RESEARCH

Supersingular zeros of divisor polynomials of elliptic curves of prime conductor

Matija Kazalicki[1*] and Daniel Kohen[2,3]

*Correspondence: matija.kazalicki@math.hr
[1]Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Full list of author information is available at the end of the article

Abstract

For a prime number p we study the zeros modulo p of divisor polynomials of rational elliptic curves E of conductor p. Ono [8, p. 118] made the observation that these zeros of are often j-invariants of supersingular elliptic curves over $\overline{\mathbb{F}_p}$. We show that these supersingular zeros are in bijection with zeros modulo p of an associated quaternionic modular form v_E.

This allows us to prove that if the root number of E is -1 then all supersingular j-invariants of elliptic curves defined over $\mathbb{F}_p$ are zeros of the corresponding divisor polynomial.

If the root number is 1 we study the discrepancy between rank 0 and higher rank elliptic curves, as in the latter case the amount of supersingular zeros in $\mathbb{F}_p$ seems to be larger. In order to partially explain this phenomenon, we conjecture that when E has positive rank the values of the coefficients of v_E corresponding to supersingular elliptic curves defined over $\mathbb{F}_p$ are even. We prove this conjecture in the case when the discriminant of E is positive, and obtain several other results that are of independent interest.

Keywords: divisor polynomial; supersingular elliptic curves; Brandt module

1 Introduction

Let E be a rational elliptic curve of prime conductor p. Denote by $f_E(\tau) \in S_2(\Gamma_0(p))$ the newform associated to E by the Shimura-Taniyama correspondence. Serre [11, Theorem 11] showed that there is an isomorphism between modular forms modulo p of weight $p+1$ and level 1 and modular forms modulo p of weight 2 and level p. More precisely he proved that $f_E(\tau) \equiv F_E(\tau) \pmod{p}$, where

$$F_E(\tau) = \mathrm{Trace}^{\Gamma_0(p)}_{\mathrm{SL}_2(\mathbb{Z})} \left(f_E(\tau) \cdot (E_{p-1}(\tau) - p^{p-1} E_{p-1}(p\tau)) \right) \in S_{p+1}(\mathrm{SL}_2(\mathbb{Z})),$$

and $E_{p-1}(\tau)$ is the normalized Eisenstein series of weight $p-1$.

Given $k \in \mathbb{Z}$ define

$$\tilde{E}_k(\tau) = \begin{cases} 1 & if \quad k \equiv 0 \bmod 12, \\ E_4(\tau)^2 E_6(\tau) & if \quad k \equiv 2 \bmod 12, \\ E_4(\tau) & if \quad k \equiv 4 \bmod 12, \\ E_6(\tau) & if \quad k \equiv 6 \bmod 12, \\ E_4(\tau)^2 & if \quad k \equiv 8 \bmod 12, \\ E_4(\tau)E_6(\tau) & if \quad k \equiv 10 \bmod 12, \end{cases}$$

where $E_4(\tau)$ and $E_6(\tau)$ are the classical Eisenstein series of weight 4 and 6 respectively.

Moreover, consider

$$m(k) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & if \quad k \not\equiv 2 \bmod 12, \\ \left\lfloor \frac{k}{12} \right\rfloor - 1 & if \quad k \equiv 2 \bmod 12. \end{cases}$$

Given any $g \in M_k(SL_2(\mathbb{Z}))$ we obtain a polynomial $\tilde{F}(g, x)$ (see [8, p. 32]) which is characterized by the formula

$$\frac{g(\tau)}{\Delta(\tau)^{m(k)}\tilde{E}_k(\tau)} = \tilde{F}(g, j(\tau)),$$

where Δ is the only weight 12 and level 1 cuspform and j is the classical j-invariant. The divisor of $\tilde{E}_k(\tau)$ is captured by the polynomial

$$h_k(x) = \begin{cases} 1 & if \quad k \equiv 0 \bmod 12, \\ x^2(x - 1728) & if \quad k \equiv 2 \bmod 12, \\ x & if \quad k \equiv 4 \bmod 12, \\ x - 1728 & if \quad k \equiv 6 \bmod 12, \\ x^2 & if \quad k \equiv 8 \bmod 12, \\ x(x - 1728) & if \quad k \equiv 10 \bmod 12. \end{cases}$$

The *divisor polynomial* is

$$F(g,x) = h_k(x)\tilde{F}(g,x).$$

Ono [8, p. 118] made the observation that the zeros of $F(F_E,x) \bmod p \in \mathbb{F}_p[x]$ (in $\overline{\mathbb{F}_p}$) are often supersingular j-invariants (i.e. j-invariants of supersingular elliptic curves over $\overline{\mathbb{F}_p}$), and asked for an explanation for this.

For example, if E_{83} is the elliptic curve of conductor 83 given by

$$E_{83}: \quad y^2 + xy + y = x^3 + x^2 + x,$$

then

$$\begin{aligned} F_{E_{83}}(\tau) \equiv{}& \Delta(\tau)E_4(\tau)^{18} + 19\Delta(\tau)^2E_4(\tau)^{15} + 21\Delta(\tau)^3E_4(\tau)^{12} \\ &+ 58\Delta(\tau)^4E_4(\tau)^9 + 21\Delta(\tau)^5E_4(\tau)^6 + 60\Delta(\tau)^6E_4(\tau)^3 \pmod{83}. \end{aligned}$$

Since $j(\tau) = E_4(\tau)^3/\Delta(\tau)$, it follows that

$$F(F_{E_{83}},x) \equiv x(x+15)(x+16)(x+33)(x+55)(x+66) \pmod{83}.$$

In this case, the roots of $F(F_{E_{83}},x)$ in $\overline{\mathbb{F}}_{83}$ are precisely the supersingular j-invariants that lie in $\mathbb{F}_{83}$.

It is worth noting that the root number of E_{83} is -1. The behavior of the roots of the divisor polynomial is explained by the following theorem.

Theorem 1 *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p with root number -1, and let $F(F_E,x)$ be the corresponding divisor polynomial. If $j \in \mathbb{F}_p$ is a supersingular j-invariant mod p, then $F(F_E,j) \equiv 0 \pmod{p}$.*

If the root number of E is 1, the supersingular zeros of divisor polynomials are harder to understand. Denote by s_p the number of isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$. Eichler proved that

$$s_p = \begin{cases} \frac{1}{2}h(-p) & \text{if } p \equiv 1 \pmod 4, \\ 2h(-p) & \text{if } p \equiv 3 \pmod 8, \\ h(-p) & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. See [4] for an excellent exposition of Eichler's work.

