1}(f^{(D)})$ for every divisor D of d, and consequently

$$\sum_{D|d} (-1)^{\omega(D)} a_n(f^{(D)} = a_{n_1}(f) \sum_{D|d} (-1)^{\omega(D)} a_{n_2}(f^{(D)}).$$

To begin with, assume that for some $p \mid d$, $\gamma_{n_2}(p) = -1$. Since $\gamma_n(DD') = \gamma_n(D)\gamma_n(D')$. we have

$$\begin{aligned}(5.3)\quad &\sum_{D|d}(-1)^{\omega(D)}a_n\left(f^{(D)}\right)\\ &= a_{n_1}(f)\left(\sum_{\substack{D|d\\ p\nmid D}}(-1)^{\omega(D)}a_{n_2}(f^{(D)}) + \sum_{\substack{D|d\\ p|D}}(-1)^{\omega(D)-1}a_{n_2}(f^{(D/p)})\right)\\ &= 2a_{n_1}(f)\sum_{D|(d/p)}a_{n_2}\left(f^{(D)}\right).\end{aligned}$$

Without loss of generality, assume that t is an integer such that $0 \le t \le m$ and for $i \le t$ we have $\gamma_{n_2}(p_i) = -1$, and for $i > t$ we have $\gamma_{n_2}(p_i) = 1$. Denote by $d_1 = p_1 \cdots p_t$, then applying equation (5.3) recursively, if $0 \le t < m$ we have that

$$\begin{aligned}\sum_{D|d}(-1)^{\omega(D)}a_n\left(f^{(D)}\right) &= 2^t a_{n_1}(f)\sum_{D|(d/d_1)}a_{n_2}(f^{(D)})\\ &= 2^t a_n(f)\sum_{D|(d/d_1)}(-1)^{\omega(D)} = 0.\end{aligned}$$

Meanwhile if $t = m$, we obtain that $a_n(\sum_{D|d}(-1)^{\omega(D)}f^{(D)}) = 2^m a_n(f)$.

Finally, if $\gamma_{n_2}(p) = -1$ for all $p \mid d$, we have that $\gamma_{q_i}(p)^{\alpha_i} = -1$ for some $1 \le i \le s$, in particular, α_i is odd, then in view of Lemma 5.2 we obtain that $a_n(f)$ is even. Even better, if $\omega(d)$ is odd, $\gamma_{n_2}(d) = -1$, then there exists $1 \le i \le s$, such that $\gamma_{q_i}(d)^{\alpha_i} = -1$, therefore α_i is odd and $\left(\frac{d}{q_i}\right) = \gamma_{q_i}(d) = -1$. Applying Lemma 5.2 we obtain that $4 \mid a_n(f)$, so

$$\sum_{D|d}(-1)^{\omega(D)}a_n\left(f^{(D)}\right) \equiv 0 \pmod{2^{m+\epsilon}},$$

which proves the desired result. □

Proof of Corollary 1.5. By Remark 2.6 $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \le 2$ when E is equal to $y^2 = x^3 - px$ or $y^2 = x^3 - p^3x$ for p a prime number. Each of these elliptic curve is the quadratic twist by p of the other, whose conductor is 2^5p^2 if $p \equiv 1 \pmod 4$ or 2^6p^2 if $p \equiv -1 \pmod 4$ (see [13, Table I]).

Furthermore, Theorem 1.4 says that $3 \le \nu_2(\delta_E)$ in both cases, which yields the desired result. □

Let us remark that the lower bound for the 2-adic valuation of the congruence number by Theorem 1.4 exceeds half of the upper bound for the Mordell–Weil rank $2\omega(d) - \delta_2(d)$, as noted in Remark 2.6.

Using data from the LMFDB [17] for $d = 21$ and $n \leq 100$, we have $\sum_{D|d}(-1)^{\omega(D)}a_n(f^{(D)}) \equiv 16 \pmod{32}$. On the other hand, Theorem 1.4 implies $\delta(E) \geq 3$ in this scenario. This observation suggests that the actual congruence between f and h may not manifest at as high a power of 2 as predicted by this theorem.

Acknowledgments

I would like to thank Hector Pasten for suggesting this problem to me, carefully reading the preliminary version of this manuscript and numerous helpful remarks. I thank the anonymous referees for several valuable comments on an earlier version of this manuscript. This paper is based on my thesis, thus, I am very grateful to my examiners Ricardo Menares and Fabien Pazuki for several suggestions which have improved the present work.

References

[1] A. ABBES & E. ULLMO, "A propos de la conjecture de Manin pour les courbes elliptiques modulaires", *Compos. Math.* **103** (1996), no. 3, p. 269-286.

[2] A. AGASHE, K. A. RIBET & W. A. STEIN, "The modular degree, congruence primes, and multiplicity one", in *Number theory, analysis and geometry. In memory of Serge Lang*, Springer, 2012, p. 19-49.

