Functiones et Approximatio
56.2 (2017), 271–286
doi: 10.7169/facm/1617

ON THE j-INVARIANTS OF CM-ELLIPTIC CURVES DEFINED OVER $\mathbb{Z}_p$

Andrew Fiori

Abstract: We characterize the possible reductions modulo p of the j-invariants of supersingular elliptic curves which admit complex multiplication by a (potentially non-maximal) order $\mathcal{O}$ where the curve itself is defined over $\mathbb{Z}_p$. In particular, we show that the collection of possible j-invariants as well as some aspects of the distribution depends on which primes divide the discriminant and conductor of the order $\mathcal{O}$.

Keywords: complex multiplication, lifting, elliptic curves.

1. Introduction

There are several different ways of framing the results of this paper. Our main object of study will be CM-elliptic curves over $\mathbb{Z}_p$ which are supersingular at p. The results we obtain will primarily be directed towards trying to address the following three questions:

1. When are there elliptic curves defined over $\mathbb{Z}_p$, which (after base extension) admit CM by an order $\mathcal{O}$ in a quadratic imaginary field K in which p is inert and where p does not divide the conductor of $\mathcal{O}$?
2. For such curves, what factors affect the possible reductions of their j-invariants modulo p amongst the set of all supersingular $\mathbb{F}_p$-rational j-invariants?
3. Given an $\mathbb{F}_p$-rational supersingular j-invariant which admits CM by $\mathcal{O}$, when does there exist an elliptic curve defined over $\mathbb{Z}_p$, which (after base extension) admits CM by $\mathcal{O}$, which reduces to it.

Though they are not necissarily framed in this way, related questions are treated in [Sta12], [Mor14] and [BM04] and some of our results can naturally be viewed as generalizations to the context of non-maximal orders. Furthermore, there are natural connections between some of our results and those presented in [LV15].

This work was done while the author was a Fields postdoctoral researcher at Queen's University.

2010 Mathematics Subject Classification: primary: 11G07; secondary: 11G15

We note one natural source of interest in these questions is the following observation of Ernst Kani:

Proposition. *Suppose p is unramified in K and does not divide the conductor of $\mathcal{O}$. Then every $\mathbb{F}_p$ elliptic curve which admits CM by $\mathcal{O}$ lifts to $\mathbb{Z}_p$ (with a lifting of its CM to $\overline{\mathbb{Z}}_p$) if and only if p does not divide the conductor of the ring $\mathbb{Z}[j(E_1), \ldots, j(E_n)]$ generated by the j invariants of all elliptic curves which admit CM by $\mathcal{O}$.*

Remark 1.1. This ring $\mathbb{Z}[j(E_1), \ldots, j(E_n)]$ is a natural order in the ring class field of K associated to $\mathcal{O}$, its structure is mysterious.

The results we will describe are in contrast to what one would obtain for the same questions asked for elliptic curves over $\mathbb{Z}_{p^2}$, the unramified quadratic extension of $\mathbb{Z}_p$. In particular, over $\mathbb{Z}_{p^2}$, we have the following answers:

1. There are always CM-elliptic curves over $\mathbb{Z}_{p^2}$ which admit CM by $\mathcal{O}$ an order in a quadratic imaginary field K in which p is inert, and where p does not divide the conductor.
2. From the work of Cornut-Vatsal [CV05, CV07] and Jetchev-Kane [JK11] we have that the reductions of the j-invariants of elliptic curves with CM by $\mathcal{O}$ are equidistributed among the supersingular values in $\mathbb{F}_{p^2}$ (as we vary the conductors $\mathcal{O}$ subject to certain congruence conditions). Moreover, for each p and all but finitely many $\mathcal{O}$ where p is inert, the map from elliptic curves with CM by $\mathcal{O}$ to supersingular j-invariants in $\mathbb{F}_{p^2}$ is surjective.
3. By the work of Deuring [Deu41] we know that given a supersingular elliptic curve $\overline{E}$ with CM by $\mathcal{O}$ there always exists a lift to an elliptic curve over $\mathbb{Z}_{p^2}$ with CM by $\mathcal{O}$ which reduces to $\overline{E}$ (along with its CM).

The results we obtain are motivated by computations, which gave results which seemed contrary to the above. In particular if we consider only the elliptic curves which are defined over $\mathbb{Z}_p$ then:

- They are not always surjective onto supersingular $\mathbb{F}_p$ values as we vary $\mathcal{O}$ among
  - maximal orders subject to certain congruence conditions on the discriminant;
  - orders in a certain fixed K subject to certain congruence conditions on the conductor;
  - orders subject to certain congruence conditions on the conductor and discriminant of K.
- The set of possible values, and hence the overall distributions depends on congruence conditions on both the discriminant of K and the conductor of $\mathcal{O}$.
- For certain congruence conditions on discriminants and conductors there are irreducible factors which always appear together, in equal numbers. So the appearance of a given factor is not independent on the appearance of another.

We should emphasize before proceeding that though perhaps unexpected in light of them, the above does not actually conflict with the aforementioned equidistribution results.

This paper is organized as follows:

- In Section 2 we introduce the relevant background.
- In Section 3 we state and prove our results.
- In Section 4 we discuss two natural questions our work leaves open.

2. Background

In this section we will be introducing the results necessary to state and prove our theorems. Much of what we are saying is very well known, and can be found in many references on the theory of complex multiplication. Some results which are perhaps less well known can be found in [Sch10], [Deu41], [Ibu82], [Dor89] or [LV15].