Denote by $N_p(E)$ the number of $\mathbb{F}_p$-supersingular zeros of the divisor polynomial $F(F_E,x)$, i.e.

$$N_p = \#\{j : j \in \mathbb{F}_p, F(F_E,j) \equiv 0 \bmod p \text{ and } j \text{ is supersingular } j\text{-invariant}\}.$$

Figure 1 shows the graph of the function $\frac{N_p(E)}{s_p}$ where E ranges over all elliptic curves of root number 1 and conductor p where $p < 10000$. The elliptic curves of rank zero (158 of them) are colored in blue, while the elliptic curves of rank two (59 of them) are colored in red.

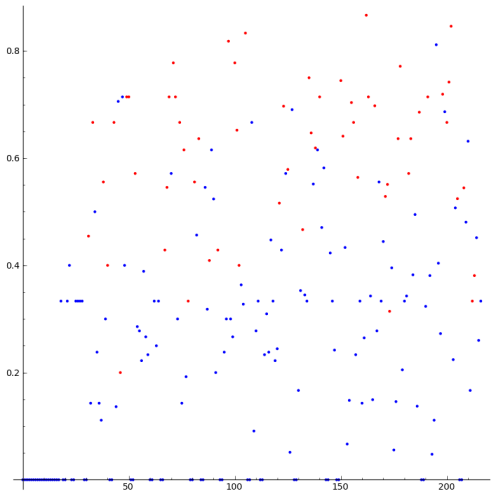

Figure 1 $\frac{N_p}{s_p}$ for $p < 10000$.

It would be interesting to understand this data. In particular,

Questions

1. Why are there "so many" $\mathbb{F}_p$-supersingular zeros?
2. How can we explain the difference between rank 0 and rank 2 curves?
3. What about the outlying rank 0 curves (e.g. of conductor $p = 4283$ and $p = 5303$) with the "large" number of zeros?

Remark It seems that there is no obvious connection between the number of $\mathbb{F}_{p^2}$-supersingular zeros of the divisor polynomial $F(F_E, x)$ and the rank of elliptic curve E.

The key idea to study these questions is to show (following [13]) how to associate to F_E a modular form v_E on the quaternion algebra B over $\mathbb{Q}$ ramified at p and ∞. Such modular form is a function on the (finite) set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$. In order to explain this precisely we combine the expositions from [3] and [4].

Let $X_0(p)$ be the curve over $\operatorname{Spec}\mathbb{Z}$ that is a coarse moduli space for the $\Gamma_0(p)$-moduli problem. The geometric fiber of $X_0(p)$ in characteristic p is the union of two rational curves meeting at $n = g+1$ ordinary double points: $e_1, e_2, \ldots, e_n$ (g is the arithmetic genus of the fibers of $X_0(p)$.) They are in bijective correspondence with the isomorphism classes of supersingular elliptic curves $E_i/\overline{\mathbb{F}_p}$. Denote by $\mathcal{X}$ the free $\mathbb{Z}$-module of divisors supported on the e_i. The action of Hecke correspondences on the set of e_i induces an action on $\mathcal{X}$. Explicitly, the action of the correspondence

t_m ($m \geq 1$) is given by the transpose of the Brandt matrix $B(m)$

$$t_m e_i = \sum_{j=1}^{n} B_{ij}(m) e_j.$$

There is a correspondence between newforms of level p and weight 2 and modular forms for the quaternion algebra B that preserves the action of the Hecke operators. Let $v_E = \sum v_E(e_i)e_i \in \mathcal{X}$ be an eigenvector for all t_m corresponding to f_E, i.e. $t_m v_E = \lambda_m v_E$, where $f_E(\tau) = \sum_{m=1}^{\infty} \lambda_m q^m$. We normalize v_E (up to the sign) such that the greatest common divisor of all its entries is 1. We are now able to state the following crucial theorem.

Theorem 2 *Let $j = j(E_i)$ be the j-invariant of the supersingular elliptic curve E_i. Then*

$$F(F_E, j) \equiv 0 \bmod p \iff v_E(e_i) \equiv 0 \bmod p.$$

This theorem allows us to give a more explicit description of the supersingular zeros of the divisor polynomial. Furthermore it enables us to obtain computational data in a much more efficient manner. The proof of Theorems 1 and 2 will be the main goal of Section 2. In order to prove them we will use both Serre's and Katz's theory of modular forms modulo p and the modular forms introduced in [13].

Now, let D_E be the congruence number of f_E, i.e. the largest integer such that there exists a weight two cusp for on $\Gamma_0(p)$, with integral coefficients, which is orthogonal to f_E with respect to the Petersson inner product and congruent to f_E modulo D_E. The congruence number is closely related to $\deg \phi_{f_E}$, the modular degree of f_E, which is the degree of the minimal parametrization $\phi_{f_E} : X_0(p) \to E'$ of the strong Weil elliptic curve $E'/\mathbb{Q}$ associated to f_E (E' is isogenous to E but they may not be equal). In general, $\deg \phi_{f_E} | D_E$, and if the conductor of E is prime, we have that $\deg \phi_{f_E} = D_E$ (see [1]).

The idea is to relate these concepts to the aforementioned quaternion modular form v_E. Denote by $w_i = \frac{1}{2}\#\mathrm{Aut}(E_i)$. It is known that $w = \prod_i w_i$ is equal to the denominator of $\frac{p-1}{12}$ and $\sum_{i=1}^{n} \frac{1}{w_i} = \frac{p-1}{12}$ (Eichler's mass formula). We define a $\mathbb{Z}$-bilinear pairing

$$\langle -, - \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{Z},$$

by requiring $\langle e_i, e_j \rangle = w_i \delta_{i,j}$ for all $i, j \in \{1, \ldots, n\}$.

We have the following theorem due to Mestre [7, Theorem 3]

Theorem 3 *Using the notation above, we have*

$$\langle v_E, v_E \rangle = t D_E,$$

where t is the size of $E(\mathbb{Q})_{tors}$.

