The field generated by the points of small prime order on an elliptic curve

Loïc Merel and William A. Stein

Introduction

Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$, and for any prime number p, denote by $\mathbf{Q}(\mu_p)$ the cyclotomic subfield of $\bar{\mathbf{Q}}$ generated by the pth roots of unity.

Theorem . — *Let p be a prime. If there exists an elliptic curve E over $\mathbf{Q}(\mu_p)$ such that the points of order p of $E(\bar{\mathbf{Q}})$ are all $\mathbf{Q}(\mu_p)$-rational, then $p = 2, 3, 5, 13$ or $p > 1000$.*

The case $p = 7$ was treated by Emmanuel Halberstadt. The part of the theorem that concerns the case $p \equiv 3 \pmod 4$ is given in [3]. In this paper, we give the details that permit our treating the more difficult case in which $p \equiv 1 \pmod 4$. We treat this last case with the aid of Proposition 2 below, which is not present in *loc. cit.*. The case $p = 13$ is currently under investigation by Marusia Rebolledo, as part of her Ph.D. thesis.

1. Counterexamples define points on $X_0(p)(\mathbf{Q}(\sqrt{p}))$

First we recall some of the results and notation of [3]. Let $S_2(\Gamma_0(p))$ denote the space of cusp forms of weight 2 for the congruence subgroup $\Gamma_0(p)$. Denote by $\mathbf{T}$ the subring of $\operatorname{End} S_2(\Gamma_0(p))$ generated by the Hecke operators T_n for all integers n. Let $f \in S_2(\Gamma_0(p))$ have q-expansion $\sum_{n=1}^{\infty} a_n q^n$. When χ is a Dirichlet character, denote by $L(f, \chi, s)$ the entire function which extends the Dirichlet series $\sum_{n=1}^{\infty} a_n \chi(n)/n^s$.

Let S be the set of isomorphism classes of supersingular elliptic curves in characteristic p. Denote by Δ_S the group formed by the divisors of degree 0 with support on S. It is equipped with a structure of $\mathbf{T}$-module (induced, for example, from the action of the Hecke correspondences on the fiber at p of the regular minimal model of $X_0(p)$ over $\mathbf{Z}$).

Let $j \in \bar{\mathbf{F}}_p - J_S$, where J_S denotes the set of supersingular modular invariants. We denote by ι_j the homomorphism of groups $\Delta_S \longrightarrow \bar{\mathbf{F}}_p$ that associates to $\sum_E n_E[E]$ the quantity $\sum_E n_E/(j - j(E))$, where $j(E)$ denotes the modular invariant of E.

One says that an element $j \in \mathbf{F}_p$ is *anomalous* if there exists an elliptic curve over $\mathbf{F}_p$ with modular invariant j that possesses an $\mathbf{F}_p$-rational point of order p (then necessarily $j \notin J_S$).

Let p be a prime that is congruent to 1 modulo 4. In the following proposition we prove, under a hypothesis on p, that if E is an elliptic curve over $\mathbf{Q}(\mu_p)$ all of whose torsion is $\mathbf{Q}(\mu_p)$-rational, then for each subgroup $C \subset E(\bar{\mathbf{Q}})$ of order p, the point (E, C) on $X_0(p)$ is defined over $\mathbf{Q}(\sqrt{p})$. As we will see in Proposition 2, this $\mathbf{Q}(\sqrt{p})$-rationality conclusion is contrary to fact, from which we conclude that such elliptic curves E do not exist when the hypothesis on p is satisfied. In Section 3 we verify this hypothesis for $p = 11$ and $13 < p < 1000$.

PROPOSITION 1. — *Suppose that p is congruent to 1 modulo 4. Suppose that for all anomalous $j \in \mathbf{F}_p$ and all non-quadratic Dirichlet characters $\chi\colon (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{C}^*$, there exists $t_\chi \in \mathbf{T}$ and $\delta \in \Delta_S$ such that $L(f, \chi, 1) \neq 0$ for every newform $f \in t_\chi S_2(\Gamma_0(p))$ and $\iota_j(t_\chi \delta) \neq 0$.*

Let E be an elliptic curve over $\mathbf{Q}(\mu_p)$, such that the points of order p of $E(\bar{\mathbf{Q}})$ are all $\mathbf{Q}(\mu_p)$-rational. Then for all subgroups C of order p of $E(\bar{\mathbf{Q}})$, there exists an elliptic curve E_C over $\mathbf{Q}(\sqrt{p})$ equipped with a $\mathbf{Q}(\sqrt{p})$-rational subgroup D_C of order p, and the pairs (E, C) and (E_C, D_C) are $\bar{\mathbf{Q}}$-isomorphic.