Convention. *Throughout this paper whenever we write $End(E)$ we shall mean the endomorphism algebra of E over an algebraically closed field containing the ring of definition of E.*

We recall the following important facts:

Theorem 2.1. *If E is an elliptic curve over a field of characteristic 0 then either:*

- *$End(E) = \mathbb{Z}$, this is the general case.*
- *$End(E) = \mathcal{O}$, for $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ an order in a quadratic imaginary field, this is the so-called CM-case.*

Convention. *We shall say an elliptic curve E admits CM by $\mathcal{O}$ if $\mathrm{End}(E) \simeq \mathcal{O}$. To say that E admits CM does not require that we have chosen a particular isomorphism of $\mathcal{O}$ with $\mathrm{End}(E)$.*

We will be interested in the CM or complex multiplication case in characteristic 0, where we have the following classification result:

Theorem 2.2. *The elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ has $End(E) \simeq \mathcal{O}$ if and only if*

1. *$\tau \in \mathbb{Q}(\sqrt{-D})$, that is τ generates a (complex) quadratic field, and*
2. *$\mathbb{Z} + \tau\mathbb{Z} \subset \mathbb{Q}(\sqrt{-D})$ is a (projective) $\mathcal{O}$-module.*

Moreover, for any algebraically closed field C of characteristic 0 the collection of elliptic curves which admit CM by $\mathcal{O}$ is a principal homogeneous space under the action of $C\ell(\mathcal{O})$ the ideal class group of $\mathcal{O}$.

Remark 2.3. Note that the collection of elliptic curves E which admit CM by $\mathcal{O}$ and the collection of pairs $(E, \rho : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E))$ of E and an isomorphism of $\mathcal{O}$ with $\mathrm{End}(E)$ of a fixed CM-type are in bijection. In most contexts this later moduli problem is more natural. However, this moduli space never has $\mathbb{Z}_p$-points. As we are primarily concerned with the field of definition of E and not the field over which CM is obtained we shall be considering instead the "moduli" of elliptic curves which admit CM by $\mathcal{O}$.

Theorem 2.4. *If E is an elliptic curve over a field of characteristic p then either:*

- *$End(E) = \mathbb{Z}$, this is the general case.*
- *$End(E) = \mathcal{O}$, for $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ an order in a quadratic imaginary field in which p splits.*
- *$End(E) = \mathbb{B}$, for $\mathbb{B}$ a maximal order in a quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞. This is the so-called supersingular case.*

From the above we see that if ever we can reduce a CM elliptic curve E at a prime inert in K we will obtain a supersingular elliptic curve. In the characteristic p setting it will be this case we are most interested in.

Notation 2.5. Let $m \in \mathbb{Z}^+$ be square free so that $K = \mathbb{Q}(\sqrt{-m})$ is the quadratic imaginary field of discriminant D, denote by $\mathcal{O}_K$ its maximal order and $\mathcal{O} = \mathcal{O}_{K,\mathfrak{f}} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ an order of conductor $\mathfrak{f} \in \mathbb{Z}$. Denote by:

$$P_{\mathcal{O}}(X) = \prod_{\mathfrak{a}} (X - j(\mathbb{C}/\mathfrak{a})).$$

where the product is over a set of representatives $\mathfrak{a} \lhd \mathcal{O}$ for the class group $C\ell(\mathcal{O})$ of $\mathcal{O}$. Denote by L the splitting field of $P_{\mathcal{O}}(X)$ over K.

The following facts are well known, for a reference see for example [Sch10].

- $P_{\mathcal{O}}(X) \in \mathbb{Z}[X]$ and is irreducible over K.
- L is abelian over K, with $\mathrm{Gal}(L/K) \simeq C\ell(\mathcal{O})$, the action being the natural permutation action of $C\ell(\mathcal{O})$ on the roots.
- L is galois over $\mathbb{Q}$, the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $C\ell(\mathcal{O})$ being $g \mapsto g^{-1}$ so that $\mathrm{Gal}(K/\mathbb{Q})$ is a generalized dihedral group.
- The action of complex conjugation on the ideals of K agrees with the action on the set of elliptic curves which admit CM by $\mathcal{O}$, which in turn agrees with the action of $\mathrm{Gal}(K/\mathbb{Q})$.
- L/K is ramified only at primes over $\mathfrak{f}$, whereas $L/\mathbb{Q}$ is ramified only at primes over $D\mathfrak{f}$.

We shall denote by $N = \mathbb{Q}(j) = \mathbb{Q}[X]/(P_{\mathcal{O}}(X)) \subset L$.

Based on the above we can conclude the following:

- If p is inert in K and p does not divide $\mathfrak{f}$ (or equivalently that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$) then p splits in L/K.
- If $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$ then $P_{\mathcal{O}}(X)$ factors as a product of quadratic and linear terms over $\mathbb{Z}_p$.

Remark 2.6. The above agrees with the fact that the reductions of these elliptic curves (together with their CM actions) have models over $\mathbb{F}_{p^2}$, as they are known to be supersingular.

Proposition 2.7. *If p is inert in K and E is an elliptic curve which admits CM by $\mathcal{O}$ then the reduction of E modulo p is supersingular. In particular,* $\mathrm{End}(\overline{E}) = \mathbb{B}$, *where $\mathbb{B}$ is a maximal order in a quaternion algebra ramified only at p and infinity. By reduction we may associate to such a curve E the pair* $(\mathrm{End}(E) \subset \mathrm{End}(\overline{E}))$. *This mapping gives a bijection between elliptic curves E, which admit CM by $\mathcal{O}$, and isomorphism classes of pairs $(\mathcal{O} \subset \mathbb{B})$ of $\mathcal{O}$ with an optimal embedding into a maximal order $\mathbb{B}$ as above.*

Moreover, there is a natural action of $C\ell(\mathcal{O})$ on such pairs, that is $\mathfrak{a} \lhd \mathcal{O}$ takes the pair $(\mathcal{O} \subset \mathbb{B})$ to $(\mathcal{O} \subset \mathfrak{a}\mathbb{B}\mathfrak{a}^{-1})$. Under this action the set of elliptic curves which admit CM by $\mathcal{O}$ is a principal homogeneous space under $C\ell(\mathcal{O})$. In particular $\mathrm{End}(\overline{\mathfrak{a} * E}) = \mathfrak{a}\,\mathrm{End}(\overline{E})\mathfrak{a}^{-1}$.