We observe that the modular degree of the elliptic curves under consideration (of rank 0 or 2, conductor p, where $p < 10000$) is "small", which suggests that the integral vector v_E will have many zero entries. This gives a partial answer to Question 1. Zagier [15, Theorem 5] proved that if we consider elliptic curves with bounded j-invariants we have

$$\deg \phi_{f_E} << p^{7/6} \log(p)^3.$$

On the other hand, Watkins [14, Theorem 5.1] showed that

$$\deg \phi_{f_E} >> p^{7/6} / \log(p).$$

To address Questions 2 and 3 we focus on the mod 2 behavior of v_E. Based on the numerical evidence we pose the following conjecture.

Conjecture 1 *If E is an elliptic curve of prime conductor p, root number 1, and $rank(E) > 0$, then $v_E(e_i)$ is an even number for all e_i with $j(E_i) \in \mathbb{F}_p$*

While this is true for all 59 rank 2 curves we observed, it holds for 35 out of 158 rank 0 curves. This explains in a way a difference in the number of $\mathbb{F}_p$-supersingular zeros between rank 0 and rank 2 curves (Question 2), since, heuristically, it seems more likely for a number to be zero if we know it is even (especially in light of Theorem 3 which suggests that the numbers $v_E(e_i)$ are small.)

The thirty two out of thirty five elliptic curves of rank 0 for which the conclusion of Conjecture 1 holds (the remaining three curves have conductors $p = 571, 6451$ and 8747) are distinguished from the other rank 0 curves by the fact that their set of real points $E(\mathbb{R})$ is not connected (i.e. E has positive discriminant). In general, we have the following theorem, which will be the subject of Section 3.

Theorem 4 *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p such that*

1. *E has positive discriminant*
2. *E has no rational point of order 2,*

then $v_E(e_i)$ is an even number for all e_i with $j(E_i) \in \mathbb{F}_p$.

Note that this gives a partial answer to Question 3 since, for example, all outlying elliptic curves of rank 0 for which $\frac{N_p}{s_p} > 0.5$ have positive discriminant and no rational point of order 2.

Note that among 59 rank 2 curves, for 25 of them $E(\mathbb{R})$ is not connected (and have no rational point of order 2). For the rest of the rank 2 elliptic curves, we don't have an explanation of why they satisfy the conjecture.

Lastly, in the final section we will show how the Gross-Waldspurger formula might answer question 2. More precisely, we will show that the quaternion modular form v_E associated to an elliptic curve E of rank 2 must be orthogonal to divisors arising from optimal embeddings of certain imaginary quadratic fields into maximal orders of the quaternion algebra B, leading to a larger amount of supersingular zeros.

2 Proof of the main theorems

2.1 Katz's modular forms

We will recall the definition of modular forms given by Katz in [5].

Definition 5 *A modular form of weight $k \in \mathbb{Z}$ and level 1 over a commutative ring R_0 is a rule g that assigns to every pair $(\tilde{E}/R, \omega)$, where $\tilde{E}$ is and elliptic curve over $Spec(R)$ for R an R_0-algebra and ω is a nowhere vanishing section of $\Omega^1_{\tilde{E}/R}$ on $\tilde{E}$, an element $g(\tilde{E}/R, \omega) \in R$ that satisfies the following properties:*

1 $g(\tilde{E}/R, \omega)$ depends only on the R-isomorphism class of $(\tilde{E}/R, \omega)$.

2 For any $\lambda \in R^\times$,

$$g(\tilde{E}/R, \lambda\omega) = \lambda^{-k} g(\tilde{E}/R, \omega).$$

3 $g(\tilde{E}/R, \omega)$ commutes with base change by morphisms of R_0-algebras.

The space of modular forms of weight k and level 1 over R_0 is denoted by $\mathcal{M}(R_0, k, 1)$.

Given any $g \in \mathcal{M}(R_0, k, 1)$, we say that g is holomorphic at ∞ if its q-expansion,

$$g((Tate(q), \omega_{can})_{R_0} \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0,$$

actually belongs to $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$. The submodule of all such elements will be denoted by $M(R_0, k, 1)$.

Remark The reader should notice that the notations used here are not the same as the ones used by Katz.

In the rest of the article we will only consider the case when $R_0 = \overline{\mathbb{F}_p}$, for $p \geq 5$ a prime number.

In [10] and [11] Serre considers the space of modular forms modulo p of weight k and level 1 as the space consisting of all elements of $\overline{\mathbb{F}_p}[[q]]$ that are the reduction modulo p of the q-expansions of elements in M_k that have p-integer coefficients. The following proposition shows that under mild assumptions, this definition agrees with the previous definition.

Proposition 6 ([2] Lemma 1.9) *Let $k \geq 2$ and $p \geq 5$. Then, the natural map*

$$M(\overline{\mathbb{Z}_p}, k, 1) \to M(\overline{\mathbb{F}_p}, k, 1),$$

is surjective.

Example Given $p \geq 5$, and an elliptic curve $\tilde{E}/\overline{\mathbb{F}_p}$ we can write an equation for $\tilde{E}$ of the form

$$\tilde{E} : y^2 = x^3 - 27c_4 - 54c_6.$$

It is equipped with a canonical nowhere vanishing differential $\omega_{can} = \frac{dx}{y}$.

- $E_4(\tilde{E}/\overline{\mathbb{F}_p}, \omega_{can}) := c_4$ defines an element in $M(\overline{\mathbb{F}_p}, 4, 1)$ whose q-expansion is the same as the the reduction modulo p of the classical Eisenstein series E_4.
- $E_6(\tilde{E}/\overline{\mathbb{F}_p}, \omega_{can}) := c_6$ defines an element in $M(\overline{\mathbb{F}_p}, 6, 1)$ whose q-expansion is the same as the the reduction modulo p of the classical Eisenstein series E_6.
- $\Delta(\tilde{E}/\overline{\mathbb{F}_p}, \omega_{can}) := \frac{c_4^3 - c_6^2}{1728} = \Delta(\tilde{E})$ defines an element in $M(\overline{\mathbb{F}_p}, 12, 1)$ whose q-expansion is the same as the the reduction modulo p of the classical cuspform Δ.
- $j(\tilde{E}/\overline{\mathbb{F}_p}, \omega_{can}) := \frac{c_4^3}{\Delta} = j(\tilde{E})$ defines an element in $\mathcal{M}(\overline{\mathbb{F}_p}, 0, 1)$ whose q-expansion is the same as the the reduction modulo p of the classical j-invariant.