Proof. — We prove the proposition using the results of [3]. The hypothesis $\iota_j(t_\chi \delta) \neq 0$ forces $t_\chi \notin p\mathbf{T}$ and, *a fortiori*, $t_\chi \neq 0$; in addition, the non-vanishing hypothesis on the L-series forces the hypothesis $H_p(\chi)$ of *loc. cit.*, introduction.

By assumption, hypothesis $H_p(\chi)$ is satisfied for all non-quadratic Dirichlet characters χ of conductor p. Thus Corollary 3 of Proposition 6 of *loc. cit.* implies that E has potentially good reduction at the prime ideal $\mathcal{P}$ of $\mathbf{Z}[\mu_p]$ that lies above p.

Denote by j the modular invariant of the fiber at $\mathcal{P}$ of the Néron model of E. According to the corollary of Proposition 15 of *loc. cit.*, j is anomalous.

Let C be a subgroup of $E(\bar{\mathbf{Q}})$ of order p. By assumption E is an elliptic curve over $\mathbf{Q}(\mu_p)$ whose points of order p are all $\mathbf{Q}(\mu_p)$-rational, so the pair (E, C) defines a $\mathbf{Q}(\mu_p)$-rational point P of the modular curve $X_0(p)$.

Consider the morphism $\phi_\chi = \phi_{t_\chi} : X_0(p) \to J_0(p)$ obtained by composing the standard embedding of $X_0(p)$ into $J_0(p)$ with t_χ. As in section 1.3 of *loc. cit.*, ϕ_χ extends to a map from the minimal regular model of $X_0(p)$ to the Néron model of $J_0(p)$. When $\iota_j(t_\chi \delta) \neq 0$, this map is a formal immersion at the point $P_{/\mathbf{F}_p}$, according to *loc. cit.*, Proposition 4. The hypothesis that $L(f, \chi, 1) \neq 0$ for every newform $f \in t_\chi S_2(\Gamma_0(p))$, translates into $L(t_\chi J_0(p), \chi, 1) \neq 0$, which in turn implies that the χ-isotypical component of $t_\chi J_0(p)(\mathbf{Q}(\mu_p))$ is finite (this is Kato's theorem, see the discussion in section 1.5 of *loc. cit.*). We can then apply Corollary 1 of Proposition 6 of *loc. cit.*. This proves that P is $\mathbf{Q}(\sqrt{p})$-rational, which translates into the conclusion of Proposition 1.

Remark 1: Proposition 1 is true even under the weaker hypothesis that t_χ lies in $\mathbf{T} \otimes \mathbf{Z}[\chi]$, which acts $\mathbf{Z}[\chi]$-linearly on modular forms.

2. Elliptic curves and quadratic fields

Proposition 2. — *Let p be a prime number > 5 and congruent to 1 modulo 4. Let E be an elliptic curve over $\bar{\mathbf{Q}}$. There exists a subgroup $C \subset E(\bar{\mathbf{Q}})$ of order p such that (E, C) can not be defined over $\mathbf{Q}(\sqrt{p})$.*

Proof. — We procede by contradiction, i.e., we assume that for all cyclic subgroups C of order p of $E(\bar{\mathbf{Q}})$, the pair (E, C) can be defined over $\mathbf{Q}(\sqrt{p})$. We choose such a pair (E_0, C_0) over $\mathbf{Q}(\sqrt{p})$.

Assume first that all twists of E are quadratic, i.e. that $j(E)$ is neither 0 nor 1728. We show that the group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$ acts by scalars on the $\mathbf{F}_p$-vector space $E_0(\bar{\mathbf{Q}})[p]$. For this it suffices to show that all subgroups of order p of $E_0(\bar{\mathbf{Q}})[p]$ are stable by $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$.

