

# Constructing supersingular elliptic curves with a given endomorphism ring

Ilya Chevyrev and Steven D. Galbraith

## ABSTRACT

Let  $\mathcal{O}$  be a maximal order in the quaternion algebra  $B_p$  over  $\mathbb{Q}$  ramified at  $p$  and  $\infty$ . The paper is about the computational problem: construct a supersingular elliptic curve  $E$  over  $\mathbb{F}_p$  such that  $\text{End}(E) \cong \mathcal{O}$ . We present an algorithm that solves this problem by taking gcds of the reductions modulo  $p$  of Hilbert class polynomials.

New theoretical results are required to determine the complexity of our algorithm. Our main result is that, under certain conditions on a rank three sublattice  $\mathcal{O}^T$  of  $\mathcal{O}$ , the order  $\mathcal{O}$  is effectively characterized by the three successive minima and two other short vectors of  $\mathcal{O}^T$ . The desired conditions turn out to hold whenever the  $j$ -invariant  $j(E)$ , of the elliptic curve with  $\text{End}(E) \cong \mathcal{O}$ , lies in  $\mathbb{F}_p$ . We can then prove that our algorithm terminates with running time  $O(p^{1+\varepsilon})$  under the aforementioned conditions.

As a further application we present an algorithm to simultaneously match all maximal order types with their associated  $j$ -invariants. Our algorithm has running time  $O(p^{2.5+\varepsilon})$  operations and is more efficient than Cerviño's algorithm for the same problem.

## 1. Introduction

Let  $p$  be a prime and  $E$  a supersingular elliptic curve over  $\mathbb{F}_{p^2}$ . Then  $\text{End}(E)$  is a maximal order in the quaternion algebra  $B_p$  ramified exactly at  $p$  and  $\infty$  (all notation and definitions are explained in §2). A special case of interest is when  $E$  is defined over  $\mathbb{F}_p$ , in which case  $\text{End}(E)$  contains an element  $\pi$  such that  $\pi^2 = -p$  (the Frobenius). Supersingular elliptic curves have a number of algorithmic applications [5, 20].

Ibukiyama [11] has given an explicit description of all maximal orders in  $B_p$  that contain  $\sqrt{-p}$ . For example, let  $p \equiv 1 \pmod{4}$  and let  $\mathcal{O}$  be such a maximal order in  $B_p$ . Then there is a prime  $q \equiv 3 \pmod{8}$  such that  $(-q/p) = -1$ , and a  $\mathbb{Q}$ -algebra isomorphism  $\phi : B_p \rightarrow \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$  where  $i^2 = -p$ ,  $j^2 = -q$  and  $k = ij = -ji$ , such that  $\phi(\mathcal{O}) \cong \mathbb{Z} + \mathbb{Z}(1+j)/2 + \mathbb{Z}(i+k)/2 + \mathbb{Z}(rj+k)/q$  where  $r$  is any integer such that  $q \mid (r^2 + p)$ .

Consider the  $\mathbb{Z}$ -module  $\mathcal{O}^T = \{2x - \text{Tr}(x) \mid x \in \mathcal{O}\}$  of rank 3 (we discuss this object in greater detail in §3). Note that  $y \in \mathcal{O}^T$  implies  $\text{Tr}(y) = 0$  and so  $\mathcal{O}^T$  is a subset of the pure quaternions. Fix a  $\mathbb{Z}$ -module basis  $\{\omega_1, \omega_2, \omega_3\}$  for  $\mathcal{O}^T$  and consider the ternary quadratic form  $Q(x, y, z) = \text{Nr}(x\omega_1 + y\omega_2 + z\omega_3)$  giving a norm on  $\mathcal{O}^T$ . Kaneko [13] has shown, in the special case where  $\sqrt{-p} \in \mathcal{O}$ , that there is an element  $x \in \mathcal{O}^T$  of norm at most  $4\sqrt{p}/\sqrt{3}$ .

Let  $\mathcal{O}'$  be another maximal order in the same quaternion algebra  $B_p$  and let  $Q'$  be the ternary form associated with  $\mathcal{O}'$ . A natural question is whether  $Q$  determines  $\mathcal{O}$ . In other words, if  $Q'$  is equivalent to  $Q$  in the sense of quadratic forms then is  $\mathcal{O}'$  isomorphic to  $\mathcal{O}$ ? We will show that this is the case. Indeed, our main result (Theorem 2.2) is much stronger: it states that if the forms  $Q$  and  $Q'$  are such that  $Q'$  represents the successive minima of  $Q$  (which is not the same as saying that the forms have the same successive minima), plus some other mild conditions, then  $\mathcal{O} \cong \mathcal{O}'$ , and hence  $Q$  and  $Q'$  are equivalent. Schiemann [16] has shown that

---

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G20, 11Y16, 11R52, 11E20, 11H55 (primary), 14G15 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

two ternary quadratic forms are determined up to equivalence by their theta series. Our result may be viewed as a strong form of Schiemann's theorem in the case where both forms arise from maximal orders in the same quaternion algebra.

Our work is motivated by several computational questions about supersingular elliptic curves. One problem is, given a maximal order  $\mathcal{O}$  in  $B_p$ , to compute an elliptic curve  $E$  over  $\mathbb{F}_{p^2}$  such that  $\text{End}(E) \cong \mathcal{O}$ . A second problem is to compute a list of all isomorphism classes of supersingular elliptic curves  $E$  over  $\mathbb{F}_{p^2}$  (or over  $\mathbb{F}_p$  in a restricted case) together with a description of  $\text{End}(E)$ . To solve both problems we use Hilbert class polynomials. The main idea is that if  $\mathcal{O} \cong \text{End}(E)$  and if  $\mathcal{O}^T$  has an element of small norm  $d$  then  $E$  has a 'complex multiplication' of degree  $d$  and so  $j(E)$  is a root of the Hilbert class polynomial  $H_{-d}(x)$ . The first problem does not seem to have been considered in the literature previously. Cerviño [4] has given an algorithm to solve the second problem that seems to run in  $O(p^{3+\varepsilon})$  operations (or  $O(p^{2.5+\varepsilon})$  in the restricted case over  $\mathbb{F}_p$ ); our approach leads to a superior running time of  $O(p^{2.5+\varepsilon})$  operations (or  $O(p^{1.5+\varepsilon})$  in the restricted case).

## 2. Background and main results

Let  $B_p$  be the quaternion algebra over  $\mathbb{Q}$  ramified exactly at  $p$  and at  $\infty$ . A general reference for many of the facts in this section is Vignéras [21]. We recall that  $B_p$  is a four-dimensional division  $\mathbb{Q}$ -algebra containing  $\mathbb{Q}$  with an anti-involution  $x \mapsto \bar{x}$ . Define the reduced trace  $\text{Tr}(x) = x + \bar{x}$ . Then  $B_p$  is equipped with the symmetric positive-definite bilinear form  $\text{Tr}(x\bar{y})$  and the associated positive-definite quadratic form  $\text{Nr}(x) = x\bar{x}$ . Every element  $x \in B_p$  satisfies its characteristic equation  $x^2 - \text{Tr}(x)x + \text{Nr}(x) = 0$ . We define  $B_p^0$  to be the subring of  $B_p$  of elements of zero trace.