Proposition 7 *Given $\tilde{E}/\overline{\mathbb{F}_p}$ an elliptic curve and ω a nowhere vanishing differential on $\tilde{E}$, the following holds:*

- *$\Delta(\tilde{E}, \omega)$ never vanishes.*
- *$E_4(\tilde{E}, \omega)$ vanishes if and only if $j(\tilde{E}) = 0$.*
- *$E_6(\tilde{E}, \omega)$ vanishes if and only if $j(\tilde{E}) = 1728$.*
- *$j((\tilde{E}, \omega)) = j(\tilde{E})$, i.e., it only depends on the isomorphism class of $\tilde{E}$.*

Proof If we evaluate $\Delta(\tilde{E}, \omega_{can})$ we recover the discriminant of $\tilde{E}$. This is non-zero as, by definition, an elliptic curve is non-singular. The remaining statements are analogous. □

Now we have the ingredients to prove the following proposition that relates the zeros of the divisor polynomial of E with the zeros of the modular form F_E modulo p.

Proposition 8 *Given $\tilde{E}/\overline{\mathbb{F}_p}$ an elliptic curve with a nowhere vanishing invariant differential ω we have that*

$$F(F_E, j(\tilde{E})) \equiv 0 \bmod p \iff F_E(\tilde{E}, \omega) = 0.$$

Proof Suppose that $j(\tilde{E}) \neq 0, 1728$. Consider

$$\frac{F_E}{\Delta^{m(k)} \tilde{E}_k} = \tilde{F}(F_E, j(-)) \in \mathcal{M}(\overline{\mathbb{F}_p}, 0, 1).$$

It can be evaluated at pairs $(\tilde{E}, \omega)$, but since it is has weight zero it depends only on the isomorphism class of $\tilde{E}$. Therefore it only depends on the j-invariant of the elliptic curve. Note that by Proposition 7 the denominator does not vanish and the result follows. If $j = 0$ or $j = 1728$ an analogous argument shows the proposition, as $F(F_E, x) = h_k(x)\tilde{F}(F_E, x)$, and h_k takes into account the vanishing of these special j-invariants.

□

2.2 The spaces $S(\overline{\mathbb{F}_p}, k, 1)$

Following [13], we introduce a definition:

Definition 9 *$S(\overline{\mathbb{F}_p}, k, 1)$ is the space of rules g that assign to every pair $(\tilde{E}/\overline{\mathbb{F}_p}, \omega)$, where $\tilde{E}$ is a **supersingular** elliptic curve and ω is a nowhere vanishing differential on $\tilde{E}$, an element $g(\tilde{E}/\overline{\mathbb{F}_p}, \omega) \in \overline{\mathbb{F}_p}$ that satisfies the same properties as in Definition 5.*

Definition 10 *For $\ell \neq p$ a prime number we define the Hecke operator T_ℓ acting on $S(\overline{\mathbb{F}_p}, k, 1)$ as*

$$(g\mid_{T_\ell})(\tilde{E}, \omega) = \frac{1}{\ell}\sum_C g(\tilde{E}/C, \pi_{C*}\omega),$$

where the sum is taken over the $\ell+1$ subgroups of $\tilde{E}$ of order ℓ and $\pi_C : \tilde{E} \to \tilde{E}/C$ is the corresponding isogeny.

Proposition 11 *We have a natural inclusion $M(\overline{\mathbb{F}_p}, k, 1) \subset S(\overline{\mathbb{F}_p}, k, 1)$. If $g \in M(\overline{\mathbb{F}_p}, k, 1)$ is an eigenform for the Hecke operators T_ℓ ($\ell \neq p$) with eigenvalues $\lambda_\ell \in \overline{\mathbb{F}_p}$, then, the image of g in $S(\overline{\mathbb{F}_p}, k, 1)$ is an eigenform for the Hecke operators with the same eigenvalues λ_ℓ.*

Proof This is clear from the definitions. □

We have the following proposition that allows us to shift from weight $p+1$ to weight 0.

Proposition 12 ([9], Lemma 6) *The map from $S(\overline{\mathbb{F}_p}, 0, 1) \to S(\overline{\mathbb{F}_p}, p+1, 1)$ given by multiplication by E_{p+1} induces an isomorphism of Hecke modules*

$$S(\overline{\mathbb{F}_p}, 0, 1)[1] \cong S(\overline{\mathbb{F}_p}, p+1, 1),$$

where $S(\overline{\mathbb{F}_p}, 0, 1)[1]$ denotes the Tate twist. More precisely we have that for all $g \in S(\overline{\mathbb{F}_p}, 0, 1)$,

$$\ell E_{p+1}.(g\mid_{T_\ell}) = (g.E_{p+1})\mid_{T_\ell}.$$

If we consider the isobaric polynomials A, B such that $A(E_4, E_6) = E_{p-1}$ and $B(E_4, E_6) = E_{p+1}$, the reductions $\tilde{A}$, $\tilde{B}$ have no common factor ([10, Corollary 1 of Theorem 5]). Since E_{p-1} vanishes at supersingular elliptic curves we obtain that E_{p+1} does not vanish at supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

The reduction modulo p of F_E can be regarded as an element of $S(\overline{\mathbb{F}_p}, p+1, 1)$, and by the above remarks we can consider

$\overline{F_E} = F_E/E_{p+1}$.

Combining these results with Proposition 8 we obtain the following result.

Proposition 13 *Given $\tilde{E}/\overline{\mathbb{F}_p}$ a **supersingular** elliptic curve with a nowhere vanishing invariant differential ω we have that*

$$F(F_E, j(\tilde{E})) \equiv 0 \bmod p \iff \overline{F_E}(\tilde{E}) = 0.$$

Finally, we state a proposition that will be useful later.

Proposition 14 *The element $\overline{F_E} \in S(\overline{\mathbb{F}_p}, 0, 1)[1]$ has the same eigenvalues for T_ℓ ($\ell \neq p$) as F_E. In addition, it has the same eigenvalues modulo p as f_E.*

Proof The first part follows from Proposition 12 while the second part follows from the discussion given in the introduction.

