WATKINS'S CONJECTURE FOR ELLIPTIC CURVES WITH NON-SPLIT MULTIPLICATIVE REDUCTION

JERSON CARO AND HECTOR PASTEN

ABSTRACT. Let E be an elliptic curve over the rational numbers. In 2002, Watkins conjectured that the rank of E is bounded by the 2-adic valuation of the modular degree of E. We prove this conjecture for semistable elliptic curves having exactly one rational point of order 2, provided that they have an odd number of primes of non-split multiplicative reduction or no primes of split multiplicative reduction.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. By the modularity theorem [4, 23, 25] there is a modular parametrization $\phi : X_0(N) \to E$ over $\mathbb{Q}$ which we assume to be of minimal degree. The *modular degree* of E is $m_E = \deg(\phi)$. This number is linked to important arithmetic questions such as the *abc* conjecture [10, 16] and congruences of modular forms [27, 6, 1]. Watkins conjectured:

Conjecture 1.1 (Watkins, see [24])**.** *We have that* 2^r *divides* m_E*, where* $r = \operatorname{rk} E(\mathbb{Q})$*.*

Progress on this conjecture has been difficult. Conditional evidence is provided in [7]. The case of odd m_E (which amounts to showing $\operatorname{rk} E(\mathbb{Q}) = 0$) is addressed in [22, 5, 12, 13, 26]. Also, in [9] it is shown that if $E(\mathbb{Q})[2] \neq (0)$, then Watkins's conjecture holds for all quadratic twists of E by a squarefree integer d with sufficiently many prime factors. To these results we add:

Theorem 1.2 (Main Result)**.** *Let* E *be a semistable elliptic curve over* $\mathbb{Q}$ *with* $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$*. If the number of primes of non-split multiplicative reduction for* E *is odd, or if there is no prime of split multiplicative reduction, then Watkins's conjecture holds for* E*.*

On the way, we also prove the following rank bound which seems to be missing in the literature:

Proposition 1.3 (Rank bound)**.** *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})[2] \neq (0)$*. Let* α *and* μ *be the number of primes of additive and multiplicative reduction of* E *respectively. Then*

$$\operatorname{rk} E(\mathbb{Q}) \leq 2\alpha + \mu - 1.$$

A similar bound is obtained in [2], but the notion of additive and multiplicative reduction in *loc.cit.* is with respect to a choice of Weierstrass equation of the form $y^2 = x^3 + Ax^2 + Bx$.

Let $v_2(n)$ be the 2-adic valuation of an integer n. The proof of Theorem 1.2 confronts the previous upper bound for the rank with a lower bound for $v_2(m_E)$ coming from Atkin-Lehner involutions. The bounds, however, do not match and additional work is needed. A crucial step in our argument will follow from either non-triviality of $\text{Ш}(E)[2]$, or —when it is trivial— known cases of the parity conjecture.

Finally, we mention that there are plenty of examples where Theorem 1.2 applies. Checking in the database LMFDB [14] we find 99 elliptic curves of conductor $N < 500$ which are $\Gamma_0(N)$-optimal

---

Date: November 10, 2021.

2010 *Mathematics Subject Classification.* Primary: 11G05; Secondary: 11G18, 11G40.

Key words and phrases. Watkins's conjecture, modular degree, rank, parity conjecture.

J.C. was supported by ANID Doctorado Nacional 21190304. H.P. was supported by ANID (ex CONICYT) FONDECYT Regular grant 1190442 from Chile.

and for which Theorem 1.2 applies. Some examples are sharp; for instance $65.a1$ has rank 1 and $m_E = 2$, while $185.c1$ has rank 1 and $m_E = 6$. Although all the examples with $N < 500$ have rank 0 or 1, for larger conductor one finds higher rank examples such as $2130.a2$ of rank 2, and $84534.a2$ of rank 3.

2. Bounds for 2-isogeny Selmer groups

For an elliptic curve E over $\mathbb{Q}$ with a 2-isogeny $\theta : E \to E'$ defined over $\mathbb{Q}$ and dual isogeny $\theta' : E' \to E$, we let $s(E, \theta) = \dim_{\mathbb{F}_2} \mathrm{Sel}_\theta(E)$ and $s'(E, \theta) = s(E', \theta')$. Here, $\mathrm{Sel}_\theta(E)$ is the 2-isogeny Selmer group. From Section 3.6 of [20] one deduces

$$\mathrm{rk}\, E(\mathbb{Q}) + 2 \leq s(E, \theta) + s'(E, \theta).$$

Let $\omega(n)$ be the number of different prime factors of n. The following result is Lemma 2.1 in [2], keeping track of the contribution of the place $v = 2$ in the relevant Selmer groups.