We let  $\mathcal{O}$  and  $\mathcal{O}'$  be orders of  $B_p$ . We recall that an *order* of  $B_p$  is a subring of  $B_p$  that contains  $\mathbb{Z}$  and has four linearly independent generators as a  $\mathbb{Z}$ -module. We recall furthermore that for all  $x \in \mathcal{O}$ , we have  $\text{Tr}(x), \text{Nr}(x) \in \mathbb{Z}$ . Finally, we say that  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same *type* if there exists non-zero  $c \in B_p$  such that  $c\mathcal{O}c^{-1} = \mathcal{O}'$ , in which case we write  $\mathcal{O} \sim \mathcal{O}'$ .

An order  $\mathcal{O}$  of  $B_p$  is called *maximal* if it is not properly contained in any other order. Deuring showed that, associated to a maximal order  $\mathcal{O}$ , there exists either one supersingular  $j$ -invariant  $j(\mathcal{O}) \in \mathbb{F}_p$ , or a conjugate pair  $j(\mathcal{O}), \bar{j}(\mathcal{O}) \in \mathbb{F}_{p^2}$ , such that  $\text{End}(E(j(\mathcal{O}))) = \text{End}(E(\bar{j}(\mathcal{O}))) = \mathcal{O}$ , where  $E(j)$  is the unique (up to isomorphism) elliptic curve with  $j$ -invariant  $j$ . We let the total number of maximal order types be  $t_p$ , the *type number* of  $B_p$ .

If  $\#\mathcal{O}^* > 2$  then  $j(\mathcal{O}) \in \{0, 1728\}$  and the problems considered in the paper are all straightforward. More precisely,  $j(\mathcal{O}) = 0$  if and only if there are units of (multiplicative) order 3 and 6, and  $j(\mathcal{O}) = 1728$  if and only if there is a unit of order 4. Hence, unless otherwise stated, we assume that  $\#\mathcal{O}^* = 2$ .

Let  $V$  be any vector space over  $\mathbb{Q}$  with a positive-definite quadratic form  $\text{Nr}$ . For arbitrary vectors  $v_1, v_2, \dots, v_n \in V$ , we denote by

$$\Lambda = \langle v_1, v_2, \dots, v_n \rangle := \{a_1v_1 + a_2v_2 + \dots + a_nv_n \mid a_1, a_2, \dots, a_n \in \mathbb{Z}\}$$

the standard lattice generated by these vectors.

We say that a non-zero lattice element  $x \in \Lambda$  is *primitive* if there do not exist  $y \in \Lambda$  and  $a \in \mathbb{Z}$  such that  $ay = x$  and  $a \neq \pm 1$ . If  $x = a_1v_1 + \dots + a_nv_n$ , then  $x$  is primitive if and only if  $\text{gcd}(a_1, \dots, a_n) = 1$ . We also say that an integer  $k$  is *represented* by  $\Lambda$  if there exists  $x \in \Lambda$  such that  $\text{Nr}(x) = k$ , in which case we also say that  $x$  *represents*  $k$ . Furthermore, we say that  $x$  *optimally represents*  $k$  if  $x$  is primitive.

If  $k \neq 0$ , we say that  $k$  is represented by  $\Lambda$  with *multiplicity*  $\theta_\Lambda(k)$ , where

$$\theta_\Lambda(k) = \frac{1}{2} \#\{(a_1, \dots, a_n) \in \mathbb{Z}^n \mid \text{Nr}(a_1v_1 + \dots + a_nv_n) = k\},$$

and likewise  $k$  is represented optimally by  $\Lambda$  with *optimal multiplicity*  $\theta'_\Lambda(k)$ , where

$$\theta'_\Lambda(k) = \frac{1}{2} \#\{(a_1, \dots, a_n) \in \mathbb{Z}^n \mid \text{Nr}(a_1 v_1 + \dots + a_n v_n) = k, \text{gcd}(a_1, \dots, a_n) = 1\}.$$

The factor  $\frac{1}{2} = 1/\#\mathcal{O}^*$  is to avoid counting both  $x$  and  $-x$ , since  $\text{Nr}(x) = \text{Nr}(-x) = k$  is effectively the same representation.

Turning to the case  $V = B_p$  with the quadratic form  $\text{Nr}$ , for a lattice  $\Lambda = \langle v_1, v_2, v_3, v_4 \rangle \subset B_p$  we define its discriminant as  $D(\Lambda) = D(v_1, v_2, v_3, v_4) = |\det(\text{Tr}(v_i v_j))|$  (see [21, §I.4]). It is a standard fact that  $D(\mathcal{O}) = p^2$  for a maximal order  $\mathcal{O} \subset B_p$  (see, for example, Vignéras [21, Corollary III.5.3]). Note that  $D(\mathcal{O}) = |\det(\text{Tr}(v_i \bar{v}_j))|$ .

We will often think of  $B_p$  simply as an inner product space and forget its algebraic structure. For example, we can find a  $\mathbb{Q}$ -basis  $\{1, \tau, \rho, \tau\rho\}$  for  $B_p$  such that  $\tau^2 = -p, \rho^2 = -q$  and  $\tau\rho = -\rho\tau$ , where  $q$  is a prime such that  $q \equiv 3 \pmod{8}$  and  $(-p/q) = 1$  (see, for example, Ibukiyama [11, Lemma 1.1]). Then in particular,  $\text{Nr}(a + b\tau + c\rho + d\tau\rho) = a^2 + b^2\text{Nr}(\tau) + c^2\text{Nr}(\rho) + d^2\text{Nr}(\tau\rho)$  for  $a, b, c, d \in \mathbb{Q}$ . As such, we will embed  $B_p$  into  $\mathbb{R}^4$  by the mapping

$$\phi : a + b\tau + c\rho + d\tau\rho \mapsto ae_1 + b\sqrt{\text{Nr}(\tau)}e_2 + c\sqrt{\text{Nr}(\rho)}e_3 + d\sqrt{\text{Nr}(\tau\rho)}e_4,$$

where  $e_i$  are the usual orthonormal vectors in  $\mathbb{R}^4$ . We observe that  $\phi$  is indeed an isometry (the quadratic form on  $\mathbb{R}^4$  being understood as the square of the standard Euclidean norm). We note that this is not the only standard way to represent  $B_p$  (see, for example, Pizer [15, Proposition 5.1] for a different, but related representation). In particular, the above representation of  $B_p$  is not the one used in the two examples of §6.

For an  $n$ -dimensional lattice  $L$  in  $\mathbb{R}^m$ , let  $\det(L)$ , the determinant of  $L$ , be the square of the volume of  $L$ , that is, if  $B$  is a basis matrix for  $L$  then  $\det(L) := \det(BB^T) = \text{Vol}(L)^2$ . Notice that this is different to the more common definition of  $\det(L) = \sqrt{\det(BB^T)} = \text{Vol}(L)$ . We say that the  $n$  successive minima of  $L$  are  $D_1, D_2, \dots, D_n \in \mathbb{R}$  such that  $D_i$  is minimal such that there exist  $i$  linearly independent vectors  $v_1, v_2, \dots, v_i \in L$  with  $\|v_j\|^2 \leq D_i$  for all  $j \leq i$ , where  $\|\cdot\|$  is the standard Euclidean norm in  $\mathbb{R}^m$ . Again we remark that our definition is the square of the more common definition where  $\|v_j\| \leq D_i$  is taken instead of  $\|v_j\|^2 \leq D_i$ .

Under this notation, standard lattice bounds show that there is a minimal constant  $\gamma_n$  (called the  $n$ th Hermite constant) such that

$$\det(L) \leq \prod_{i=1}^n D_i \leq \gamma_n^n \det(L). \tag{2.1}$$

Again, this is the square of the usual equation  $\prod_i \|v_j\| \leq \gamma_n^{n/2} \text{Vol}(L)$ . It is known that  $\gamma_2^2 = \frac{4}{3}$  and  $\gamma_3^3 = 2$  (see Siegel [17, §§ XI.5 and XI.6]).