□

2.3 Modular forms on quaternion algebras

We will recall some of the results previously stated in the introduction. This exposition follows entirely the fundamental work of Gross [4]. The geometric fiber of the curve $X_0(p)$ in characteristic p is the union of two rational curves meeting at n ordinary double points: e_1, e_2, …, e_n that are in bijective correspondence with the isomorphism classes of supersingular elliptic curves E_i. Recall that $\mathcal{X}$ is the free $\mathbb{Z}$-module of divisors supported on the e_i with a $\mathbb{Z}$-bilinear pairing

$$\langle , \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{Z},$$

given by $\langle e_i, e_j \rangle = w_i \delta_{i,j}$ for all $i, j \in \{1, \ldots, n\}$, where $w_i = \frac{1}{2}\#\mathrm{Aut}(E_i)$.

This pairing identifies $\mathcal{X}^* = Hom(\mathcal{X}, \mathbb{Z})$ with the subgroup of $\mathcal{X} \otimes \mathbb{Q}$ with basis $e_i^* = \frac{e_i}{w_i}$.

The action of Hecke correspondences on the set of e_i induces an action on $\mathcal{X}$. Explicitly, the action of the correspondence t_m ($m \geq 1$) is given by the transpose of the Brandt matrix $B(m)$

$$t_m e_i = \sum_{j=1}^{n} B_{ij}(m) e_j,$$

where $B_{ij}(m)$ is the number of subgroups schemes of order m in E_i such that $E_i/C \simeq E_j$. Furthermore, the pairing is Hecke compatible [4, Proposition 4.6].

Let M_2 be the $\mathbb{Z}$-module consisting of holomorphic modular forms for the group $\Gamma_0(p)$ such that when we consider its q-expansion, all coefficients are integers except maybe the first coefficient which is only required to be in $\mathbb{Z}[1/2]$. The Hecke algebra

$\mathbb{T} = \mathbb{Z}[\cdots, T_m, \cdots]$ acts on M_2 by the classical formulas. Moreover, we have that as endomorphisms of M_2

$$T_p + W_p = 0,$$

where W_p is the Atkin-Lehner involution ([4, p. 141]. In addition, the map given by $T_m \to t_m$ defines an isomorphism of Hecke algebras.

Proposition 15 ([4], Proposition 5.6) *The map $\phi : \mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \to M_2$ given by*

$$\phi(e, f) = \frac{deg(e)deg(f)}{2} + \sum_{m \geq 1} \langle t_m e, f \rangle q^m,$$

defines a $\mathbb{T}$-morphism which becomes an isomorphism over $\mathbb{T} \otimes \mathbb{Q}$.

Now we can define

$$v_E = \sum v_E(e_i) e_i \in \mathcal{X}$$

to be an eigenvector for all t_m corresponding to f_E, i.e. $t_m v_E = \lambda_m v_E$, where $f_E(\tau) = \sum_{m=1}^{\infty} \lambda_m q^m$. We normalize v_E (up to the sign) such that the greatest common divisor of all its entries is 1. The key observation is that v_E has the same eigenvalues modulo p as F_E.

The rule

$$\overline{F_E} = F_E / E_{p+1} \in S(\overline{\mathbb{F}_p}, 0, 1)$$

can be evaluated at supersingular elliptic curves over $\overline{\mathbb{F}_p}$ (it has weight zero), and by duality, it defines an element $\overline{F_E}^* \in \overline{\mathcal{X}}$, where $\overline{\mathcal{X}}$ is the reduction modulo p of $\mathcal{X}$. Note that by the definitions of t_ℓ and T_ℓ, if $\overline{F_E}^* \in \overline{\mathcal{X}}$ has eigenvalues λ_ℓ for t_ℓ then $\overline{F_E} \in S(\overline{\mathbb{F}_p}, 0, 1)$ has eigenvalues $\ell\lambda_\ell$ for T_ℓ.

Proposition 16 $\overline{F_E}^* = \sum \overline{F_E}(e_i) e_i^* = \sum \overline{F_E}(e_i)(1/w_i) e_i$ *and* $v_E = \sum v_E(e_i) e_i$ *have the same eigenvalues modulo p for the Hecke operators t_ℓ ($\ell \neq p$).*

Proof By Proposition 14, $\overline{F_E}$ has the same eigenvalues as F_E for T_ℓ ($\ell \neq p$), but with the action twisted, that is, $T_\ell \overline{F_E} = \ell \lambda_\ell \overline{F_E}$. Since the pairing defining the duality is Hecke linear and by the above remarks we must have $t_\ell \overline{F_E} = \lambda_\ell \overline{F_E}$, which has the same eigenvalues modulo p as v_E. □

Corollary 17 $\overline{F_E}(e_i) \equiv 0 \bmod p \iff v_E(e_i) \equiv 0 \bmod p.$

Proof The forms $\overline{F_E}^* = \sum \overline{F_E}(e_i)(1/w_i) e_i$ and $v_E = \sum v_E(e_i) e_i$ have the same eigenvalues for T_ℓ ($\ell \neq p$) by Proposition 16. By the work of Emerton [3, Theorem 0.5 and Theorem 1.14] we have the multiplicity one property for $\mathcal{X}$ modulo p, since p is a prime different from 2.

Therefore, up to a non-zero scaling, the coefficients of these two quaternion modular forms agree modulo p. Finally, noting that the w_i are not divisible by p, the result follows. □

Now we are in position to prove Theorem 2.

Proof of Theorem 2

$$v_E(e_i) \equiv 0 \iff \overline{F_E}(e_i) = 0 \iff F(F_E, j(E_i)) \equiv 0.$$

The first equivalence is Corollary 17; the last one is Proposition 13. □

Let $S_p \subset \{1, \dots, n\}$ be a subset of indices such that $i \in S_p$ if and only if $j(E_i) \in \mathbb{F}_p$ (hence $\#S_p = s_p$). For $i \in \{1, \dots, n\}$ let $\bar{i}$ be the unique element of $\{1, \dots, n\}$ such that $E_i^p \cong E_{\bar{i}}$. Note that, $\bar{i} = i$ if and only if $i \in S_p$.

Proposition 18 ([4], Proposition 2.4) *The Hecke operator t_p induces an involution on $\mathcal{X}$ which satisfies that for every $1 \leq i \leq n$*

$$t_p e_i = e_{\bar{i}}.$$

Now we finish the section with the proof of Theorem 1.