Lemma 2.1. *Let E be an elliptic curve over $\mathbb{Q}$ admitting a Weierstrass equation*

$$y^2 = x^3 + Ax^2 + Bx, \qquad \text{with } A, B \in \mathbb{Z}.$$

Let $\theta : E \to E'$ be the map obtained by taking the quotient by the 2-torsion point $(0, 0)$. We have

$$s(E, \theta) + s'(E, \theta) \leq \omega(B) + \omega(A^2 - 4B) + 1.$$

Furthermore, let us define the affine curves

$$C^{(1)} : \quad 2W^2 = 4U^4 - 4AU^2 + (A^2 - 4B)$$
$$C^{(2)} : \quad 2W^2 = 4U^4 + 2AU^2 + B.$$

Suppose that A is even and $C^{(1)}(\mathbb{Q}_2) = \emptyset$, or that B is even and $C^{(2)}(\mathbb{Q}_2) = \emptyset$. Then

$$s(E, \theta) + s'(E, \theta) \leq \omega(B) + \omega(A^2 - 4B).$$

The last assertion is not explicitly made in the statement of Lemma 2.1 [2], but it follows from its proof, by noticing that $C^{(1)}$ and $C^{(2)}$ are affine open sets of the homogeneous spaces C_2 and C'_2 in the notation of *loc. cit.* Basically, the last assertion says that if the appropriate homogeneous spaces have no $\mathbb{Q}_2$-points, then we get an additional constraint on the corresponding Selmer groups. See also Section X.4 in [21]. Using this, we prove

Theorem 2.2. *Let E be an elliptic curve over $\mathbb{Q}$ admitting a 2-isogeny $\theta : E \to E'$ over $\mathbb{Q}$. Let α and μ be the number of places of additive and of multiplicative reduction of E respectively. Then $s(E, \theta) + s'(E, \theta) \leq 2\alpha + \mu + 1$. In particular, $\mathrm{rk}\, E(\mathbb{Q}) \leq 2\alpha + \mu - 1$.*

Proof. Consider a minimal Weierstrass equation for E over $\mathbb{Z}$ of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{2.1}$$

The change of variables $X = z/4$, $Y = y/8 - a_1z/8 - a_3/2$ transforms (2.1) into

$$y^2 = z^3 + b_2z^2 + 8b_4z + 16b_6 \tag{2.2}$$

where

$$b_2 = 4a_2 + a_1^2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = 4a_6 + a_3^2.$$

Let $\gamma \in \mathbb{Q}$ be a root of the previous cubic associated to the rational 2-torsion point in $\ker(\theta)$. Then $\gamma \in \mathbb{Z}$ and the change of variables $z = x + \gamma$ turns (2.2) into

$$y^2 = x^3 + Ax^2 + Bx \tag{2.3}$$

where

$$A = 3\gamma + b_2 \quad \text{and} \quad B = 3\gamma^2 + 2b_2\gamma + 8b_4. \tag{2.4}$$

Let $\Delta^{\min}$ be the discriminant of the minimal model (2.1) and let Δ be the discriminant of the model (2.2). We note that (2.3) has the same discriminant Δ. Then $\Delta = 2^{12}\Delta^{\min}$ by the standard transformation formulas and $\Delta = 16B^2(A^2 - 4B)$ by (2.3). In particular, the models (2.2) and (2.3) are minimal at each $p > 2$. This implies that for $p > 2$ we have that p divides neither, one, or both of B and $A^2 - 4B$ if and only if E has good, multiplicative, or additive reduction at p respectively. Hence, the following bounds hold when E has bad reduction at $p = 2$:

- If E has additive reduction at $p = 2$ then $\omega(B) + \omega(A^2 - 4B) \leq \mu + 2\alpha$.
- If E has multiplicative reduction at $p = 2$, then b_2 is odd (cf. Notation (3.1) Ch. 3 and Remark (7.2) Ch. 5 in [11]). Thus, by (2.4) we see that A and B have opposite parity. This gives $\omega(B) + \omega(A^2 - 4B) = \mu + 2\alpha$.

On the other hand, when E has good reduction at $p = 2$, then a_1 or a_3 in (2.1) is odd, for otherwise one directly checks that $(X, Y) = (a_4, a_4 + a_2a_4 + a_4 + a_6)$ is a singular point. By considerations on Newton polygons as in Section 2 of [19], the fact that the cubic in (2.2) is reducible (γ is a root) shows that a_1 is odd; for otherwise a_1 is even and a_3 is odd, giving that the Newton polygon of the right hand side of (2.2) is the segment joining $(0, 4)$ and $(3, 0)$ which has no other integer points, and Dumas's irreducibility criterion (cf. the Corollary in p.55 of [17]) would give that the the right hand side of (2.2) is irreducible.