Now for any lattice  $\Lambda \subset B_p$ , the determinant, volume and successive minima of  $\Lambda$  are defined to be those of  $\phi(\Lambda) \subset \mathbb{R}^4$ , where  $\phi : B_p \mapsto \mathbb{R}^4$  is the embedding described above. We note that for a 4-dimensional lattice  $\Lambda \subset B_p$ , we have

$$D(\Lambda) = 16 \det(\phi(\Lambda)) \tag{2.2}$$

since  $\text{Tr}(x\bar{y}) = 2\phi(x)\phi(y)^T$ .

One goal of this paper is to give sufficient conditions under which the elements of small norm of a maximal order  $\mathcal{O}$  of  $B_p$  characterize its type. The first theorem is that the successive minima of the lattice  $\mathcal{O}^T$  determine the type of the order.

**THEOREM 2.1.** *Let  $\mathcal{O}$  and  $\mathcal{O}'$  be two maximal orders of  $B_p$ . Let  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  have the same successive minima  $D_1 \leq D_2 \leq D_3$ . Assume moreover that  $D_1 D_2 < 16p/3$  and that  $p$  is sufficiently large. Then  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type.*

Our main result is a stronger statement as it does not require both orders to give lattices with the same successive minima. It is this result we need later for our algorithmic application.

**THEOREM 2.2.** *Let  $p > 286$  and  $\mathcal{O}, \mathcal{O}'$  be two maximal orders of  $B_p$ . Let  $D_1, D_2$  and  $D_3$  be the successive minima of  $\mathcal{O}^T$  and let  $x, y \in \mathcal{O}^T$  be such that  $\text{Nr}(x) = D_1$  and  $\text{Nr}(y) = D_2$ . Suppose that  $D_1, D_2, \text{Nr}(x + y), \text{Nr}(x - y)$  and  $D_3$  are all represented optimally in  $\mathcal{O}'^T$  and that  $\theta'_{\mathcal{O}^T}(D_3) \leq \theta'_{\mathcal{O}'^T}(D_3)$ . Assume moreover that*

$$D_1 D_2 < \frac{16}{3} p. \tag{2.3}$$

Then  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type.

We prove Theorem 2.1 in §4 and Theorem 2.2 in the Appendix. Lemma 2.3 gives a set of cases when the condition  $D_1 D_2 < 16p/3$  holds.

**LEMMA 2.3.** *Let  $\mathcal{O}$  be a maximal order in  $B_p$  and  $D_1$  and  $D_2$  the first two successive minima of  $\mathcal{O}^T$ . If  $\mathcal{O}$  contains an element  $\pi$  such that  $\pi^2 = -p$  (or equivalently, if  $j(\mathcal{O}) \in \mathbb{F}_p$ ), then  $D_1 D_2 < 16p/3$ .*

*Proof.* When  $j(\mathcal{O}) \in \mathbb{F}_p$ , Kaneko proves (see [13, pages 851–852]) that there exists a 2-dimensional sublattice  $\Lambda$  of  $\mathcal{O}^T$  with determinant  $\det(\Lambda) = 4p$ . Let  $d_1$  and  $d_2$  be the first two successive minima of  $\Lambda$ . Using the second Hermite constant  $\gamma_2^2 = \frac{4}{3}$  in (2.1), we obtain that  $4p \leq d_1 d_2 < 16p/3$  (the second inequality is strict since  $d_1 d_2$  is an integer and the case  $p = 3$  is trivial). Finally, since  $D_i \leq d_i$  for  $i = 1, 2$ , it follows that  $D_1 D_2 < 16p/3$ .  $\square$

Elkies showed that  $D_1 \leq 2p^{2/3}$  for any maximal order in  $B_p$ . Yang [22] has shown that Elkies’ result is the best possible.

### 3. The lattice $\mathcal{O}^T$ and its properties

**DEFINITION 3.1.** For an order  $\mathcal{O} \subset B_p$ , we define  $\mathcal{O}^T = \{2x - \text{Tr}(x) \mid x \in \mathcal{O}\}$ .

We remark that  $\mathcal{O}^T$  is a sublattice of  $\mathcal{O} \cap B_p^0$ , and this inclusion is strict. The set  $\mathcal{O}^T$  is called the ‘Gross lattice’ by some authors (see Yang [22] and Kane [12]).

If we have  $\mathcal{O} = \langle 1, u_1, u_2, u_3 \rangle$  for  $u_1, u_2, u_3 \in B_p$  and let  $v_i = 2u_i - \text{Tr}(u_i)$ , it follows immediately that  $\mathcal{O}^T = \langle v_1, v_2, v_3 \rangle$ . As already noted, the discriminant of a maximal order  $\mathcal{O} \in B_p$  is  $p^2$ . The following basic result on the determinant of  $\mathcal{O}^T$  follows directly from these two remarks and is a special case of Kohel [14, Corollary 71] with  $\alpha = 1$ .

**LEMMA 3.1.** *Let  $\mathcal{O}$  be a maximal order of  $B_p$ . Then  $\det(\mathcal{O}^T) = 4p^2$ .*

The following easy lemma allows us to characterize the conjugacy classes of  $B_p$ . For any  $x, y \in B_p$ , we write  $x \sim y$  if there exists non-zero  $c \in B_p$  such that  $cxc^{-1} = y$ . Likewise for lattices  $\Lambda, \Lambda' \subset B_p$  we write  $\Lambda \sim \Lambda'$  if there exists non-zero  $c \in B_p$  such that  $c\Lambda c^{-1} = \Lambda'$ .

**LEMMA 3.2.** *Let  $x, y \in B_p$ . Then  $x \sim y$  if and only if  $\text{Tr}(x) = \text{Tr}(y)$  and  $\text{Nr}(x) = \text{Nr}(y)$ .*

If  $\mathcal{O}^T = \langle v_1, v_2, v_3 \rangle$  as above, it is not difficult to see that  $\mathcal{O} = \{x \in 1/2\langle 1, \mathcal{O}^T \rangle \mid \text{Nr}(x) \in \mathbb{Z}\}$ . From this observation we obtain the following lemma, which characterizes  $\mathcal{O}$  in terms of  $\mathcal{O}^T$ .

**LEMMA 3.3.** *Two orders  $\mathcal{O}, \mathcal{O}' \subset B_p$  are of the same type if and only if  $\mathcal{O}^T \sim \mathcal{O}'^T$ .*

*Proof.* It is clear that if  $c\mathcal{O}c^{-1} = \mathcal{O}'$ , then  $c\mathcal{O}^Tc^{-1} = \mathcal{O}'^T$ . Conversely, assume that  $c\mathcal{O}^Tc^{-1} = \mathcal{O}'^T$ . By conjugating  $\mathcal{O}$  by  $c$ , we see it suffices only to prove that if  $\mathcal{O}^T = \mathcal{O}'^T$ , then  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type. But from the above observation, if  $\mathcal{O}^T = \mathcal{O}'^T$ , then  $\langle 1, \mathcal{O}^T \rangle = \langle 1, \mathcal{O}'^T \rangle$  and so in fact we obtain  $\mathcal{O} = \mathcal{O}'$ .  $\square$

We now make some remarks about lattices generated by pairs of elements  $x, y \in \mathcal{O}^T$ . Let  $x, y \in \mathcal{O}^T$  be such that  $\langle x, y \rangle$  is a rank 2 lattice. Define the two-dimensional subspace

$$\langle x, y \rangle^\perp = \{v \in B_p \mid \text{Tr}(v\bar{x}) = \text{Tr}(v\bar{y}) = 0\}. \tag{3.1}$$

As  $x, y$  have zero trace, we see that  $\mathbb{Q} \subset \langle x, y \rangle^\perp$ , and so we can suppose  $\langle x, y \rangle^\perp$  has  $\mathbb{Q}$ -basis  $\{1, w\}$  with  $\text{Tr}(w) = 0$ .