The original result of [Dor89] is corrected and generalized in [LV15].

From now on we shall be working in the setting where p is split in K and p does not divide $\mathfrak{f}$. In particular we are assuming that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$.

Proposition 2.8. *If $P_{\mathcal{O}}(X)$ has a linear factor over $\mathbb{Z}_p$, the number of such linear factors is* $|\mathrm{Gal}(L/K)[2]|$ *the size of the two torsion of the class group.*

Proof. By basic algebraic number theory we must count the size of the conjugacy class of Frobenius. This is then a basic property to dihedral groups. ■

Remark 2.9. If $|\mathrm{Gal}(L/K)[2]| = 1$ then $P_{\mathcal{O}}(X)$ has a unique linear factor over $\mathbb{Z}_p$.

Theorem 2.10 (Deuring). *If E corresponds to the data $(\mathcal{O} \subset \mathbb{B})$ then the reduction of E modulo p is defined over $\mathbb{F}_p$ (rather than simply $\mathbb{F}_{p^2}$) if and only if $\mathbb{B}$ contains $\mathbb{Z}[\sqrt{-p}]$.*

See [Deu41].

In [Ibu82] Ibukiyama gives a complete classification of the maximal orders $\mathbb{B}$ which contain $\mathbb{Z}[\sqrt{-p}]$.

Notation 2.11. Fix p and $q = 3 \pmod 8$ such that $\mathbb{B} = (-p, -q)$ is the quaternion algebra ramified only at p and ∞. Fix $\alpha, \beta \in \mathbb{B}$ such that $\alpha^2 = -p$, $\beta^2 = -q$ and $\alpha\beta = -\beta\alpha$. Choose $r \in \mathbb{Z}$ such that $r^2 + p = mq$ for some $m \in \mathbb{Z}$.

Denote:

$$O(p, q, r, m) = \mathbb{Z} + \mathbb{Z}\frac{\alpha(1+\beta)}{2} + \mathbb{Z}\frac{1+\beta}{2} + \mathbb{Z}\frac{(r+\alpha)\beta}{q}$$

If $p = 3 \pmod 4$ choose $r' \in \mathbb{Z}$ such that $(r')^2 + p = 4m'q$ for some $m' \in \mathbb{Z}$. Denote:

$$O'(p, q, r', m') = \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(r+\alpha)\beta}{2q}.$$

Theorem 2.12 (Ibukiyama). *The sets $O(p,q,r,m)$ (and $O'(p,q,r',m')$) are maximal orders of $\mathbb{B}$, their isomorphism classes depend only on q and not on r or m. Moreover, all pairs consisting of a maximal order in $\mathbb{B}$ with an embedding of $\mathbb{Z}[\sqrt{-p}]$ are of the form $O(p,q,r,m)$ (or $O'(p,q,r',m')$) with the embedding taking $\sqrt{-p} \to \pm\alpha$.*

The orders $O(p,q,r,m)$ and $O'(p,q,r',m')$ are only ever isomorphic if they correspond to the j-invariant 1728, equivalently if they admit an embedding of $\mathbb{Z}[\frac{\sqrt{-3}+1}{2}]$.

See [Ibu82].

Remark 2.13. In $O(p,q,r,m)$ we may write:

$$\alpha = 2\left(\frac{\alpha(1+\beta)}{2}\right) - q\left(\frac{(r+\alpha)\beta}{q}\right) + qr.$$

Remark 2.14. We can count the number of isomorphism classes of $O(p,q,r,m)$ (respectively $O'(p,q,r',m')$) by looking at the class numbers h_p for $\mathbb{Z}[\sqrt{-p}]$ (and $\tilde{h}_p$ for $\mathbb{Z}[(1+\sqrt{-p})/2]$), we have the following standard formulas (for $p \neq 3$):

- The number of supersingular j invariants over $\mathbb{F}_{p^2}$ is $n = \lfloor (p-1)/12 \rfloor + e_0 + e_{1728}$, where e_x is 0 or 1 depending on if x is supersingular at p.
- If $p = 7 \pmod 8$ then $h_p = \tilde{h}_p$ and there are $(h_p+1)/2$ options for both $O(p,q,r,m)$ and $O'(p,q,r',m')$.
- If $p = 3 \pmod 8$ then $h_p = 3\tilde{h}_p$ and there are $(h_p+1)/2$ options for $O'(p,q,r',m')$ and $(\tilde{h}_p+1)/2$ options for $O'(p,q,r',m')$.
- If $p = 1 \pmod 4$ there are $h_p/2$ options for $O(p,q,r,m)$.

Combining the above allows us to compute the number of $\mathbb{F}_p$ rational supersingular values in terms of h_p.

More generally, if we fix $K = \mathbb{Q}(\sqrt{-D})$ a quadratic imaginary field of discriminant $-D$ and class number h_K. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ and write $\mathfrak{f} = \prod q_i^{a_i}$ The class number of $\mathcal{O}$ is given by:

$$h_{\mathcal{O}} = \epsilon h_K \prod_i \left(q_i - \left(\frac{-D}{q_i}\right)\right) q_i^{a_i - 1}$$

where $\epsilon = 1$ unless $D = -3$ or $D = -4$.

If $D = -3$ and the formula above is divisible by 3 then $\epsilon = \frac{1}{3}$. If $D = -4$ and the formula above is divisible by 2 then $\epsilon = \frac{1}{2}$.