Hence, when E has good reduction at $p = 2$ we have that $b_2 \equiv 1 \bmod 4$. Thus, (2.4) implies that A and B have opposite parity, which gives $\omega(B) + \omega(A^2 - 4B) = \mu + 2\alpha + 1$.

In order to conclude, let us apply Lemma 2.1 to (2.3). The only remaining point is to show that in the case of good reduction at $p = 2$ the additional requirement on the curves $C^{(i)}$ is satisfied. For this, from now on we assume good reduction at $p = 2$; in particular $b_2 \equiv 1 \bmod 4$.

Note that γ is odd or divisible by 4, for otherwise we could write $\gamma = 2\delta$ with δ odd, then (2.2) would imply $0 = 2\delta^3 + b_2\delta^2 + 4b_4\delta + 4b_6$ which is impossible as b_2 is odd.

If γ is odd, then A is even and B is odd. Since $v_2(B^2(A^2 - 4B)) = v_2(2^8\Delta^{\min}) = 8$ we deduce

$$A \equiv 2 \bmod 4,\ B \equiv 1 \bmod 8 \text{ and } A^2 - 4B \equiv 0 \bmod 256. \tag{2.5}$$

If $4|\gamma$ then (2.4) shows that A is odd and B even. Hence, $2v_2(B) = v_2(B^2(A^2 - 4B)) = 8$. Furthermore, we recall that $b_2 \equiv 1 \bmod 4$ and $A = 3\gamma + b_2$. Hence

$$A \equiv 1 \bmod 4 \text{ and } v_2(B) = 4. \tag{2.6}$$

Let us now analyze the $\mathbb{Q}_2$-points of the curves $C^{(1)}$ and $C^{(2)}$.

First, if A is odd and B is even (i.e. $4|\gamma$), let us show that $C^{(2)}(\mathbb{Q}_2)$ is empty. For the sake of contradiction, assume that $C^{(2)}(\mathbb{Q}_2) \neq \emptyset$. That implies that there are $u, w \in \mathbb{Q}_2$ such that

$$2w^2 = 4u^4 + 2Au^2 + 16k, \tag{2.7}$$

where $B = 16k$ with k odd (cf. (2.6)). Notice that $v_2(4u^4) = 4v_2(u) + 2$, $v_2(2Au^2) = 2v_2(u) + 1$ and $v_2(16k) = 4$, in particular, all of these valuations are different. Consequently, we have that

$$2v_2(w) + 1 = v_2(2w^2) = \min\{4v_2(u) + 2, 2v_2(u) + 1, 4\}.$$

Since $2v_2(w) + 1$ is odd, we get $2v_2(w) + 1 = 2v_2(u) + 1$. That shows not only that $v_2(w) = v_2(u)$, but also that $2v_2(u) + 1 < \min\{4v_2(u) + 2, 4\}$, which implies that $v_2(u) \in \{0, 1\}$. Then:

- If $v_2(w) = v_2(u) = 0$, since 1 is the only invertible square modulo 8, from (2.7) we get $2A \equiv 2w^2 - 4u^4 \equiv 6 \bmod 8\mathbb{Z}_2$, which is not possible by (2.6).
- If $v_2(w) = v_2(u) = 1$, then there exist $s, t \in \mathbb{Z}_2^\times$ such that $w = 2s$ and $u = 2t$. Then equation (2.7) yields $s^2 = 8t^4 + At^2 + 2k$. Since k is odd and $A \equiv 1 \bmod 4$, we deduce $1 \equiv 1 + 2 \bmod 4\mathbb{Z}_2$; a contradiction.

Finally, if A is even and B is odd (i.e. γ is odd), we have to show that $C^{(1)}(\mathbb{Q}_2)$ is empty. The standard equation for E' is $Y^2 = X^3 - 2AX^2 + (A^2 - 4B)X$ which, upon the substitution $X = 4x$,

$Y = 8y$, becomes $y^2 = x^3 - Ax^2/2 + (A^2 - 4B)x/16$. Since E' has good reduction at $p = 2$ (it is isogenous to E) by (2.5) we see that the same analysis of the case $4|\gamma$ for E applies to the last equation for E'. This shows that the curve $C'^{(2)} : 2W^2 = 4U^4 - AU^2 + (A^2 - 4B)/16$ (which is the analogue of $C^{(2)}$ for E') has no $\mathbb{Q}_2$-points. The change of variables $W = w/4$, $U = u/2$ transforms the equation for $C'^{(2)}$ into the equation for $C^{(1)}$, hence $C^{(1)}(\mathbb{Q}_2) = \emptyset$. □

3. Watkins's conjecture

From now on we let E be a semistable elliptic curve over $\mathbb{Q}$; so, N is squarefree and $\mu = \omega(N)$. Let $f \in S_2(\Gamma_0(N))$ be its associated newform. Let $\mathrm{Sel}_2(E)$ be the 2-Selmer group of E.