LEMMA 3.4. *Let  $x, y \in \mathcal{O}^T$ . It then holds that  $w = 2xy - \text{Tr}(xy) \in \mathcal{O}^T \cap \langle x, y \rangle^\perp$ , where  $\langle x, y \rangle^\perp$  is defined in equation (3.1).*

*Proof.* Clearly  $w$  has trace zero. We observe that  $\text{Tr}(xy\bar{x}) = \text{Tr}(xy\bar{y}) = 0$  since both  $x$  and  $y$  have zero trace. So we have  $xy \in \langle x, y \rangle^\perp$ , and since  $\mathbb{Q} \subset \langle x, y \rangle^\perp$ , it follows that indeed  $2xy - \text{Tr}(xy) \in \langle x, y \rangle^\perp$ .  $\square$

Let  $D_1 = \text{Nr}(x)$ ,  $D_2 = \text{Nr}(y)$  and  $L = \langle x, y \rangle$ . Writing  $T = \text{Tr}(x\bar{y}) = x\bar{y} + y\bar{x} = -(xy + yx)$  we have that the lattice  $L$  has determinant  $D_1D_2 - (T/2)^2 = (4D_1D_2 - T^2)/4$ . Write  $w = 2x\bar{y} - T = x\bar{y} - y\bar{x}$ . Then, by Lemma 3.4,  $w \in \mathcal{O}^T \cap \langle x, y \rangle^\perp$ . An immediate calculation gives  $\text{Nr}(w) = 4D_1D_2 - T^2$ . Hence, the determinant of  $\langle x, y, w \rangle$  and  $\langle 1, x, y, w \rangle$  is  $(4D_1D_2 - T^2)^2/4$ . The discriminant of the order  $\langle 1, x, y, w \rangle$  is thus  $4(4D_1D_2 - T^2)^2$ , and since  $\langle 1, x, y, w \rangle \subseteq \mathcal{O}$ , we have  $p^2 \mid (4D_1D_2 - T^2)^2$  and so

$$p \mid (4D_1D_2 - T^2). \tag{3.2}$$

(This argument appears in Kaneko [13].)

For an integer  $D < 0$  ( $D \equiv 0$  or  $1 \pmod{4}$ ), we consider the imaginary quadratic order  $\mathcal{O}_D := \mathbb{Z}[\frac{1}{2}(D + \sqrt{D})]$  of discriminant  $D$ . An embedding  $i : \mathcal{O}_D \mapsto \mathcal{O}$  is called *optimal* if  $(\mathbb{Q} \otimes i(\mathcal{O}_D)) \cap \mathcal{O} = i(\mathcal{O}_D)$ . By a straightforward argument (see, for example, the beginning of § 3 of Elkies *et al.* [7]), we see that there is a bijection between primitive elements of  $\mathcal{O}^T$  and optimal embeddings in the following sense: for every optimal representation of  $|D|$  in  $\mathcal{O}^T$  by a primitive element  $x \in \mathcal{O}^T$ , there is a unique optimal embedding  $i : \mathcal{O}_D \mapsto \mathcal{O}$  such that  $i(\sqrt{D}) = x$ , and vice versa. Hence, whenever we talk of an optimal representation or primitive element, we will always associate to it the corresponding optimal embedding.

#### 4. Proof of Theorem 2.1

We remark first that when  $p$  is small, all maximal orders of  $B_p$  can be found feasibly through an exhaustive search, and so this case is easily handled for both Theorems 2.1 and 2.2. It will furthermore turn out that we require bounds like  $p > 168$  or  $p > 286$  for some technical lemmas. Hence, we introduce some notation to be used for the rest of the paper.

NOTATION 4.1. Let  $p > 286$  be a prime and  $\mathcal{O}$  and  $\mathcal{O}'$  two maximal orders in  $B_p$ . Let  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  be as in Definition 3.1. Let  $D_1, D_2, D_3$  (respectively,  $D'_1, D'_2, D'_3$ ) be the successive minima of  $\mathcal{O}^T$  (respectively,  $\mathcal{O}'^T$ ). Denote by  $x, y, z \in \mathcal{O}^T$  (respectively,  $x', y', z' \in \mathcal{O}'^T$ ) elements such that  $D_1 = \text{Nr}(x), D_2 = \text{Nr}(y), D_3 = \text{Nr}(z)$  (respectively,  $D'_1 = \text{Nr}(x'), D'_2 = \text{Nr}(y'), D'_3 = \text{Nr}(z')$ ).

Before describing the general strategy of the proof, we remove a small number of trivial cases when  $D_1$  is small. We recall that the number of different types of maximal orders of  $B_p$  containing an optimal embedding of the imaginary quadratic order  $\mathcal{O}_D$  is bounded above by  $h_D$ , the class number of  $\mathcal{O}_D$  (we refer to Theorem 5.1 of §5 for a more detailed result). However it is known that  $h_D = 1$  for all discriminants  $-15 < D < 0$ . We thus obtain the following result, relevant to both theorems.

LEMMA 4.1. *Let  $-15 < D < 0$ . If  $\mathcal{O}$  and  $\mathcal{O}'$  are maximal orders of  $B_p$  that both optimally represent  $|D|$ , then  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type.*

Unless otherwise stated, we will always impose the conditions

$$D_1 D_2 < \frac{16}{3} p, \quad 15 \leq D_1, \quad \text{and} \quad 286 < p. \tag{4.1}$$

We further remark that in the setting of Theorems 2.1 and 2.2, where  $\mathcal{O}^T$  optimally represents the successive minima of  $\mathcal{O}^T$ , it trivially holds that

$$D'_1 \leq D_1 \quad \text{and} \quad D'_2 \leq D_2. \tag{4.2}$$

We now describe the general strategy of the proof of Theorem 2.1. The goal is to show that  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type, which will follow from showing that  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  are conjugate. The first step is to take appropriate sublattices  $\langle x, y \rangle$  in  $\mathcal{O}^T$  and  $\langle x', y' \rangle$  in  $\mathcal{O}'^T$  and then to show that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric. The final stage of the proof is to extend to the full lattices  $\mathcal{O}^T$  and  $\mathcal{O}'^T$ .

4.1. *Proving that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric*

Let  $x, y \in \mathcal{O}^T$  and  $x', y' \in \mathcal{O}'^T$  be as in Notation 4.1, and recall that  $D_1 = D'_1$  and  $D_2 = D'_2$  in the case of Theorem 2.1. To show that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric it suffices to show that  $\text{Tr}(xy) = \text{Tr}(x'y')$ . This follows from equation (3.2).