[3] J. AGUIRRE, Á. LOZANO-ROBLEDO & J. C. PERAL, "Elliptic curves of maximal rank", in *Proceedings of the "Segundas Jornadas de Teoría de Números", Madrid, Spain, July 16–19, 2007*, Biblioteca de la Revista Matemática Iberoamericana, Revista Matemática Iberoamericana, 2008, p. 1-28.

[4] C. BREUIL, B. CONRAD, F. DIAMOND & R. TAYLOR, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Am. Math. Soc.* **14** (2001), no. 4, p. 843-939.

[5] F. CALEGARI & M. EMERTON, "Elliptic curves of odd modular degree", *Isr. J. Math.* **169** (2009), no. 1, p. 417-444.

[6] J. CARO & H. PASTEN, "Watkins's conjecture for elliptic curves with non-split multiplicative reduction", *Proc. Am. Math. Soc.* **150** (2022), no. 8, p. 3245-3251.

[7] A. C. COJOCARU & E. KANI, "The modular degree and the congruence number of a weight 2 cusp form", *Acta Arith.* **114** (2004), no. 2, p. 159-167.

[8] J. CREMONA & A. PACETTI, "On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1", *Proc. Lond. Math. Soc. (3)* **118** (2019), no. 5, p. 1245-1276.

[9] C. DELAUNAY, "Computing modular degrees using L-functions", *J. Théor. Nombres Bordeaux* **15** (2003), no. 3, p. 673-682.

[10] B. EDIXHOVEN, "On the Manin constants of modular elliptic curves", in *Arithmetic algebraic geometry*, Progress in Mathematics, vol. 89, Birkhäuser, 1991, p. 25-39.

[11] J. A. ESPARZA-LOZANO & H. PASTEN, "A conjecture of Watkins for quadratic twists", *Proc. Am. Math. Soc.* **149** (2021), no. 6, p. 2381-2385.

[12] G. FREY, "Links between solutions of $A - B = C$ and elliptic curves", in *Number theory. Proceedings of the 15th journées arithmétiques held in Ulm, FRG, September 14-18, 1987*, Lecture Notes in Mathematics, vol. 1380, Springer, 1989, p. 31-62.

[13] T. HADANO, "Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor", *Proc. Japan Acad.* **51** (1975), no. 2, p. 92-95.

[14] M. KAZALICKI & D. KOHEN, "On a special case of Watkins' conjecture", *Proc. Am. Math. Soc.* **146** (2018), no. 2, p. 541-545.

[15] ———, "Corrigendum to: "On a special case of Watkins' conjecture"", *Proc. Am. Math. Soc.* **147** (2019), no. 10, p. 4563.
[16] N. I. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97, Springer, 2012, x+248 pages.
[17] The LMFDB Collaboration, "The L-functions and Modular Forms Database", 2021, `https://www.lmfdb.org`.
[18] B. Mazur & D. Goldfed, "Rational isogenies of prime degree", *Invent. Math.* **44** (1978), p. 129-162.
[19] J.-F. Mestre & J. Oesterlé, "Courbes de Weil semi-stables de discriminant une puissance m-ième", *J. Reine Angew. Math.* **400** (1989), p. 173-184.
[20] J. T. Mulholland, "Elliptic curves with rational 2-torsion and related ternary Diophantine equations", PhD Thesis, University of British Columbia, Canada, 2006.
[21] V. Pal, "Periods of quadratic twists of elliptic curves", *Proc. Am. Math. Soc.* **140** (2012), no. 5, p. 1513-1525.
[22] V. V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics, vol. 11, Springer, 2004, xiv+301 pages.
[23] B. Setzer, "Elliptic curves of prime conductor", *J. Lond. Math. Soc. (2)* **10** (1975), p. 367-378.
[24] G. Shimura, "The special values of the zeta functions associated with cusp forms", *Commun. Pure Appl. Math.* **29** (1976), p. 783-804.
[25] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Studies in Mathematics, vol. 151, Springer, 1994, xiii+525 pages.
[26] ———, *The arithmetic of elliptic curves*, 2nd ed., Graduate Studies in Mathematics, vol. 106, Springer, 2009, xx+513 pages.
[27] R. Taylor & A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. Math. (2)* **141** (1995), no. 3, p. 553-572.
[28] M. Watkins, "Computing the modular degree of an elliptic curve", *Exp. Math.* **11** (2002), no. 4, p. 487-502.
[29] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. Math. (2)* **141** (1995), no. 3, p. 443-551.
[30] S. Yazdani, "Modular abelian varieties of odd modular degree", *Algebra Number Theory* **5** (2011), no. 1, p. 37-62.

Jerson Caro
Department of Mathematics & Statistics, Boston University
665 Commonwealth Avenue
Boston, MA 02215, USA
E-mail: `jlcaro@bu.edu`
URL: `https://sites.google.com/view/jerson-caro/about-me`