Lemma 3.1. *Assume $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. Then we have $\mathrm{rk}\, E(\mathbb{Q}) \leq \mu - 1$. If equality holds, then $Ш(E)[2] = (0)$.*

Proof. Theorem 2.2 we have $\mathrm{rk}\, E(\mathbb{Q}) \leq \mu - 1$, thus, $\dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) \leq \mu$. By the exact sequence

$$(0) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to Ш(E)[2] \to (0),$$

it suffices to prove $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \leq \mu$. Let $\theta : E \to E'$ be the 2-isogeny with kernel $E(\mathbb{Q})[2]$ and let $\theta' : E' \to E$ be its dual. Consider the exact sequence from Lemma 6.1 of [18]:

$$(0) \to E'(\mathbb{Q})[\theta']/\theta(E(\mathbb{Q})[2]) \to \mathrm{Sel}_\theta(E) \to \mathrm{Sel}_2(E) \to \mathrm{Sel}_{\theta'}(E').$$

The assumption $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ gives that $\theta(E(\mathbb{Q})[2]) = (0)$ and that 2 divides $\#E'(\mathbb{Q})[\theta']$. From this we deduce $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \leq s(E, \theta) + s'(E, \theta) - 1$. We conclude by Theorem 2.2. □

For each $d|N$ there is the Atkin-Lehner involution W_d on $X_0(N)$. They form a group $W \simeq (\mathbb{Z}/2\mathbb{Z})^\mu$. For every $d|N$ we have $W_d(f) = \pm f$. Let $w_d(f) \in \{-1, 1\}$ be defined by $W_d(f) = w_d(f) \cdot f$. These eigenvalues satisfy $\prod_{p|N} w_p(f) = w_N(f) = -\epsilon(f)$ where $\epsilon(f)$ is the sign of the functional equation of $L(f, s)$. In [3] it is shown that $-w_p(f) = a_p(f)$, the p-th Fourier coefficient of f. Thus:

$$w_p(f) = \begin{cases} 1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has split multiplicative reduction at } p. \end{cases}$$

The rule $W_d \mapsto w_d$ defines a morphism $\rho : W \to \{-1, 1\}$. Let $W' = \ker(\rho)$. A morphism $W' \to E(\mathbb{Q})[2]$ is constructed in [8] with kernel denoted by W''. They prove that $\#W''$ divides m_E and that $\dim_{\mathbb{F}_2} W'' \geq \mu - \dim_{\mathbb{F}_2}(W/W') - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2]$. We get:

Lemma 3.2. *Assume $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. If $w_p = 1$ for all $p|N$, then $v_2(m_E) \geq \mu - 1$. On the other hand, if $w_p = -1$ for some $p|N$, then $v_2(m_E) \geq \mu - 2$.*

With these lemmas at hand, we can prove Theorem 1.2.

Proof of Theorem 1.2. Let us assume that E is a semistable elliptic curve of conductor N and modular degree m_E, with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$.

If E has no place of split multiplicative reduction, then the first part of Lemma 3.2 gives $v_2(m_E) \geq \mu - 1$, while Lemma 3.1 gives $\mathrm{rk}\,(E) \leq \mu - 1$.

So, we may assume that E has an odd number of places of non-split multiplicative reduction. By the second part of Lemma 3.2 it suffices to show $\mathrm{rk}\,(E) \leq \mu - 2$. If $Ш(E)[2]$ is non-trivial then Lemma 3.1 gives $\mathrm{rk}\,(E) \leq \mu - 2$ and we are done. So, let us assume that $Ш(E)[2]$ is trivial. Then $Ш(E)[2^\infty] = (0)$ and by results of Monsky [15] the parity conjecture holds for E: we get $\epsilon(f) = (-1)^{\mathrm{rk}\, E(\mathbb{Q})}$.