Theorem 2.15 (Halter-Koch). *If n is the number of prime divisors of $D\mathfrak{f}$ then:*

$$|C\ell(\mathcal{O})[2]| = \begin{cases} 2^{n-1} & D\mathfrak{f} \text{ odd} \\ 2^{n-2} & 2||D\mathfrak{f} \\ 2^{n-1} & 4||D\mathfrak{f} \\ 2^{n-1} & 8||D\mathfrak{f} \\ 2^{n} & 16|D\mathfrak{f} \end{cases}.$$

More precisely, the ring class field of $\mathcal{O}$ contains:

$$\mathbb{Q}\left(\sqrt{(-1)^{(q-1)/2}q}\right)$$

where q is an odd prime factor of $D\mathfrak{f}$.

If $D = -8m$ then the ring class field of $\mathcal{O}$ contains:

$$\mathbb{Q}\left(\sqrt{(-1)^{(m-1)/2}2}\right).$$

If $D = 4 \pmod 8$ and $4|\mathfrak{f}$ then the ring class field of $\mathcal{O}$ contains:

$$\mathbb{Q}\left(\sqrt{2}\right).$$

If D is odd, and $8|\mathfrak{f}$ then the ring class field of $\mathcal{O}$ contains:

$$\mathbb{Q}\left(\sqrt{2}\right).$$

If $D = 4 \pmod 8$, or $2|\mathfrak{f}$ and $2|D$, or D is odd and $4|\mathfrak{f}$ then the ring class field of $\mathcal{O}$ contains:

$$\mathbb{Q}\left(\sqrt{-1}\right).$$

The above fields generate the genus field F, moreover, this is thee maximal subextension of the ring class field of $\mathcal{O}$ generated by quadratic extensions.

See [Sch10, Thm 6.1.4].

3. Results

In this section we will present our main theorems. These are primarily structured so as to explain patterns noticed in tabulations of these values.

We will begin by looking at certain conditions on $\mathcal{O}$ under which there can be no elliptic curves over $\mathbb{Z}_p$ which admit CM by $\mathcal{O}$. These first results can naturally be viewed as generalizations of those of [Mor14] and [Sta12] which can be interpreted as giving the conditions on the odd prime factors of the discriminants.

Theorem 3.1. *Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z}+\mathfrak{f}\mathcal{O}_K$ of conductor $\mathfrak{f} \in \mathbb{Z}$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. There are no elliptic curves over $\mathbb{Z}_p$ which admit CM by $\mathcal{O}$ if any of the following occur:*

- *there is an odd prime factor q of $D\mathfrak{f}$ with $\left(\dfrac{-p}{q}\right) = -1$*
- *$p = 1 \pmod 4$ and $16|D\mathfrak{f}^2$.*
- *$p = 3 \pmod 8$ and $8|D$.*
- *$p = 3 \pmod 8$ and $64|D\mathfrak{f}^2$*

Otherwise there are exactly $|C\ell(\mathcal{O})[2]|$ j-invariants for elliptic curves over $\mathbb{Z}_p$ which admit CM by $\mathcal{O}$.

Remark 3.2. The condition that there is an odd prime factor q of D with $\left(\frac{-p}{q}\right) = -1$ implies in particular that the quaternion algebra $(-p, -D)$ is ramified at q. Though this can be used to justify the condition for those $q|D$, we will not follow this strategy of proof, rather we give a proof which has a more natural connection to class field theory.

The condition on odd primes cannot be extended to even primes by use of the Kronecker symbol, the dependence on the behaviour at 2 is more subtle.

In order to prove the result we shall make use of a few lemmas.

Lemma 3.3. *Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. The polynomial $P_{\mathcal{O}}(X)$ has a linear factor over $\mathbb{Z}_p$ if and only if $N = \mathbb{Q}(j(\mathcal{O}))$ has no quadratic subextension in which p is inert.*

Proof. If there is a quadratic subextension of N which is inert at p, then all factors of p in N have inertial degree 2, and thus there can be no linear factors.

Conversely, suppose every factor of p in N has inertial degree 2. let $\mathfrak{p}$ be a prime of L over p and let σ be a generator for the decomposition group of $\mathfrak{p}$ and let τ be a generator of $\mathrm{Gal}(L/N)$. Then

- σ is 2-indivisible ($\sigma \neq x \cdot x$ for any x) with exact order 2, because this is true of Frob_p.
- σ and τ are not conjugate, since if τ were a conjugate of Frob_p the field $N = L^\tau$ would have a non-inert prime.
- σ and τ commute since σ has order 2.
- $\sigma\tau$ is in $\mathrm{Gal}(L/K)$ as they both act non-trivially on K.
- It follows from the above, and the basic structure of dihedral groups, that $\sigma\tau$ is indivisible with exact order 2.

Thus we may write:

$$\mathrm{Gal}(L/K) = \langle \sigma\tau \rangle \times H$$

and thus

$$\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle \times (H \rtimes \langle \tau \rangle).$$

We see that $G = (H \rtimes \langle \tau \rangle)$ is a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, moreover, the field L^G is an inert quadratic subextension of N. ∎

Lemma 3.4. *The maximal subextension of N generated by quadratic extensions is the totally real subfield M of F the genus field of L.*

Proof. It suffices to show that N has a real embedding since any composite of quadratic extensions is either totally complex or totally real.

To see this we use the fact that:

$$\overline{j(\mathfrak{a})} = j(\overline{\mathfrak{a}}).$$

It is thus sufficient to find $\mathfrak{a}$ such that $\overline{\mathfrak{a}} = \mathfrak{a}$, but indeed we may simply take $\mathfrak{a} = \mathcal{O}$. ∎

Proof of Theorem 3.1. The idea of the proof is to show that p is inert in a quadratic subextension of the totally real subfield N of F if and only if one of the conditions of the theorem holds.