Suppose C_1 is a cyclic subgroup of order p of $E_0(\bar{\mathbf{Q}})[p]$. By assumption, there exists a quadratic twist E_1 of E_0 and a cyclic subgroup C_1' of $E_1(\bar{\mathbf{Q}})[p]$ that is defined over $\mathbf{Q}(\sqrt{p})$, such that the image of C_1 by the isomorphism $E_0 \simeq E_1$ is C_1'. Since $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$ leaves C_1' stable and the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$ on $E_0(\bar{\mathbf{Q}})[p]$ is a quadratic twist of the action on $E_1(\bar{\mathbf{Q}})[p]$, we see that $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$ leaves C_1 stable. Thus $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$ fixes all lines in $E_0(\bar{\mathbf{Q}})[p]$, and hence acts by scalars. Denote by α the corresponding character of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p}))$.

Because of the Weil pairing, α^2 coincides with the cyclotomic character modulo p, and it factors through $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}(\sqrt{p}))$. But, when $p \equiv 1 \pmod 4$, the group $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}(\sqrt{p}))$ is of even order, and the characters modulo p form a group generated by the reduction modulo p of the cyclotomic character, which, therefore, can not be a square.

Next suppose that $j(E) = 0$ or $j(E) = 1728$. Indeed, in these two cases E has complex multiplication by an order of $K = \mathbf{Q}[\sqrt{-3}]$ or $\mathbf{Q}[\sqrt{-1}]$. Let $d_K = 3$ or $d_K = 2$ in these two cases respectively. Let C be a subgroup of order p of $E(\bar{\mathbf{Q}})$. Consider the map $\rho_0 : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{p})) \longrightarrow \mathrm{Aut}\, E_0(\bar{\mathbf{Q}})[p]$. Since E has complex multiplication, the image of ρ_0 has no element of order p. Therefore, there are at least two subgroups, including C_0, of order p of $E(\bar{\mathbf{Q}})$ stable under the image of ρ_0. Call the other subgroup C_1. Let C_2 be a subgroup of order p of $E(\bar{\mathbf{Q}})$ which is distinct from C_0 and C_1. The pair (E, C_2) can be defined over $\mathbf{Q}(\sqrt{p})$. Therefore, there exists an extension field K_2 of $\mathbf{Q}(\sqrt{p})$, whose degree d_2 divides $2d_K$, such that the image of the restriction of ρ_0 to $\mathrm{Gal}(\bar{\mathbf{Q}}/K_2)$ leaves stable three distinct subgroups of order p of $E_0(\bar{\mathbf{Q}})$, and therefore consists only of scalars. If $d_2 \leq 2$, one concludes as in the cases where $j(E) \neq 0$ and $j(E) \neq 1728$. We suppose now that $d_2 > 2$. The projective image of ρ_0 has order d_K.

Since E is an elliptic curve over $\bar{\mathbf{Q}}$ with complex multiplication by a field of class number one, there is a model for E that is defined over $\mathbf{Q}$. Consider the map $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}\, E(\bar{\mathbf{Q}})[p]$. By the theory of complex multiplication, the projective image of ρ has order $2(p+1)$ or $2(p-1)$. There exists a field extension L of degree dividing d_K of $\mathbf{Q}(\sqrt{p})$ such that the restrictions to $\mathrm{Gal}(\bar{\mathbf{Q}}/L)$ of the projective images of ρ and ρ_0 coincide. Therefore one has $(p-1)|d_K^2$ or $(p+1)|d_K^2$. This imposes $p = 5$ and $d_K = 2$.

3. Verification of the hypothesis of Proposition 1 Let p be a prime number. In this section we explain how we used a computer to verify that the second hypothesis of Proposition 1 are satisfied for $p = 11$ and $13 < p < 1000$. (In the present paper, this verification is only required for p that are congruent to 1 modulo 4.)

We first list the anomalous j-invariants $j \in \mathbf{F}_p$. Since p is fairly small in the range of our computations, we created this list by simply enumerating all of the elliptic curves over $\mathbf{F}_p$ and counting the number of points on each curve. For example, when $p = 31$ the anomalous j-invariants are $j = 10, 14$.

Let $\chi : \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{C}$ be a non-quadratic Dirichlet character, and denote by $\mathbf{Z}[\chi]$ the subring of $\mathbf{Q}(\zeta_{p-1})$ generated by the image of χ. Denote by $S_2(\Gamma_0(p); \mathbf{Z})$ the set of modular forms $f \in S_2(\Gamma_0(p))$ whose Fourier expansion at the cusp ∞ lies in $\mathbf{Z}[[q]]$.