LEMMA 4.2. *Let notation be as above and suppose  $p > 128$ . Then  $\text{Tr}(x\bar{y}) = \text{Tr}(x'\bar{y}')$ .*

*Proof.* We know that  $0 < D_1 D_2 < 16p/3$  and  $0 \leq T^2 \leq 4\text{Nr}(x)\text{Nr}(y) \leq 4D_1 D_2$ , and similarly for  $D'_1, D'_2, T'$ . Hence,  $0 \leq 4D_1 D_2 - T^2 \leq 4D_1 D_2 < 64p/3 < 22p$  and  $|T| < \sqrt{64p/3} < 4.7\sqrt{p}$ . We also know that  $4D_1 D_2 - T^2 \equiv 4D_1 D_2 - T'^2 \equiv 0 \pmod{p}$ . Further, there are at most two solutions modulo  $p$  to  $T^2 \equiv 4D_1 D_2 \pmod{p}$ , and so all possible values for  $T' = \text{Tr}(x'y')$  are of the form  $T' = \pm T + kp$  for some integer  $k$ . Now,  $0 \leq 4D_1 D_2 - T'^2 \leq 4D_1 D_2 < 22p$ , and

$$4D_1 D_2 - T'^2 = (4D_1 D_2 - T^2) \mp 2Tkp - k^2 p^2.$$

For  $p > 128$  and  $|k| \geq 1$  we remark that  $|\mp 2Tkp - k^2 p^2| \geq p(p - 2|T|) > p(p - 9.4\sqrt{p}) > 22p$ . Thus  $k = 0$  and so  $T' = \pm T$ . Changing the sign of  $y'$ , if necessary, gives the result.  $\square$

We deduce that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$ , are isometric. Hence, as shown in Lemma 4.3 below, we can conjugate so that  $x' = x$  and  $y' = y$ .

LEMMA 4.3. *Let  $\mathcal{O}, \mathcal{O}' \subset B_p$  be two orders. For any elements  $x, y \in \mathcal{O}^T$  and  $x', y' \in \mathcal{O}'^T$  such that  $x \sim x', y \sim y'$  and  $x + y \sim x' + y'$  it holds that  $\langle x, y \rangle \sim \langle x', y' \rangle$ , that is, there exists non-zero  $c \in B_p$  such that  $c\langle x, y \rangle c^{-1} = \langle x', y' \rangle$ .*

*Proof.* As  $\text{Tr}(\mathcal{O}^T) = \text{Tr}(\mathcal{O}'^T) = 0$ , for all  $r \in \mathcal{O}^T$  and  $r' \in \mathcal{O}'^T$ , it holds that  $r \sim r'$  if and only if  $\text{Nr}(r) = \text{Nr}(r')$  by Lemma 3.2. It follows that

$$\text{Nr}(x') + \text{Nr}(y') + \text{Tr}(x'\overline{y'}) = \text{Nr}(x' + y') = \text{Nr}(x + y) = \text{Nr}(x) + \text{Nr}(y) + \text{Tr}(x\overline{y}),$$

and we obtain  $\text{Tr}(x\overline{y}) = \text{Tr}(x'\overline{y'})$ .

We recall that for any  $u, v \in B_p$ , we have

$$uv + vu = \text{Tr}(u)v + \text{Tr}(v)u + \text{Tr}(uv) - \text{Tr}(u)\text{Tr}(v).$$

From this, it follows that  $\langle 1, x, y, xy \rangle$  and  $\langle 1, x', y', x'y' \rangle$  are both rings (just check that the product of any two generators is in the lattice), and hence they are both orders. Furthermore, since  $\overline{x} = -x$ ,  $\overline{y} = -y$  and  $\text{Tr}(x\overline{y}) = \text{Tr}(x'\overline{y'})$ , we obtain that these orders are isomorphic under the natural mapping  $\psi : a + bx + cy + dxy \mapsto a + bx' + cy' + dx'y'$ . Since all isomorphisms of orders come from conjugation, we know that there exists non-zero  $c \in B_p$  such that  $c\langle 1, x, y, xy \rangle c^{-1} = \langle 1, x', y', x'y' \rangle$ . The lemma follows.  $\square$

#### 4.2. Completing the proof

We now have  $\mathcal{O}^T = \langle x, y, z \rangle$  and  $\mathcal{O}'^T = \langle x, y, z' \rangle$  with  $\text{Nr}(z) = \text{Nr}(z') = D_3$ . It remains to prove that  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  are equal. We have the following result for any ternary lattice.

LEMMA 4.4. *Let  $L$  be a lattice of dimension 3 endowed with a norm  $\|\cdot\|$ . Let  $x, y, z \in L$  and assume that  $D_1 := \|x\|^2, D_2 := \|y\|^2$  and  $D_3 := \|z\|^2$  are the successive minima of  $L$ . Then  $L = \langle x, y, z \rangle$  and (recalling that  $\det(L) = \text{Vol}(L)^2$ )*

$$\det(L) \leq D_1 D_2 D_3 \leq 2 \det(L).$$

*Proof.* As mentioned in §2, the third Hermite constant  $\gamma_3$  is given by  $\gamma_3^3 = 2$ . The desired inequality follows immediately from (2.1).

To deduce that  $L = \langle x, y, z \rangle$ , we observe that the volume of a sublattice  $L' \subseteq L$  is always a multiple of the volume of  $L$ . Furthermore  $\text{Vol}(L) = \text{Vol}(L')$  if and only if  $L = L'$ . Hence if  $\langle x, y, z \rangle \neq L$ , then  $\text{Vol}(\langle x, y, z \rangle) \geq 2\text{Vol}(L)$ , and so again by (2.1), we have

$$D_1 D_2 D_3 \geq \det(\langle x, y, z \rangle) \geq 4 \det(L),$$

which contradicts  $D_1 D_2 D_3 \leq 2 \det(L)$ . We conclude that  $L = \langle x, y, z \rangle$  as claimed.  $\square$

Lemma 4.4 allows us to conclude that  $\mathcal{O}^T = \langle x, y, z \rangle$  and  $\mathcal{O}'^T = \langle x', y', z' \rangle$ , and, in conjunction with Lemma 3.1, that

$$4p^2 \leq D_1 D_2 D_3, \quad D'_1 D'_2 D'_3 \leq 8p^2. \tag{4.3}$$

LEMMA 4.5. *Let notation be as in Notation 4.1. Suppose that  $\mathcal{O}^T = \langle x, y, z \rangle$  and  $\mathcal{O}'^T = \langle x, y, z' \rangle$  with  $\text{Nr}(z) = \text{Nr}(z') = D_3$ . Then  $z = \pm z'$  (and so  $\mathcal{O}^T = \mathcal{O}'^T$ ) provided that*

$$D_1 D_2 < \frac{16}{3} p, \tag{4.4}$$

$$15 \leq D_1, \quad \text{and} \tag{4.5}$$

$$168 < p. \tag{4.6}$$

*Proof.* Recall from equation (3.1) the two-dimensional subspace

$$\langle x, y \rangle^\perp := \{v \in B_p \mid \text{Tr}(v\overline{x}) = \text{Tr}(v\overline{y}) = 0\}. \tag{4.7}$$



As  $x, y$  have zero trace, we see that  $\mathbb{Q} \subset \langle x, y \rangle^\perp$ , and so  $\langle x, y \rangle^\perp$  has  $\mathbb{Q}$ -basis  $\{1, v\}$  with  $\text{Tr}(v) = 0$ . Let  $u \in \langle x, y \rangle^\perp$  be the projection of  $z$  onto  $\langle x, y \rangle^\perp$  (that is,  $u = \text{Tr}(z\bar{v})v / (2\text{Nr}(v))$ ). Similarly, let  $u'$  be the projection of  $z'$  onto  $\langle x, y \rangle^\perp$ . We remark that  $u, u' \in B_p^0$ .