To show this we must find a subextension of N defined by adjoining the square root of a positive integer which is not a square modulo p, in each of the following cases we describe how to find such a non-square. Note that if $q = 3 \pmod 4$ then $\sqrt{Dq} \in N$ whereas if $q = 1 \pmod 4$ then $\sqrt{q} \in N$.

- Consider the case where $p = 1 \pmod 4$ and $4||D$. In this case there exists odd prime factor q' of D with $\left(\frac{-p}{q'}\right) = -1$. Moreover, D has a factor q such that both $\pm q$ are not squares mod p.
- Suppose there is an odd prime factor q of $D\mathfrak{f}$ with $\left(\frac{-p}{q}\right) = -1$.
  - if $q = p = 3 \pmod 4$ we obtain $\left(\frac{q}{p}\right) = -1$ and thus Dq is not a square mod p.
  - if $q = 3 \pmod 4$, $p = 1 \pmod 4$ and $2 \nmid D$ we obtain $\left(\frac{q}{p}\right) = 1$ and thus Dq is not a square mod p.
  - if $q = 1 \pmod 4$ we obtain $\left(\frac{q}{p}\right) = -1$ and thus q and is not a square mod p.
- Suppose $p = 3 \pmod 8$ and $8|D$ and $D/8 = 3 \pmod 4$ then D has a factor d congruent to $3 \pmod 4$ which is not a square mod p.
- Suppose $p = 3 \pmod 8$ and $8|D$ and $D/8 = 1 \pmod 4$ then 2 is not a square mod p.
- Suppose $p = 3 \pmod 8$ and $64|D\mathfrak{f}^2$ then 2 is not a square mod p.
- Suppose $p = 1 \pmod 4$ and $16|D\mathfrak{f}^2$ then D has a factor q such that both $\pm q$ are not square mod p.

The above covers all of the cases of the theorem.

To prove the converse we remark that if p is inert in N it is inert in a quadratic subextension of one of the following types:

- $\mathbb{Q}(\sqrt{q})$ where $q|fD$ or
- $\mathbb{Q}(\sqrt{q_1 q_2})$ where both $q_1, q_2 = 3 \pmod 4$ and $q_1 q_2 | fD$.

as such fields generate the genus field of N. Completing the proof follows a similar case analysis to the above. ■

We now shift to discussing a phenomenon whereby certain $\mathbb{F}_p$ reductions are disallowed based on the ramification behavior of 2.

Remark 3.5. In the following theorem we will be distinguishing the supersingular j-invariants in $\mathbb{F}_p$ by identifying them as roots of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ or $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.

To understand the significance we recall the theorems above of Ibukiyama which asserted that this naturally divides the supersingular values into two almost

disjoint sets. More precisely, by [Elk87] and [Kan89] we have that for $p = 3 \pmod 4$ these polynomials factor as $(X - 1728)\prod_i (X - \alpha_i)^2$ whereas for $p = 1 \pmod 4$ the factorization is $\prod_i (X - \alpha_i)^2$. In each case the α_i are distinct in $\mathbb{F}_p$. Furthermore, in the case $p = 3 \pmod 4$ the α_i for $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ are distinct from those for $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$. The polynomial for $\sqrt{-2}$ is precisely $P_{\mathbb{Z}[\sqrt{-2}]}(X) = X - 8000$.

Theorem 3.6. *Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ of conductor $\mathfrak{f} \in \mathbb{Z}$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. Let j be a $\mathbb{Z}_p$ root of $P_{\mathcal{O}}(X)$.*

- *Suppose $p = 7 \pmod 8$*
  - *If 2 is unramified in K and $2 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$.*
  - *If 2 is unramified in K and $2|\mathfrak{f}$ but $8 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is unramified in K and $8|\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ or $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is tamely ramified in K and $2 \nmid \mathfrak{f}$ or $4|\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ or $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is tamely ramified in K and $2||\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is wildly ramified in K and $2 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is wildly ramified in K and $2|\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ or $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
- *Suppose $p = 3 \pmod 8$*
  - *If 2 is unramified in K and $2 \nmid \mathfrak{f}$ or $4||\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$.*
  - *If 2 is unramified in K and $2||\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is unramified in K and $8|\mathfrak{f}$ then there are no linear terms.*
  - *If 2 is tamely ramified in K and $2 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$ or $P_{\mathbb{Z}[(1+\sqrt{-p})/2]}(X)$.*
  - *If 2 is tamely ramified in K and $2||\mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$.*
  - *If 2 is tamely ramified in K and $4|\mathfrak{f}$ then there are no linear terms.*
  - *If 2 is wildly ramified in K then there are no linear terms.*
- *Suppose $p = 1 \pmod 4$*
  - *If 2 is unramified in K and $4 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$.*
  - *If 2 is unramified in K and $4|\mathfrak{f}$ then there are no linear terms.*
  - *If 2 is tamely ramified then there are no linear terms.*
  - *If 2 is wildly ramified in K and $2 \nmid \mathfrak{f}$ then j is a root of $P_{\mathbb{Z}[\sqrt{-p}]}(X)$.*
  - *If 2 is wildly ramified in K and $2|\mathfrak{f}$ then there are no linear terms.*

Notation 3.7. Given that any quaternion algebra A is equipped with a canonical bilinear form, given an element $\alpha \in A$ we shall denote by $\alpha^\perp$ the collection of all elements in A perpendicular to α, that is elements $x \in A$ with $\mathrm{Tr}(\alpha x) = 0$.

Similarly, given a subspace such as $\mathcal{O} \subset A$, we shall denote $\mathcal{O}^\perp$, the complementary subspace of A with respect to this pairing.

To prove this we will make use of the following lemma.