We study the $\mathbf{T}$-modules $\mathbf{T}$, Δ_S, and $S_2(\Gamma_0(p); \mathbf{Z})$. After extension of scalars to $\mathbf{Q}$, these are $\mathbf{T} \otimes \mathbf{Q}$-modules that are free of rank 1, of which the irreducible sub-$\mathbf{T} \otimes \mathbf{Q}$ modules are the annihilators of the minimal prime ideals of $\mathbf{T}$. We compute a list of the minimal prime ideals of $\mathbf{T}$ by computing appropriate kernels and characteristic polynomials of Hecke operators of small index on Δ_S, which we find using the graph method of Mestre and Oesterlé [4].

Having computed the minimal prime ideals of $\mathbf{T}$, we verify that some nontrivial ideal $\mathcal{I}$ of $\mathbf{T}$ (always a minimal prime ideal in the range of our computations) simultaneously satisfies the following three conditions:

1) For each anomalous j-invariant, there exists $x \in \Delta_S$ such that $\mathcal{I}x = 0$ and $\iota_j(x) \neq 0$.

2) Each of the newforms $f \in S_2(\Gamma_0(p))$ with $\mathcal{I}f = 0$ satisfies $L(f, \chi, 1) \neq 0$.

3) The image of $\mathcal{I}$ in the $\mathbf{T}$-module $\mathbf{T}/p\mathbf{T}$ is a direct factor.

Let $\mathcal{I}$ be an ideal of $\mathbf{T}$. Here is how we verify these conditions for $\mathcal{I}$.

Verification of condition 1.

We verified that $\mathcal{I}$ satisfies the first condition by finding a $\mathbf{T}$-eigenvector v of $\Delta_S \otimes \bar{\mathbf{Z}}$ that is annihilated by $\mathcal{I}$ and satisfies $\iota_j(v) \neq 0$ for all anomalous j-invariants. Because ι_j is a homomorphism, this implies the existence of x as in condition 1.

Verification of condition 2.

We verified the second condition using modular symbols. Our method is purely algebraic, so we do not perform any approximate computation of integrals. Using the algorithm described in [2], we compute the action of the Hecke algebra $\mathbf{T}$ on the space $\mathrm{Hom}_{\mathbf{Q}[\chi]}(H_1(X_0(p); \mathbf{Q}[\chi]), \mathbf{Q}[\chi])$. By intersecting the kernels of appropriate elements of $\mathbf{T}$, we find a basis $\varphi_1, \ldots, \varphi_n$ for the subspace of $\mathrm{Hom}_{\mathbf{Q}[\chi]}(H_1(X_0(p); \mathbf{Q}[\chi]), \mathbf{Q}[\chi])$ that is annihilated by $\mathcal{I}$. Let $\Phi_{\mathcal{I}} = \varphi_1 \times \cdots \times \varphi_n$ denote the linear map $H_1(X_0(p); \mathbf{Q}[\chi]) \longrightarrow \mathbf{Q}[\chi]^n$ defined by the φ_i.

Let $\mathbf{T}_{\mathbf{Q}[\chi]} = \mathbf{T} \otimes \mathbf{Q}[\chi]$, where $\mathbf{Q}[\chi]$ is the number field generated the image of χ. The *χ-twisted winding element* (denoted θ_χ in [3])

$$\mathbf{e}_\chi = \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^*} \bar{\chi}(a) \left\{ \infty, \frac{a}{p} \right\}$$

generates the χ-*twisted winding submodule* $\mathbf{T}_{\mathbf{Q}[\chi]} \cdot \mathbf{e}_\chi$. To compute this submodule, we use that $\mathbf{T}$ is generated, even as a $\mathbf{Z}$-module, by $T_1, T_2, \ldots, T_b$, for any $b \geq (p+1)/6$ (see [1]).