Proof of Theorem 1 Let E_i be a supersingular elliptic curve with $j(E_i) \in \mathbb{F}_p$. The operator t_p acts as $-W_p$ on M_2 and since the elliptic curve has root number -1 we get that t_p acts as -1. By Proposition 18 we have that $t_p e_i = e_i$, hence $v_E(e_i) = 0$, and the result follows from Theorem 2. □

3 Proof of Theorem 4

3.1 Some basic properties of Brandt matrices

Following [4], we will recall some useful properties of Brandt matrices. Let B be the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. For each $i = 1, \dots, n$ let R_i be a maximal order of B such that $R_i \cong End(E_i)$. Set $R = R_1$ and let $\{I_1, \dots, I_n\}$ be a set of left R-ideals representing different R-ideal classes, with $I_1 = R$. We can choose the I_i's such that the right order of I_i is equal to R_i. For $1 \leq i, j \leq n$, define $M_{ij} = I_j^{-1} I_i$; this is a left R_i-module and a right R_j-module. The Brandt matrix of degree m, $B(m) = (B_{ij}(m))_{1 \leq i,j \leq n}$, is defined by the formula

$$B_{ij}(m) = \frac{1}{2w_j} \#\{b \in M_{ij} : \frac{\mathrm{Nr(b)}}{\mathrm{Nr(M_{ij})}} = m\},$$

where Nr(b) is the reduced norm of b, and $\mathrm{Nr(M_{ij})}$ is the unique positive rational number such that the quotients $\frac{\mathrm{Nr(b)}}{\mathrm{Nr(M_{ij})}}$ are all integers with no common factor.

Alternatively, $M_{ij} \cong Hom_{\overline{\mathbb{F}_p}}(E_i, E_j)$ and $B_{ij}(m)$ is equal to the number of subgroup schemes C of order m in E_i such that $E_i/C \simeq E_j$ [4, Proposition 2.3].

Following the discussion before 18 we can state the following results.

Proposition 19 *We have the equality $v_E(e_j) = \lambda_p v_E(e_{\bar{j}})$. In particular, $v_E(e_j)$ and $v_E(e_{\bar{j}})$ have the same parity.*

Proof The first assertion follows from the fact that $\sum_i v_E(e_i)e_i$ is an eigenvector for the action of t_p and Proposition 18. The last assertion follows from the fact that $\lambda_p = \pm 1$. □

Proposition 20 *For all $i, j \in \{1, \dots, n\}$ and $m \in \mathbb{N}$, we have*

$$B_{ij}(m) = B_{\bar{i}\bar{j}}(m).$$

Proof For any m we have that, since the Brandt matrices commute, $B(m)B(p) = B(p)B(m)$. In other words,

$$\sum_k B_{\bar{i}k}(p)B_{kj}(m) = \sum_k B_{\bar{i}k}(m)B_{kj}(p).$$

Using Proposition 18 we know that $B_{k\ell}(p) = \delta_{\bar{k}\ell}$, in consequence we have

$$B_{ij}(m) = B_{\bar{i}\bar{j}}(m),$$

as we wanted. □

Proposition 21 *Let $l \neq p$ be an odd prime such that $\left(\frac{-p}{l}\right) = -1$. Then for all $i, j \in S_p$,*

$$B_{ij}(l) \equiv 0 \pmod 2.$$

Proof Let $\phi_i \in R_i \cong End(E_i)$ and $\phi_j \in R_j \cong End(E_j)$ be the Frobenius endomorphisms of the elliptic curves E_i and E_j respectively (they exist since $E_i \cong E_i^p$ and $E_j \cong E_j^p$). These are trace zero elements of reduced norm p, i.e. $\phi_i^2 = \phi_j^2 = -p$. Consider the map $\Theta : B \to B$ given by

$$\Theta(f) = \frac{-1}{p}\phi_j f \phi_i.$$

Note that $\Theta^2 = Id$, and $\mathrm{Nr}(\Theta(\mathrm{f})) = \mathrm{Nr}(\mathrm{f})$.

First we prove that $\Theta(M_{ij}) \subset M_{ij}$. Take $f \in Hom(E_i, E_j)$ and consider

$$g = \phi_j \circ f \circ \phi_i \in Hom(E_i, E_j).$$

Since the inseparable degree of g is divisible by p^2, it factors as $h \circ [p]$ with $h \in Hom(E_i, E_j)$, hence $\Theta(f)$ belongs to $Hom(E_i, E_j)$.

Next, we show that Θ has two eigenspaces W_- and W_+ of dimension 2 with eigenvalues -1 and 1 respectively. We consider two cases:

a) $i = j$ (i.e. $M_{ij} = R_i$)
Direct calculation shows that the vectors 1 and ϕ_i span the eigenspace with eigenvalue 1. The eigenspace with eigenvalue -1 is the orthogonal complement of ϕ_i in the trace zero subspace B^0 of B (since for $f \in B^0$ we have $f \perp \phi_i \iff \mathrm{Nr(f+\phi_i) = Nr(f) + Nr(\phi_i)} \iff \mathrm{f\hat{\phi}_i + \hat{f}\phi_i = 0} \iff \mathrm{f\phi_i = -\phi_i f} \iff \Theta(f) = -f$).

b) $i \neq j$
Let $\phi_{ji} := \phi_j \phi_i$. The matrix representations of Θ in the invariant subspaces generated by $\{1, \phi_{ji}\}$ and $\{\phi_i, \phi_j\}$ are equal to $\left(\begin{smallmatrix} 0 & -p \\ -1/p & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, hence Θ has two eigenspaces of dimension 2 with eigenvalues -1 and 1.

For $b \in M_{ij}$ let $w_1 \in W_-$ and $w_2 \in W_+$ be such that $b = w_1 + w_2$. Then $\Theta(b) = -w_1 + w_2 \in M_{ij}$, and $2w_1, 2w_2 \in M_{ij}$. Let $V_- = W_- \cap M_{ij}$ and $V_+ = W_+ \cap M_{ij}$. Thus

$$M_{ij}/(V_- + V_+) \leq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}.$$

In order to prove that $B_{ij}(l)$ is even, it is enough to show that for every $b \in M_{ij}$ such that $\frac{\mathrm{Nr(b)}}{\mathrm{Nr(M_{ij})}} = l$ the set

$$C = \{\omega b : \omega \in R_j^\times\} \cup \{\omega \Theta(b) : \omega \in R_j^\times\}$$

has maximal cardinality $\#C = 4w_j$ (note that all elements of C have the same norm.) It is enough to prove that b is not an eigenvector of Θ.