Lemma 3.8. *If E is an elliptic curve over $\mathbb{Z}_p$ which admits CM by $\mathcal{O}$ which corresponds to a datum $(\mathcal{O} \subset \mathbb{B})$ then the Galois Frobenius Frob_p acting on $E(\overline{\mathbb{Q}}_p)$ over $\mathbb{Z}_p$ induces the endomorphism Frobenius $\widetilde{\mathrm{Frob}_p}$ of $\overline{E}$. Moreover we have:*

- *Frob_p, the Galois action of Frobenius on E, acts on $\mathcal{O}$ by $x \mapsto \overline{x}$.*
- *$\widetilde{\mathrm{Frob}_p}$, the endomorphism of $\overline{E}$, satisfies $\widetilde{\mathrm{Frob}_p} x = \overline{x} \widetilde{\mathrm{Frob}_p}$ for $x \in \mathcal{O}$.*
- *Frob_p^2, the Galois action of Frobenius on E, commutes with $\mathcal{O}$.*
- *$\widetilde{\mathrm{Frob}_p}^2$, the endomorphism of $\overline{E}$, satisfies $\widetilde{\mathrm{Frob}_p}^2 = -p$.*

In particular $\widetilde{\mathrm{Frob}_p} \in \mathcal{O}^\perp$ is an element of norm p.

See [Sch10].

Proof of Theorem 3.6. We must show, using Ibukiyama's classification of maximal orders containing $\sqrt{-p}$, that the only CM-orders in $\alpha^\perp$ are those satisfying the conditions of the theorem.

We note that in selecting the values of q, r and m we may assume by replacing r by $r + aq$ that $8|r$. With this assumption we have that $pq = m \pmod 8$. When selecting q, r' and m' we must have that r' is odd, when $p = 3 \pmod 8$ this then implies that m is odd.

We observe the following important facts about $\alpha^\perp$ in the various cases:

1. For the maximal orders of the form $O'(p, q, r', m')$ we have that $\alpha^\perp$ contains no elements with odd trace.
2. For the maximal orders of the form $O'(p, q, r', m')$ we have that all primitive elements of $\mathbb{Z}[\sqrt{-p}]^\perp$ are of the form:

$$y\beta + z\frac{(r' + \alpha)\beta}{2q}$$

for some choice of y and z coprime.
The square of such an element is:

$$-y^2 q - z^2 m - yzr'.$$

Notice that if $p = 3 \pmod 8$ this cannot be even.
3. For the maximal orders of the form $O(p, q, r, m)$ we have that all primitive elements of odd trace in $\mathbb{Z}[\sqrt{-p}]^\perp$ are of the form:

$$y\beta + z\frac{(r + \alpha)\beta}{q}$$

for some choice of y and z coprime, with z odd.
The square of such an element is:

$$-y^2q - z^2m - 2yzr$$

modulo 8 this becomes:

$$-q(y^2 - z^2p).$$

Notice that if this is odd, then y is even and $-q(y^2-z^2p) = pq \pmod 8$. Also, if it is even then y and z are both odd and it is divisible by $(1-p)|-q(y^2-z^2p)$.

By considering each of the cases of the theorem, the above allows us to conclude the result. ■

Proposition 3.9. *Suppose there exists $\mathbb{Z}[\sqrt{-D}] = \mathcal{O} \subset \alpha^\perp$, then $P_{\mathcal{O}}(X)$ has $\mathbb{Z}_p$ roots.*

Proof. By the above argument we note that $\mathcal{O} \subset \alpha^\perp$ implies the existence of a solution to:

$$y^2q + z^2m + 2yzr = D \qquad \text{or} \qquad y^2q + z^2m + yzr' = D.$$

In the first case, multiplying by q we obtain:

$$qD = y^2q^2 + z^2(p + r^2) + 2yzrq = z^2p + (yq + rz)^2.$$

reducing modulo 8 and modulo all the odd prime factors of D the result then follows from Theorem 3.1. In the second case, multiplying by $4q$ we obtain:

$$4qD = 4y^2q^2 + z^2(p + r^2) + 2yzrq = z^2p + (2yq + rz)^2$$

and the result follows similarly. ■

Remark 3.10. Note that the above does not actually prove the converse to Lemma 3.8 though it would provide for an alternate proof for one direction of Theorem 3.1.

We now explain the phenomenon where in specific circumstances certain $\mathbb{F}_p$ reductions always occur with the same frequency. Based on [CV07] we should expect that this is caused by systematic collections of isogenies (coming from Hecke relations), and in our case we should expect 2-isogenies to play a role. The results here have a similar flavor to those of [BM04, pp. 95-96] where they consider similar questions questions related to the orders $\mathbb{Z}[\sqrt{-p}]$ and $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$.

Lemma 3.11. *If $\sqrt{q_2} \in \alpha^\perp$ then $\mathcal{O} \simeq O(p, q_2, r, m)$ or $O(p, q_2, r', m')$ for some choice of r, m or r', m'.*

Proof. By [Ibu82, Prop 2.1 and Rmk 2.2] the conditions:

$$q_1q_2 = z^2p + (yq_1 + rz)^2 \qquad \text{or} \qquad 4q_1q_2 = z^2p + (2yq_1 + rz)^2$$

imply that q_1 and q_2 satisfy

$$O(p, q_1, r_1, m_1) \simeq O(p, q_2, r_2, m_2)$$

or respectively

$$O'(p, q_1, r_1', m_1') \simeq O'(p, q_2, r_2', m_2').$$

The results then follow from the proof of Proposition 3.9. ∎

Lemma 3.12. *Fix $p = 3 \pmod 4$. Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. Suppose further that 2 is tamely ramified in K but 2 does not divide $\mathfrak{f}$.*

Suppose that $\mathcal{O}$ is optimally embedded in $O(p, q, r, m)$ and contained in $\alpha^\perp$. Let $\mathfrak{a}^2 = (2)$ in $\mathcal{O}$. Then $\mathfrak{a}O(p, q, r, m)\mathfrak{a}^{-1} \simeq O'(p, q, r', m')$ is a maximal order with an optimal embedding of $\mathcal{O}$. Consequently, if E is an elliptic curve over $\mathbb{Z}_p$ which admits CM by $\mathcal{O}$ whose reduction has endomorphism ring $O(p, q, r, m)$, then the reduction of $\mathfrak{a} * E$ has endomorphism ring $O'(p, q, r', m')$ with the exact same choice of q.