Write $N = N^+ N^-$ where N^+ is the product of the primes of split multiplicative reduction for E and N^- is the product for non-split multiplicative reduction. Then $\omega(N^+)$ and $\mu = \omega(N^+) + \omega(N^-)$ have opposite parity, while $\epsilon(f)$ and $(-1)^{\omega(N^+)} = \prod_{p|N} w_p(f)$ have opposite sign. This means that rk (E) and μ have the same parity. Therefore, the bound rk $(E) \leq \mu - 1$ from Lemma 3.1 is strict and we get rk $(E) \leq \mu - 2$. □

4. Acknowledgments

The first author was supported by ANID Doctorado Nacional 21190304. The second author was supported by ANID (ex CONICYT) FONDECYT Regular grant 1190442 from Chile.

We sincerely thank the referee for carefully reading the manuscript and for several suggestions that improved the presentation.

References

[1] A. Agashe, K. Ribet, W. Stein, *The modular degree, congruence primes, and multiplicity one.* Number theory, analysis and geometry, 19-49, Springer, New York, 2012.

[2] J. Aguirre, A. Lozano-Robledo, J. Peral, *Elliptic curves of maximal rank.* Proceedings of the "Segundas Jornadas de Teoría de Números", 1-28, Bibl. Rev. Mat. Iberoamericana, Rev. Mat. Iberoamericana, Madrid, 2008.

[3] A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Math. Ann. 185 (1970), 134-160.

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

[5] F. Calegari, M. Emerton, *Elliptic curves of odd modular degree.* Israel J. Math. 169 (2009), 417-444.

[6] A. Cojocaru, E. Kani, *The modular degree and the congruence number of a weight 2 cusp form.* Acta Arith. 114 (2004), no. 2, 159-167.

[7] N. Dummigan, *On a conjecture of Watkins.* J. Théor. Nombres Bordeaux 18 (2006), no. 2, 345-355.

[8] N. Dummigan, S. Krishnamoorthy, *Powers of 2 in modular degrees of modular abelian varieties.* J. Number Theory 133 (2013), no. 2, 501-522.

[9] J. Esparza-Lozano, H. Pasten, *A conjecture of Watkins for quadratic twists.* Proc. Amer. Math. Soc. 149 (2021), no. 6, 2381-2385.

[10] G. Frey, *Links between solutions of A-B=C and elliptic curves.* Number theory (Ulm, 1987), 31-62, Lecture Notes in Math., 1380, Springer, New York, 1989.

[11] D. Husemoller, *Elliptic curves.* Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics, 111. Springer-Verlag, New York, 2004. xxii+487 pp.

[12] M. Kazalicki, D. Kohen, *On a special case of Watkins' conjecture.* Proc. Amer. Math. Soc. 146 (2018), no. 2, 541-545.

[13] M. Kazalicki, D. Kohen, *Corrigendum to "On a special case of Watkins' conjecture".* Proc. Amer. Math. Soc. 147 (2019), no. 10, 4563.

[14] The LMFDB Collaboration, *The L-functions and Modular Forms Database.* (2021) `www.lmfdb.org`

[15] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves.* Math. Z. 221 (1996), no. 3, 415-420.

[16] R. Murty, *Bounds for congruence primes.* Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 177-192, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, 1999.

[17] V. Prasolov, *Polynomials.* Translated from the 2001 Russian second edition by Dimitry Leites. Algorithms and Computation in Mathematics, 11. Springer-Verlag, Berlin, 2004. xiv+301 pp.

[18] E. Schaefer, M. Stoll, *How to do a p-descent on an elliptic curve.* Trans. Amer. Math. Soc. 356 (2004), no. 3, 1209-1231.

[19] B. Setzer, *Elliptic curves of prime conductor.* J. London Math. Soc. (2) 10 (1975), 367-378.

[20] J. Silverman, J. Tate, *Rational points on elliptic curves.* Second edition. Undergraduate Texts in Mathematics. Springer, Cham, 2015. xxii+332 pp. ISBN: 978-3-319-18587-3; 978-3-319-18588-0.

[21] J. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9

[22] W. Stein, M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves.* Int. Math. Res. Not. 2004, no. 27, 1395-1405.

[23] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[24] M. Watkins, *Computing the modular degree of an elliptic curve.* Experiment. Math. 11 (2002), no. 4, 487-502.

[25] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443-551.

[26] S. Yazdani, *Modular abelian varieties of odd modular degree.* Algebra Number Theory 5 (2011), no. 1, 37-62.

[27] D. Zagier, *Modular parametrizations of elliptic curves.* Canad. Math. Bull. 28 (1985), no. 3, 372-384.

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Email address, J. Caro: jocaro@uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Email address, H. Pasten: hpasten@gmail.com