Lemma 3. — *Let $\mathcal{I}$ be a minimal prime ideal of $\mathbf{T}$, and let $\chi : (\mathbf{Z}/N\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ be a nontrivial Dirichlet character. Then the dimension of the $\mathbf{Q}[\chi]$-vector space $\Phi_{\mathcal{I}}(\mathbf{T}_{\mathbf{Q}[\chi]} \cdot \mathbf{e}_\chi)$ is equal to the cardinality of the set of newforms f such that $\mathcal{I}f = 0$ and $L(f, \chi, 1) \neq 0$.*
Proof. — We have

$$\dim_{\mathbf{Q}[\chi]} \Phi_{\mathcal{I}}(\mathbf{T}_{\mathbf{Q}[\chi]} \cdot \mathbf{e}_\chi) = \dim_{\mathbf{C}} \Phi_{\mathcal{I}}(\mathbf{T}_{\mathbf{C}} \cdot \mathbf{e}_\chi).$$

This dimension is invariant upon changing the basis $\varphi_1, \ldots, \varphi_n$ used to define $\Phi_{\mathcal{I}}$. In particular, over $\mathbf{C}$ there is a basis $\varphi'_1, \ldots, \varphi'_n$ so that the resulting map $\Phi'_{\mathcal{I}}$ satisfies

$$\Phi'_{\mathcal{I}}(x) = \Big(\mathrm{Re}(\int_x f^{(1)}), \mathrm{Im}(\int_x f^{(1)}), \ldots, \mathrm{Re}(\int_x f^{(d)}), \mathrm{Im}(\int_x f^{(d)})\Big),$$

where $f^{(1)}, \ldots, f^{(d)}$ are the Galois conjugates of a newform $f^{(1)} = \sum a_n^{(1)} q^n$ such that $\mathcal{I}f^{(1)} = 0$. Furthermore, $\Phi'_{\mathcal{I}}$ is a $\mathbf{T}_{\mathbf{C}}$-module homomorphism if we declare that $\mathbf{T}_{\mathbf{C}}$ acts on $\mathbf{R}^{2d} = \mathbf{C}^d$ via

$$T_n(x_1, y_1, \ldots, x_d, y_d) = T_n(z_1, \ldots, z_d) = (a_n^{(1)} z_1, \ldots, a_n^{(d)} z_d),$$

where $z_j = x_j + iy_j$ and the $a_n^{(j)}$ are Fourier coefficients of the $f^{(j)}$.

As explained in Section 2.2 of [3], $\int_{\mathbf{e}_\chi} f = * \cdot L(f, \chi, 1)$, where $*$ is some nonzero real or pure-imaginary complex number, according to whether $\chi(-1)$ equals 1 or -1, respectively. Combining this observation with the equality

$$\dim_{\mathbf{C}} \Phi_{\mathcal{I}}(\mathbf{T}_{\mathbf{C}} \cdot \mathbf{e}_\chi) = \dim_{\mathbf{C}}(\mathbf{T}_{\mathbf{C}} \cdot \Phi_{\mathcal{I}}(\mathbf{e}_\chi)),$$

and that the image of $\mathbf{T}_{\mathbf{C}}$ in $\mathrm{End}(\mathbf{C}^d)$ is equal to the diagonal matrices, proves the asserted equality.

Remark 2: The dimension of $\Phi_{\mathcal{I}}(\mathbf{T}_{\mathbf{Q}[\chi]} \cdot \mathbf{e}_\chi)$ is unchanged if χ is replaced by a Galois-conjugate character.

In practice, computations over the cyclotomic field $\mathbf{Q}[\chi]$ are extremely expensive. Fortunately, for our application it suffices to give a lower bound on the dimension appearing in the lemma. Such a bound can be efficiently obtained by instead computing the reductions of Φ, χ, and the χ-twisted winding submodule modulo a suitable maximal ideal of the ring of integers of $\mathbf{Q}[\chi]$ that splits completely; this amounts to performing the above linear algebra over a relatively small finite field $\mathbf{F}_\ell$ where ℓ is congruent to 1 modulo $p-1$.

Remark 3: For every newform f in $S_2(\Gamma_0(p))$, with $p \leq 1000$, and every mod p Dirichlet character χ, we found that $L(f, \chi, 1) \neq 0$ if and only if $L(f^\sigma, \chi, 1) \neq 0$ for all conjugates f^σ of f. More generally, for any f and χ, this equivalence holds if $\mathbf{Q}[\chi]$ is linearly disjoint from the field $K_f = (\mathbf{T}/\mathcal{I}) \otimes \mathbf{Q}$. The first few primes for which there is a form f and a mod p character χ such that the linear disjointness hypothesis fails are $p = 31, 113, 127$, and 191. The analogue of this nonvanishing observation is false if we instead consider newforms on $\Gamma_1(p)$ and allow χ to be arbitrary. For example, let f be one of the two Galois-conjugate newforms in $S_2(\Gamma_1(13))$. Then there is a character $\chi : (\mathbf{Z}/7\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ of order 3 such that $L(f, \chi, 1) = 0$ and $L(f^\sigma, \chi, 1) \neq 0$.