Conversely, if E is an elliptic curve over $\mathbb{Z}_p$ which admits CM by $\mathcal{O}$ whose reduction has endomorphism ring $O'(p, q, r', m')$, then the reduction of $\mathfrak{a}*E$ has endomorphism ring $O(p, \tilde{q}, \tilde{r}, \tilde{m})$ for some $\tilde{q}$ such that $O'(p, q, r', m') \simeq O'(p, \tilde{q}, \tilde{r}', \tilde{m}')$.

Proof. Let $\mathcal{O} = \mathbb{Z}[\gamma = \sqrt{q_2}]$. It suffices to show that $\mathfrak{a}O(p, q, r, m)\mathfrak{a}^{-1}$ contains both $\frac{1+\alpha}{2}$ and β.

We note that $\mathfrak{a} = (2, 1 + \gamma)$ and $\mathfrak{a}^{-1} = (1, \frac{1-\gamma}{2})$. It follows immediately that $\beta \in \mathfrak{a}O(p, q_1, r, m)\mathfrak{a}^{-1}$.

Now we may write $\gamma = y\beta + z\frac{r+\alpha}{q}\beta$ with y and r even and z odd. Now, by observing that we may write $\left(\frac{1+\alpha}{2}\right)$ as:

$$(1+\gamma)\left(\tfrac{1}{2}(-zm + ry + 1) + (zm + ry)\left(\frac{1+\beta}{2}\right) - \tfrac{1}{2}(yq + zr)\left(\frac{r+\alpha}{q}\beta\right)\right)\left(\frac{1-\gamma}{2}\right)$$

and that this quantity is an element of $\mathfrak{a}O(p, q, r, m)\mathfrak{a}^{-1}$ we conclude by Lemma 3.11 that

$$\mathfrak{a}O(p, q, r, m)\mathfrak{a}^{-1} \simeq O'(p, q, r', m').$$

Now suppose we start with $\mathcal{O}$ optimal in $O'(p, q, r', m')$. Attempting to reverse the above calculation cannot work in general as we no longer have r and m but r' and m'. However, we observe that:

$$\left((1+\gamma)\left(\frac{1+\alpha}{2}\right)\left(\frac{1-\gamma}{2}\right) - \left(\frac{1+\gamma^2}{4}\right)\alpha\right) \in \mathfrak{a}O'(p, q, r', m')\mathfrak{a}^{-1}$$

is perpendicular to α and has odd trace. Hence, $\mathfrak{a}O'(p, q, r', m')\mathfrak{a}^{-1} \simeq O(p, \tilde{q}, \tilde{r}, \tilde{m})$. The result now follows. ∎

Remark 3.13. Note, that we could not simply run the first part of the above argument in the opposite direction to go from $O'(p,q,r',m')$ to $O(p,q,r,m)$, in particular this would be impossible in any case where the class groups which classify $O'(p,q,r',m')$ and $O(p,q,r,m)$ are not in bijection.

Theorem 3.14. *Fix $p = 3 \pmod 4$. Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. Suppose further that 2 is tamely ramified in K but 2 does not divide $\mathfrak{f}$.*

It we consider the set of supersingular values of $\mathbb{F}_p$ except 1728, each j-invariant J has a partner $\tilde{J}$ such that, the frequency of the appearance of $X - J$ and $X - \tilde{J}$ as the reduction of irreducible linear factors of $P_{\mathcal{O}}(X)$ modulo p is the same.

Proof. We first observe that if E is defined over $\mathbb{Z}_p$ then so too is $\mathfrak{a} * E$. This follows by observing that the collection of endomorphisms in $\mathfrak{a}$ is Galois stable. Moreover, in the case $p = 3 \pmod 4$ the map from $O(p,q,r,m)$ to $O'(p,q,r',m')$ being injective implies it is bijective as the collections have the same size.

By Lemma 3.12 it now follows that $O(p,q,r,m)$ and $O'(p,q,r',m')$ must occur with the same frequency.

We note that j-invariant 1728 is the only one that can ever be identified with itself through this process, and in fact it must, because the class group has odd order. ∎

Remark 3.15. For $p = 3 \pmod 4$ we obtain other less obvious relationships between the counts for maximal orders of type O' and of type O arising from the fact that the map is generically $3:1$. In particular, in general the frequency for those of type O' is the sum of the frequencies of a specific collection of three of orders of type O. We note that there will be a curve which is 2-isogenous to the one with j-invariant 1728.

We should point out that the $\mathbb{F}_p$ points of the 2-torsion is well understood, that there is a unique $\mathbb{F}_p$ rational 2-torsion point is suggestive of the above results, but does not show that the association is between $O(p,q,r,m)$ and $O'(p,q,r',m')$ and certainly not that it 'respects q'.

Theorem 3.16. *Fix $p = 1 \pmod 4$. Fix $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. Fix an order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ and suppose that $\left(\frac{-D\mathfrak{f}^2}{p}\right) = -1$. Suppose further that 2 is wildly ramified in K but 2 does not divide $\mathfrak{f}$.*

It we consider the set of supersingular values of $\mathbb{F}_p$, each j-invariant J has a partner $\tilde{J}$ such that, the frequency of the appearance of $X - J$ and $X - \tilde{J}$ as the reduction of irreducible linear factors of $P_{\mathcal{O}}(X)$ modulo p is the same.