Now, (recalling that the determinant is the square of the volume of a lattice)

$$\det(\langle x, y \rangle)\text{Nr}(u) = \det(\mathcal{O}^T) = \det(\mathcal{O}'^T) = \det(\langle x, y \rangle)\text{Nr}(u'). \tag{4.8}$$

Since  $u, u' \in \langle v \rangle$ , it follows that  $u' = \pm u$ , so, replacing  $z'$  by  $-z'$  if necessary, we may assume  $u' = u$ . Write  $z = (\alpha x + \beta y) + u$  for some  $\alpha, \beta \in \mathbb{Q}$ .

Let  $s = 2xy - \text{Tr}(xy)$ , which by Lemma 3.4 lies in  $\mathcal{O}^T \cap \langle x, y \rangle^\perp$  and in  $\mathcal{O}'^T \cap \langle x, y \rangle^\perp$ . Hence there exist  $a, b, c, a', b', c' \in \mathbb{Z}$  such that  $s = ax + by + cz$  and  $s = a'x + b'y + c'z'$ .

Since  $s \in \langle x, y \rangle^\perp \cap \mathcal{O}^T$ , and  $u$  is the projection of  $z$  and  $z'$  onto  $\langle x, y \rangle^\perp$ , it holds that  $s = cu = c'u$ , which implies  $c = c'$ . Furthermore, we have that

$$\text{Nr}(ax + by) = \text{Nr}(s - cz) = \text{Nr}(s) + c^2\text{Nr}(z) - c\text{Tr}(s\bar{z}) \quad \text{and} \tag{4.9}$$

$$\text{Nr}(a'x + b'y) = \text{Nr}(s - cz') = \text{Nr}(s) + c^2\text{Nr}(z') - c\text{Tr}(s\bar{z}'). \tag{4.10}$$

Since the projections of  $z$  and  $z'$  onto  $\langle x, y \rangle^\perp$  are equal, we obtain  $\text{Tr}(s\bar{z}) = \text{Tr}(s\bar{z}')$ . We also recall that  $\text{Nr}(z) = D_3 = \text{Nr}(z')$ . Together with (4.9) and (4.10), this implies that

$$\text{Nr}(ax + by) = \text{Nr}(a'x + b'y). \tag{4.11}$$

We now show that  $\text{Nr}(ax + by)$  cannot be too large and then apply [13, Theorem 2'] to conclude that  $ax + by = \pm(a'x + b'y)$ . Recall that  $u = -\alpha x - \beta y + z$ , for some  $\alpha, \beta \in \mathbb{Q}$ . We claim that the closest element to  $\alpha x + \beta y$  in the lattice  $\langle x, y \rangle$  is 0. Indeed, let  $k \in \langle x, y \rangle$  be the closest lattice element to  $\alpha x + \beta y$ . Then  $\text{Nr}(\alpha x + \beta y - k) \leq \text{Nr}(\alpha x + \beta y)$ . On the other hand

$$\text{Nr}(-z - k) = \text{Nr}(u) + \text{Nr}(\alpha x + \beta y - k) \geq \text{Nr}(z) = \text{Nr}(u) + \text{Nr}(\alpha x + \beta y),$$

where the inequality holds since  $-z - k$  is outside  $\langle x, y \rangle$  and  $z$  represents the third successive minimum of  $\mathcal{O}^T$ . Thus  $\text{Nr}(\alpha x + \beta y - k) = \text{Nr}(\alpha x + \beta y)$ , and hence 0 is the closest element to  $\alpha x + \beta y$  in the lattice  $\langle x, y \rangle$  as claimed.

It is well known that the covering radius  $\rho(\Lambda)$  of a lattice  $\Lambda$  is always bounded by  $\rho(\Lambda) \leq \sigma(\Lambda)/2$ , where  $\sigma(\Lambda)$  is the length of the diagonal of the orthogonal parallelepiped of  $\Lambda$  (see, for example, Micciancio and Goldwasser [9, Theorem 7.9, page 138]). As a result, we have that

$$\text{Nr}(\alpha x + \beta y) \leq \rho(\langle x, y \rangle)^2 \leq \frac{1}{4}\sigma(\langle x, y \rangle)^2 \leq \frac{1}{4}(D_1 + D_2).$$

Since  $s = cu$ , it holds that  $a = c\alpha$  and  $b = c\beta$ , and so

$$\text{Nr}(ax + by) = c^2\text{Nr}(\alpha x + \beta y) \leq \frac{c^2}{4}(D_1 + D_2). \tag{4.12}$$

We now bound  $c$ . By (4.3), we have that

$$\frac{1}{2}D_1D_2D_3 \leq 4p^2 = \det(\langle x, y, z \rangle) \leq D_1D_2\text{Nr}(u).$$

It follows that  $D_3 \leq 2\text{Nr}(u)$ . Furthermore, we observe that

$$c^2\text{Nr}(u) = \text{Nr}(s) = \text{Nr}(xy - \frac{1}{2}\text{Tr}(xy)) \leq \text{Nr}(xy) = D_1D_2.$$

Hence

$$D_3 \leq \frac{2}{c^2}D_1D_2. \tag{4.13}$$



On the other hand, by (4.3) and (4.4), we obtain

$$\frac{9}{64}D_1D_2 < \frac{3}{4}p < \frac{4p^2}{D_1D_2} \leq D_3.$$

Combined with (4.13), this gives  $c^2 < \frac{128}{9} < 15$ . As  $c \in \mathbb{Z}$ , this implies that  $c^2 \leq 9$ . Therefore, from (4.12), we obtain

$$\text{Nr}(ax + by) \leq \frac{9}{4}(D_1 + D_2) < \frac{9}{4}\left(15 + \frac{16p/3}{15}\right) < p,$$

where the last two inequalities follow from (4.4), (4.5) and (4.6). However, since  $\text{Nr}(a'x + b'y) = \text{Nr}(ax + by)$  from (4.11), we obtain by [13, Theorem 2'] that  $ax + by = \pm(a'x + b'y)$ , and so  $z = \pm z'$  as desired.  $\square$

Finally, Lemma 3.3 completes the proof of Theorem 2.1.

### 5. Algorithm to associate elliptic curves to maximal orders

In this section we consider the following problem: given a maximal order  $\mathcal{O} \subset B_p$ , compute an elliptic curve  $E/\mathbb{F}_{p^2}$  such that  $\text{End}(E) \cong \mathcal{O}$ . Our approach is to determine  $j(E)$  using Hilbert class polynomials. We give a general method, but we are only able to prove that this method terminates under the condition (2.3) (for example, when  $\sqrt{-p} \in \mathcal{O}$ , or equivalently,  $j(E) \in \mathbb{F}_p$ ).

Let  $H_D(X) \in \mathbb{F}_p[X]$  be the reduction modulo  $p$  of the Hilbert class polynomial of discriminant  $D < 0$  (see Cox [6, §13]). We recall that  $H_D(X) \in \mathbb{Z}[X]$  is the polynomial whose roots are the  $j$ -invariants of the elliptic curves over  $\mathbb{C}$  possessing the quadratic order  $\mathcal{O}_D = \mathbb{Z}[\frac{1}{2}(D + \sqrt{D})]$  as their endomorphism ring.