Verification of condition 3.

The third condition is satisfied for all $p < 10000$, except possibly $p = 389$, because we have verified that the discriminant of $\mathbf{T}$ is prime to p for all such $p \neq 389$, so the ring $\mathbf{T}/p\mathbf{T}$ is semisimple. The discriminant computation was carried out by the second author as follows. Using the method of [4], we computed discrimininants of characteristic polynomials mod p of the Hecke operators T_2, T_3, T_5, and T_7. In the few cases when all four of these characteristic polynomials had discriminant equal to 0 mod p, we resorted to modular symbols to compute several more characteristic polynomials until we found one having nonzero discriminant modulo p.

We consider the remaining case $p = 389$ in detail. There are exactly five minimal prime ideals of $\mathbf{T}$, which we denote $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, $\mathcal{P}_6$, and $\mathcal{P}_{20}$, where the quotient field of $\mathbf{T}/\mathcal{P}_i$ has dimension i. The discriminant of the characteristic polynomial of T_2 is exactly divisible by 389. Since the field of fractions of $\mathbf{T}/\mathcal{P}_{20}$ has discriminant divisible by 389, we see that 389 is not the residue characteristic of any congruence prime. Let $\mathcal{O}_i = \mathbf{T}/\mathcal{P}_i$. The natural map $\mathbf{T} \to \prod \mathcal{O}_i$ has finite kernel and cokernel each of order coprime to 389, so $\mathbf{T}/389\mathbf{T} \cong \prod \mathcal{O}_i/389\mathcal{O}_i$. The nonquadratic characters $\chi : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{C}^*$ have orders $1, 4, 97, 193, 388$. We must verify that for each of these degrees, one of the ideals $\mathcal{P}_i$ satisfies conditions 1–3. We check as above that conditions 1–3 for χ of order 4 are satisfied by $\mathcal{P}_2$ and conditions 1–3 for χ of order greater than 4 are satisfied by $\mathcal{P}_1$. When χ is the trivial character, conditions 1–3 are satisfied only by $\mathcal{P}_{20}$.

Summary.

For each prime $p < 1000$ different than $2, 3, 5, 7, 13$, we verified the existence of an ideal that satisfies the three conditions given above, as follows. We consider each Galois conjugacy class of non-quadratic characters χ. We find a single newform f such that $L(f, \chi, 1) \neq 0$ for all conjugates of f and of χ. Then we let $\mathcal{I}$ be the annihilator of f, and try to verify condition 1 for *all* of the anamolous j-invariants in $\mathbf{F}_p$. When the three conditions are satisfied for an ideal $\mathcal{I}$ of $\mathbf{T}$, there exists $t_\chi \in \mathbf{T}$ that is annihilated by $\mathcal{I}$ and is the inverse image of a projector of $\mathbf{T}/p\mathbf{T}$ on the complement of $\mathcal{I} + p\mathbf{T}$. Putting $\delta = x$, one has $\iota_j(t_\chi \delta) = \iota_j(\delta) \neq 0$ (because ι_j takes its values in characteristic p, it follows that δ is annihilated by $\mathcal{I}$ and $t_\chi \in 1 + p\mathbf{T} + \mathcal{P}$). Every newform $f \in t_\chi S_2(\Gamma_0(p))$ satisfies $\mathcal{I} f = 0$, and therefore, by our second condition, $L(f, \chi, 1) \neq 0$. The pair (t_χ, δ) then satisfies the conditions required by Proposition 1.

Acknowledgment: We would like to thank Barry Mazur for providing us several useful comments.

Bibliography

[1] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Ser. I Math. 328 (1999), no. 5, 369–374.

[2] J. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, (1997).

[3] L. Merel, *Sur la nature non cyclotomique des points d'ordre fini des courbes elliptiques*, To appear in Duke Math. Journal.

[4] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata), 217–242, (1986).