Let $a \in \mathbb{Z}$ be such that $I = aM_{ij} \subset R_j$. If M^2 is the index of I in R_j, then $q_I(x) := \frac{\mathrm{Nr(x)}}{M}$ is an integral quadratic form on I which is in the same genus as (R_j, Nr). In particular, $disc(q_I) = p^2$. Moreover, $q(x) := q_I(ax)$ is a quadratic form on M_{ij} for which $q(x) = \frac{\mathrm{Nr(x)}}{\mathrm{Nr(M_{ij})}}$ ($\mathrm{Nr(M_{ij}) = \frac{1}{M}}$). Since Θ preserves reduced norm, the lattices V_+ and V_- are orthogonal with respect to q, and $|disc(V_+)disc(V_-)| = |disc(V_+ + V_-)|$. It follows that

$$disc(V_+), disc(V_-) \in \{-p, -4p\}$$

since $M_{ij}/(V_- + V_+) \leq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$ and q is a positive definite form.

Assume that b is an eigenvector of Θ. Then $b \in V_+$ or $b \in V_-$. In any case since $l = q(b)$, it follows that l is representable by a binary quadratic form of discriminant $-p$ or $-4p$ which is not possible since $\left(\frac{-p}{l}\right) = \left(\frac{-4p}{l}\right) = -1$.

□

3.2 Fourier coefficients of $f_E(\tau)$ mod 2

Proposition 22 *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p such that E has positive discriminant and E has no rational point of order 2. There is a positive proportion of odd primes ℓ such that $\left(\frac{-p}{\ell}\right) = -1$ and $\lambda_\ell \equiv 1 \pmod 2$, where $f_E(\tau) = \sum \lambda_m q^n$ is the q-expansion of $f_E(\tau)$.*

Proof Denote by $\rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_2)$ the mod 2 Galois representation attached to the elliptic curve E (or equivalently, by the modularity theorem, to the

modular form f_E). For an odd prime $\ell \neq p$, we have that

$$\lambda_\ell \equiv \mathrm{Tr}(\rho_2(Frob_\ell)) \bmod 2,$$

where $Frob_\ell$ is a Frobenius element over ℓ. The group $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to S_3, and the elements of trace 1 are exactly the elements of order 3. ρ_2 factors through $\mathrm{Gal(K/\mathbb{Q})}$, and $\mathrm{Gal(K/\mathbb{Q})} \cong \Im(\rho_2)$ where $K = \mathbb{Q}(E[2])$. It is enough to prove that there is a positive proportion of prime numbers ℓ such that $\left(\frac{-p}{\ell}\right) = -1$ and $Frob_\ell \in \mathrm{Gal(K/\mathbb{Q})}$ has order 3. Since E has no rational point of order 2, $Gal(K/\mathbb{Q})$ is either $\mathbb{Z}/3\mathbb{Z}$ (if the discriminant of E is a square) or S_3. Moreover, since E has prime conductor and no rational two torsion, it follows from Proposition 7 in [12] that the absolute value of the discriminant is not a square. Hence, $K/\mathbb{Q}$ is an S_3 extension, and since the discriminant is positive and its only prime divisor can be p, the quadratic field F contained in K is equal to $\mathbb{Q}(\sqrt{p})$.

If $\ell \equiv 3 \pmod 4$ then $\left(\frac{-p}{\ell}\right) = -1$ implies that ℓ splits in F. If, in addition, ℓ does not split completely in K, then the order of $Frob_\ell$ is 3 and λ_ℓ is odd. There is a positive proportion of such primes ℓ since by Chebotarev density theorem (applied to the field $L = \mathbb{Q}(\sqrt{-1})K$) there is a positive proportion of primes ℓ which are inert in $\mathbb{Q}(\sqrt{-1})$, split in F and do not split completely in K.

□

3.3 Proof of Theorem 4

Proof Take ℓ an odd prime such that $\left(\frac{-p}{\ell}\right) = -1$ and $\lambda_\ell \equiv 1 \pmod 2$ as in Proposition 22. Consider the action of t_ℓ on $\sum_i v_E(e_i)e_i$. Take any $j \in S_p$, that is $\bar{j} = j$. By comparing the coefficient of e_j in the equation $t_\ell \sum_i v_E(e_i)e_i = \lambda_\ell(\sum_i v_E(e_i)e_i)$ we obtain

$$\lambda_\ell v_E(e_j) = \sum_i v_E(e_i)B_{ij}(\ell).$$

We are going to look at this equation modulo 2; we know that λ_ℓ is odd and we know by Proposition 21 that for any $i \in S_p$, $B_{ij}(\ell)$ is even. Therefore,

$$v_E(e_j) \equiv \sum_{i \notin S_p} v_E(e_i)B_{ij}(\ell) \bmod 2.$$

Proposition 20 tells us that $B_{ij}(\ell) = B_{\bar{i}\bar{j}}(\ell) = B_{\bar{i}j}(\ell)$ as $j = \bar{j}$. Moreover, by Proposition 19, the numbers $v_E(e_i)$ and $v_E(e_{\bar{i}})$ have the same parity. Therefore, rearranging the elements of the sum $\sum_{i \notin S_p} v_E(e_i)B_{ij}(\ell)$ in conjugated pairs, we obtain that this sum is zero modulo 2. In conclusion we must have $v_E(e_j) \equiv 0 \bmod 2$, as we wanted to prove. □

We are going to give a different proof of Theorem 4 under the additional assumption that E is supersingular at 2. The idea is to use the results of [6] on level raising

modulo 2 together with the multiplicity one mod 2 results from [3] to obtain mod 2 congruences between modular forms of the same level p, but with different signs of the Atkin-Lehner involution. We hope that by extending these ideas to level $2^r p$ one will be able to understand Conjecture 1 better.