As mentioned in the introduction, if  $\sqrt{-p} \in \mathcal{O}$  then  $\mathcal{O}$  can be written in a canonical form given by Ibukiyama [11]. For example, when  $p \equiv 1 \pmod{4}$  then there exists a prime  $q \equiv 3 \pmod{8}$  and an integer  $r$  such that  $q \mid (r^2 + p)$  and such that  $\mathcal{O}$  is isomorphic to an order with  $\mathbb{Z}$ -basis  $\{1, (1+j)/2, i(1+j)/2, (r+i)j/q\}$  in the quaternion algebra defined by  $i^2 = -p, j^2 = -q$  and  $ij = -ji$ . In the case  $p \equiv 3 \pmod{4}$  there are two such families of orders. Note that  $j(E) \in \mathbb{F}_p$  is a root of either  $H_{-p}(X)$  or  $H_{-4p}(X)$ , and is also a root of either  $H_{-q}(X)$  or  $H_{-4q}(X)$ . When  $q$  is small this already gives an efficient way to determine  $j(E)$ , however we cannot assume that  $q$  is always small in Ibukiyama's result.

The idea of the algorithm is to use lattice algorithms (basis reduction or enumeration) to find several small norms  $d_1, d_2, \dots, d_n$  of primitive elements in  $\mathcal{O}^T$ , and to note that  $(X - j(E))$  is a factor of  $\text{gcd}(H_{-d_1}(X), H_{-d_2}(X), \dots, H_{-d_n}(X))$ . To see this note that if  $\psi \in \mathcal{O}^T$  has norm  $d$  then  $\psi^2 = -d$ . By the remark before Lemma 3.3, either  $(1 + \psi)/2$  or  $\psi/2$  lies in  $\mathcal{O}$ . Hence  $\mathcal{O}$  contains  $\mathbb{Z}[(d + \sqrt{-d})/2]$  and so  $j(\mathcal{O})$  is a root of  $H_{-d}(X)$ . Theorem 2.2 shows that if (2.3) holds, then the algorithm is guaranteed to terminate within a bounded time. By Lemma 2.3, condition (2.3) holds in particular when  $j(\mathcal{O}) \in \mathbb{F}_p$ .

The above sketch is made precise in Theorem 5.1 and Algorithm 1 below. We explain the termination and correctness of Algorithm 1 in the subsequent discussion, and analyze the running time of each specific sub-algorithm in §5.1. Some examples of the use of the method are given in §6.

We remark that if  $p$  is small, then we may identify  $j(\mathcal{O})$  through exhaustive search. Thus we make the implicit assumption that  $p$  is sufficiently large (concretely  $p > 286$ ) so we may use Theorem 2.2. Furthermore, we recall that the case when  $\mathcal{O}$  has units other than  $\pm 1$  is trivial (see the beginning of §2). In the following theorem, the cases  $d = 3$  and  $d = 4$  would have corresponded to non-trivial units of  $\mathcal{O}$  when  $j(\mathcal{O}) = 1728$  and  $j(\mathcal{O}) = 0$  respectively.

**THEOREM 5.1.** *Assume that  $\mathcal{O}$  has no units other than  $\pm 1$ . Then  $d > 4$  is represented optimally by  $\mathcal{O}^T$  with optimal multiplicity  $m$  if and only if  $j(\mathcal{O})$  appears as a root of  $H_{-d}(X) \in \mathbb{F}_p[X]$  with multiplicity  $\varepsilon m$ , where  $\varepsilon = 1$  or  $2$  according to whether  $p$  is inert or ramified in  $\mathbb{Q}(\sqrt{-d})$ , that is,  $p$  does not divide or does divide the discriminant  $\Delta_{\mathbb{Q}(\sqrt{-d})}$  respectively.*

*Proof.* This can be viewed as a special case of Lemma 3.2 of Elkies *et al.* [7], where the maximal order has no non-trivial units, and so the equivalence class of any optimal embedding  $i$  is simply  $i$  itself. We may assume  $p$  is inert or ramified because if  $p$  splits then the roots of  $H_{-d}(X)$  correspond to ordinary elliptic curves. □

We will use Theorem 5.1 to distinguish orders that have different optimal multiplicities for some integer  $d_n$ . We use derivatives to achieve this; recall that if a polynomial  $p(X)$  over a field  $\mathbb{F}$  has  $x_0 \in \mathbb{F}$  as a root with multiplicity  $m \geq 1$ , then it holds that  $p'(X)$  has  $x_0$  as a root with multiplicity  $m - 1$ .

**Algorithm 1**

Input: Prime  $p$  and a  $\mathbb{Z}$ -basis of a maximal order  $\mathcal{O} \subset B_p$ .

Output: Minimal polynomial of  $j$ -invariant(s)  $j(\mathcal{O}) \in \mathbb{F}_{p^2}$  such that  $\text{End}(E(j(\mathcal{O}))) = \mathcal{O}$ .

Procedure:

- (1) If  $\mathcal{O}$  has a unit other than  $\pm 1$ , output the polynomial corresponding to  $j(\mathcal{O}) = 0$  or  $j(\mathcal{O}) = 1728$  accordingly (see discussion before Theorem 5.1) and terminate. Otherwise construct a  $\mathbb{Z}$ -basis of the sublattice  $\mathcal{O}^T$ , run lattice reduction/enumeration on the basis, and set  $n = 1$ ,  $k = 0$ ,  $c = 0$  and  $G(X) = 0$ .
- (2) Compute  $y_n \in \mathcal{O}^T$  such that  $y_n$  is primitive (so  $y_n \neq 0$ ) and  $y_n \neq \pm y_i$  for all  $1 \leq i < n$ , and such that  $\text{Nr}(y_n)$  is minimal over all such possible  $y_n$ .
- (3) Set  $d_n = \text{Nr}(y_n)$ . If  $p$  divides  $\Delta_{\mathbb{Q}(\sqrt{-d_n})}$ , set  $\varepsilon = 2$ , otherwise set  $\varepsilon = 1$ . If  $d_n = d_{n-1}$  set  $k = k + \varepsilon$ , otherwise set  $k = \varepsilon - 1$ . If  $\varepsilon = 2$  and  $k = 1$ , set  $G(X) = \text{gcd}(G(X), H_{-d_n}(X), H'_{-d_n}(X)) \in \mathbb{F}_p[X]$ . Otherwise set  $G(X) = \text{gcd}(G(X), H_{-d_n}^{(k)}(X)) \in \mathbb{F}_p[X]$ , where  $H_{-d_n}^{(k)}(X)$  is the  $k$ th derivative of  $H_{-d_n}(X)$ , and  $H_{-d_n}^{(0)}(X) = H_{-d_n}(X)$ .
- (4) If  $G(X)$  is either linear, or quadratic and irreducible over  $\mathbb{F}_p$ , output  $G(X)$  and terminate. If  $c = 1$ , or if  $n = 2$ ,  $15 \leq d_1$  and  $d_1 d_2 < 16p/3$ , proceed to Step (5). Otherwise set  $n = n + 1$  and return to Step (2).
- (5) If  $n = 2$ , set  $c = 1$ ,  $n = 3$  and  $y_3 = y_1 \pm y_2$ , where  $+/-$  is chosen to minimize  $\text{Nr}(y_3)$ . If  $n = 3$ , set  $n = 4$  and  $y_4 = y_1 \pm y_2$ , such that  $y_4 \neq y_3$ . If  $n = 4$ , set  $n = 5$  and find  $y_5$  outside the sublattice  $\langle y_1, y_2 \rangle$  such that  $\text{Nr}(y_5)$  is minimal. Return to Step (3).

If the condition (2.3) holds (for example, if  $j(\mathcal{O}) \in \mathbb{F}_p$ ) then the algorithm terminates. Furthermore, in this case we only need to consider  $n \leq 5$  (this is the reason for Step (5), which otherwise seems completely unmotivated).