This partner $\tilde{J}$ is independent of K and $\mathcal{O}$ and depends only on p.

Proof. Set $\mathfrak{a}^2 = (2)$ in $\mathcal{O}$. In this case we have $\mathfrak{a} = (2, \gamma)$ and $\mathfrak{a}^{-1} = (1, \frac{1}{2}\overline{\gamma})$. As in the previous case, we must only show that $\mathfrak{a}O(p,q,r,m)\mathfrak{a}^{-1}$ is independent of $\mathcal{O}$.

Now set $\mathfrak{b}^2 = (2)$ in $\mathbb{Z}[\sqrt{-p}]$. We have that $\mathfrak{b} = (2, 1 + \alpha)$.

We recall that we have $\gamma = y\beta + z\frac{r+\alpha}{q}\beta = \frac{1}{q}(yq + zr + z\alpha)\beta$ with r even and both y and z odd.

We claim that $(1+\alpha) \in \mathfrak{a}O(p,q,r,m)$. Indeed, as $\beta \in O(p,q,r,m)$ we have $yq + zr + z\alpha = \gamma\beta \in \mathfrak{a}O(p,q,r,m)$. Since $2 \in \mathfrak{a}$ the claim then follows immediately. Conversely, it is clear that $q\gamma \in \mathfrak{b}O(p,q,r,m)$. As q is odd, and $2 \in \mathfrak{b}$ we also have that $\gamma \in \mathfrak{b}O(p,q,r,m)$. We thus have shown that $\mathfrak{a}O(p,q,r,m) = \mathfrak{b}O(p,q,r,m)$.

It follows that $\mathfrak{a}O(p,q,r,m)\mathfrak{a}^{-1} = \mathfrak{b}O(p,q,r,m)\mathfrak{b}^{-1}$ is independent of $\mathcal{O}$. ■

Remark 3.17. In this case the uniqueness of the $\mathbb{F}_p$-rational 2-torsion points is sufficient to conclude the result.

4. Further questions

Our results suggest the following natural questions:

Question 1. In Theorem 3.6 we gave necessary conditions for a datum $(\mathcal{O} \subset \mathbb{B})$ to correspond to an elliptic curve over $\mathbb{Z}_p$. Moreover, Proposition 3.9 gives the impression that this may be sufficient. It is natural to ask, if these conditions are in fact sufficient.

(a) More precisely, given an elliptic curve over $\mathbb{F}_p$, and an endomorphism (defined over some extension) when can we lift the curve to $\mathbb{Z}_p$ such that the endomorphism lifts to some extension?
(b) Is it sufficient that the endomorphism be perpendicular to Frobenious in the endomorphism algebra over $\overline{\mathbb{F}_p}$?

An answer to this question would shed light on the structure of the ring $\mathbb{Z}[j(E_1), \ldots, j(E_n)]$ as remarked in the introduction.

Question 2. Theorems 3.14 and 3.16 give situations in which there are automatic relationships between certain roots of $P_{\mathcal{O}}(X)$. As remarked a similar result holds for the same reason when $p = 3 \pmod 8$.

(a) It is natural to ask if there are other situations in such relationships must exist? In particular are there situations where the role of 2 can be replaced by some other prime?
(b) The method of proof also suggests that we could anticipate relations between the roots of $P_{\mathcal{O}}(X)$ between two different orders in the same field whose conductors differ by a factor of 2. Can the combinatorics of this be made more precise?

Acknowledgements. I would like to thank Prof. Eyal Goren for suggesting the computations which led to the discovery of these results. I would like to thank Prof. Ernst Kani for some useful discussions as well as recommending several references. I would like to thank the referee, for their numerous helpful suggestions. I would like to thank the many developers of SAGE without which the computations through which we uncovered these results would not be possible. I would also like to thank the SAGE Notebook project for the use of various computing resources which they have made available through their various funding sources.

References

[BM04] J. Brillhart and P. Morton, *Class numbers of quadratic fields, hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106** (2004), no. 1, 79–111.

[CV05] C. Cornut and V. Vatsal, *CM points and quaternion algebras*, Doc. Math. **10** (2005), 263–309.

[CV07] C. Cornut and V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186.

[Deu41] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), no. 1, 197–272.

[Dor89] D.R. Dorman, *Global orders in definite quaternion algebras as endomorphism rings for reduced cm elliptic curves*, Théorie des nombres (Quebec, PQ, 1987) (1989), 108–116.

[Elk87] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Inventiones mathematicae **89** (1987), no. 3, 561–567.

[Ibu82] T. Ibukiyama, *On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings*, Nagoya Math. J. **88** (1982), 181–195.

[JK11] D. Jetchev and Ben Kane, *Equidistribution of Heegner points and ternary quadratic forms*, Math. Ann. **350** (2011), no. 3, 501–532.

[Kan89] M. Kaneko, *Supersingular j-invariants as singular moduli* $\bmod p$, Osaka J. Math. **26** (1989), no. 4, 849–855.

[LV15] K. Lauter and B. Viray, *An arithmetic intersection formula for denominators of igusa class polynomials*, Amer. J. Math. **137** (2015), no. 2, 497–533.

[Mor14] P. Morton, *Genus theory and the factorization of class equations over* $\mathbb{F}\_p$, ArXiv e-prints (2014).

[Sch10] R. Schertz, *Complex multiplication*, New Mathematical Monographs, vol. 15, Cambridge University Press, Cambridge, 2010.

[Sta12] J. Stankewicz, *Twists of Shimura Curves*, ArXiv e-prints (2012).

Address: Andrew Fiori: Mathematics & Statistics, 612 Campus Place N.W., University of Calgary, 2500 University Drive NW, Calgary, AB, Canada T2N 1N4.

E-mail: andrew.fiori@ucalgary.ca

Received: 31 August 2015; **revised:** 26 July 2016