Theorem 23 *Let E be a rational elliptic curve of conductor p, without rational 2-torsion and with positive discriminant. Suppose further that E is supersingular at 2 . Then, there exists a newform $g \in S_2(\Gamma_0(p))$ and a prime λ above two in the field of coefficients of g such that $f \equiv g \bmod \lambda$ and such that W_p acts as -1 on g.*

Proof We will verify the assumptions of [6, Theorem 2.9], starting with our elliptic curve E of prime conductor and in the scenario where we choose no primes as level raising primes (so we are looking for a congruence between level p newforms). As we explained before, the hypotheses imply that $\rho_2 : G_{\mathbb{Q}} \to Gl_2(\mathbb{F}_2)$ is surjective and the only quadratic extension of $\mathbb{Q}(E[2])$ is given by $\mathbb{Q}(\sqrt{p})$. Therefore, the conductor of ρ_2 is p and it is not induced from $\mathbb{Q}(i)$. Moreover ρ_2 restricted to $G_{\mathbb{Q}_2}$ is not trivial if E is supersingular at 2. Thus, we are in position to use the theorem and find a g as in the statement, because, since $\Delta(E) > 0$, we can prescribe the sign of the Atkin-Lehner involution at p. □

Now we are in condition to give another proof of Theorem 4, under the additional assumption that E is supersingular at 2. Since g has eigenvalue -1 for the Atkin-Lehner operator we have that $v_g(e_i) = 0$ for every $i \in S_p$ by Proposition 18. As we did earlier, Theorem 0.5 and Theorem 1.14 in [3] imply, since E is supersingular at 2, that we have multiplicity one mod 2 in the f_E-isotypical component in $\mathcal{X}$, therefore $v_E(e_i)$ is even for $i \in S_p$ as we wanted to show.

4 Further remarks

Suppose that E is an elliptic curve with root number $+1$ and positive rank. By Gross-Zagier-Kolyvagin we must have $L(E, 1) = 0$ and we can use Gross-Waldspurger formula to obtain some relations satisfied by the $v_E(e_i)$. More precisely if we take $-D$ a fundamental negative discriminant define

$$b_D = \sum_{i=1}^{n} \frac{h_i(-D)}{u(-D)} e_i,$$

where $h_i(-D)$ is the number of optimal embeddings of the order of discriminant $-D$ into $End(E_i)$ modulo conjugation by $End(E_i)^\times$ and $u(-D)$ is the number of units of the order. In this scenario, we have Gross-Waldspurger formula ([4, Proposition 13.5]).

Proposition 24 *If $-D$ is a fundamental negative discriminant with $\left(\frac{-D}{p}\right) = -1$, then*

$$L(E, 1)L(E \otimes \varepsilon_D, 1) = \frac{(f_E, f_E)}{\sqrt{D}} \frac{{m_D}^2}{\langle v_E, v_E \rangle},$$

where ε_D is the quadratic character associated to $-D$, (f_E, f_E) is the Petersson inner product on $\Gamma_0(p)$ and $m_D = \langle v_E, b_D \rangle$.

Since $L(E,1) = 0$ we obtain that

$$m_D = \langle v_E, b_D \rangle = 0.$$

This says that, as we vary throughout all D as in the proposition, we obtain some relations that are satisfied by the $v_E(e_i)$ that make them more likely to be zero. For example, if we take a fundamental discriminant of class number 1 such that p is inert in that field, then the divisor b_D is supported in only one e_i with $i \in S_p$. Since the inner product between b_D and v_E is zero we get that $v_E(e_i) = 0$. This certainly explains a lot of the vanishing that is occurring in our setting, specially considering that the range we are looking into is not very large. One could hope to make these heuristics more precise by analyzing imaginary quadratic fields with small size compared to the degree of the modular parametrization (this measures the norm of v_E) and try to obtain explicit lower bounds on the number of zeros in this situation.

Acknowledgements
We would like to thank the ICTP and the ICERM for provding the oportunity of working on this project. We would like to thank A. Pacetti for his comments on an early version of this draft.
MK acknowledges support from the QuantiXLie Center of Excellence. DK was partially supported by a CONICET doctoral fellowship.

Author details
[1]Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia. [2]Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina. [3]IMAS, CONICET, Buenos Aires, Argentina.

References

1. Agashe, A., Ribet, K.A., Stein, W.A.: The modular degree, congruence primes, and multiplicity one. In: Number Theory, analysis and geometry, Springer, New York, pp. 19-49 (2012)
2. Edixhoven, B.: Serre's conjecture. In: Modular forms and Fermat's last theorem, Boston, MA, pp. 209–242 (1997)
3. Emerton, M.: Supersingular elliptic curves, theta series and weight two modular forms. J. Amer. Math. Soc. **15** no.3, 671-714 (2002)
4. Gross, B.: Heights and the Special Values of L-series. In: Number Theory, CMS Conference Proceedings **7**, 115-187 (1987)
5. Katz, N. M.: p-adic properties of modular schemes and modular forms. In: Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp 1972, 60–190. Lecture Notes in Math., Vol. **350**(1973)
6. Le Hung, B., Li. C.: Level raising mod 2 and arbitrary 2-Selmer ranks. Compos. Math. **152**, no. 8, 1576-1608 (2016)
7. Mestre, J. F.: La méthode des graphes. Exemples et applications. In: Proceedings of the international conference on class numbers and fundamental units of algebraic number fields, 217–242 (1986)
8. Ono, K.: The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series. CBMS Regional Conference Series in Mathematics, **102** (2003).
9. Robert, G: Congruences entre séries d'Eisenstein, dans le cas supersingulier, Invent. Math. **61** no.2, 103–158 (1980)
10. Serre, J-P.: Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. In: Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, 319–338. Lecture Notes in Math., Vol. **317** (1973)
11. Serre, J-P.: Formes modulaires et fonctions zêta p-adiques. In: Modular functions of one variable. In: III Proc. Internat. Summer School, Univ. Antwerp 1972, 191–268. Lecture Notes in Math., Vol. **350** (1973)
12. Serre, J-P.: Sur les représentations modulaires de degré 2 de $Gal(Q^-/Q)$, Duke Math. J. **54**, no. 1, 179–230 (1987)
13. Serre, J-P.: Two letters on quaternions and modular forms (mod p). Isr. J. Math. **95**, 281-299 (1996)
14. Watkins, M.: Explicit Lower Bounds on the Modular Degree of an Elliptic Curve. Mathematics Faculty Scholarship. Paper 104 (2004)
15. Zagier, D.: Modular parametrizations of elliptic curves. Canad. Math. Bull. **28**, 372-384 (1985)