We hope that the algorithm terminates in all cases, but we do not have a proof of this (see discussion in the following paragraph). We note that since  $d_1$  in Step (2) is simply the first successive minimum of  $\mathcal{O}^T$ , it must satisfy  $d_1 < p$  (otherwise we contradict (4.3)). Hence by Kaneko [13, Theorem 2'] (namely, that if there are two different embeddings of  $\mathbb{Z}[(d + \sqrt{d})/2]$  into  $\mathcal{O}$  then  $d^2 \geq p^2$ ) and Theorem 5.1 above,  $H_{-d_1}(X)$  is square-free, and hence so is  $G(X)$  after the first iteration of Step (3). Along with Theorem 5.1, this implies that if it terminates, Algorithm 1 does compute the correct minimal polynomial of  $j(\mathcal{O})$ . The reason for taking the derivative in Step (3) is to take into account the case of multiple roots of  $H_{-d_n}(X)$ , that is, when  $\theta_{\mathcal{O}^T}(d_n) \geq 2$ , or when  $p$  divides the discriminant of  $\mathbb{Q}(\sqrt{-d_n})$ .

Let us temporarily stop the algorithm for some  $n > 0$  just after Step (3), and for simplicity, let us assume that  $d_{n-1} \neq d_n$ . Consider the polynomial  $G(X)$ . One of its roots (or two in the case of a conjugate pair) will be the desired  $j$ -invariant  $j(\mathcal{O})$ . If  $j(\mathcal{O}')$  is another root of  $G(X)$ , what can we say about the associated maximal order  $\mathcal{O}'$ ? It must be the case that  $\theta'_{\mathcal{O}^T}(k) \leq \theta_{\mathcal{O}^T}(k)$

for all integers  $k \leq d_{n-1}$ , in which case we say that  $\mathcal{O}'^T$  *optimally dominates*  $\mathcal{O}^T$  up to  $d_{n-1}$ . If the algorithm never terminates, it is clear then that there must exist a maximal order  $\mathcal{O}'$  such that  $\theta'_{\mathcal{O}'^T}(k) \leq \theta_{\mathcal{O}^T}(k)$  for all  $k > 0$ , that is,  $\mathcal{O}'^T$  optimally dominates  $\mathcal{O}^T$  up to  $b$  for all  $b > 0$ , in which case we simply say that  $\mathcal{O}'^T$  *optimally dominates*  $\mathcal{O}^T$ . So the question of whether Algorithm 1 terminates, and if so, under what running time, is equivalent to the question of whether there exists another maximal order  $\mathcal{O}' \subset B_p$ , of a different type to  $\mathcal{O}$ , such that  $\mathcal{O}'^T$  optimally dominates  $\mathcal{O}^T$ , and if not, what is a bound  $b > 0$  such that  $\mathcal{O}'^T$  does not optimally dominate  $\mathcal{O}^T$  up to  $b$  for all other maximal orders  $\mathcal{O}' \subset B_p$ . We suspect that such an order  $\mathcal{O}'$  does not exist and we propose the following two conjectures.

CONJECTURE 5.1. There do not exist two maximal orders  $\mathcal{O}, \mathcal{O}' \subset B_p$  of different types such that  $\mathcal{O}'^T$  optimally dominates  $\mathcal{O}^T$ .

CONJECTURE 5.2. There exists a bound  $b = O(p)$  such that for all maximal orders  $\mathcal{O}, \mathcal{O}' \subset B_p$  of different types,  $\mathcal{O}'^T$  does not optimally dominate  $\mathcal{O}^T$  up to  $b$ .

5.1. *Analysis of running time*

We discuss each step of Algorithm 1 individually. We now assume that (2.3) holds and so we know the algorithm terminates.

Steps (1) and (2). The units of  $\mathcal{O}$  are easily found and so the first part of Step (1) poses no problem. We observe that  $\mathcal{O}^T = \langle v_1, v_2, v_3 \rangle$  is a three-dimensional sublattice of  $\mathcal{O} = \langle 1, u_1, u_2, u_3 \rangle$ , where  $\{v_1, v_2, v_3\}$  can be given explicitly in terms of  $\{u_1, u_2, u_3\}$  as in the discussion preceding Lemma 3.1. Hence constructing  $\mathcal{O}^T$  in Step (1) and searching for short elements  $y_n$  of  $\mathcal{O}^T$  in Step (2) can be done using standard lattice techniques in polynomial time.

Step (3). Several algorithms exist to compute  $H_{-d_n}(X)$ , see, for example, Belding, Bröker, Enge and Lauter [2] or Sutherland [18]. Under the generalized Riemann hypothesis,  $H_{-d_n}(X)$  can be calculated in  $\tilde{O}(d_n)$  time. It is known that  $\deg(H_{-d_n}(X)) = h_{-d_n}$ , the class number of the imaginary quadratic order  $\mathbb{Z}[\frac{1}{2}(d_n + \sqrt{-d_n})]$ .

To compute the gcd of  $G(X)$  and  $H_{-d_n}(X)$  in Step (3) when  $\deg(G(x)) \geq 1$  we use a quasi-linear method (see, for example, Aho *et al.* [1, §8.9] or [8, §11.1]). Hence, this stage can be done in  $\tilde{O}(h_{-d_n})$  operations in  $\mathbb{F}_p$ . By [2, Lemma 1], we have  $h_{-d_n} = O(\sqrt{d_n} \log d_n)$ , and so the gcd computation can be done in  $O(d_n^{0.5+\epsilon})$  field operations.

As a result, we see that the limiting step of Algorithm 1 is the calculation of  $H_{-d_n}(X)$ , which is bounded by  $O(d_n^{1+\epsilon})$ . By (A.2),  $D_1, D_2, D_3, \text{Nr}(x + y)$  and  $\text{Nr}(x - y)$  are all  $O(p)$ . It follows that the running time of Algorithm 1 under condition (2.3) is  $O(p^{1+\epsilon})$  field operations. We note that under (2.3), we have by (A.3) that  $D_3 > 3p/4$ , so we do not expect to have a faster running time if  $D_3$  is required.

More generally, if we no longer assume (2.3), then the  $O(p)$  bound on the norms is Conjecture 5.2. To analyze the running time of Algorithm 1 in the general case under Conjecture 5.2, we must bound the number of elements of  $\mathcal{O}^T$  with norm less than  $b$ , that is, the largest possible value for  $n$  in the algorithm (under condition (2.3) we knew this was  $n \leq 5$ ). Let  $B_r$  be the ball of radius  $r$  in  $\mathbb{R}^m$  centered at the origin. A special case of a result due to Henk [10] is that for any lattice  $L$  of  $\mathbb{R}^m$  with successive minima  $D_1, D_2, \dots, D_m$ , it holds that

$$\#(L \cap B_r) < 2^{m-1} \prod_{i=1}^m \left\lfloor \frac{2r}{\sqrt{D_i}} + 1 \right\rfloor.$$

Equation (4.3) implies  $D_3 \geq D_2 \geq 2\sqrt{p}$ , so taking  $r = \sqrt{b}$  and  $b = O(p)$  gives  $\#\{x \in \mathcal{O}^T \mid \text{Nr}(x) < b\} = O(p^{0.5})$ . This means  $n \leq O(p^{0.5})$  and, since  $d_i < b = O(p)$  for every  $1 \leq i \leq n$  in Step (3), we obtain a running time of  $O(p^{1.5+\epsilon})$  field operations under Conjecture 5.2.

We remark that by itself Conjecture 5.1 is equivalent to the fact that Algorithm 1 halts for every maximal order  $\mathcal{O}$ , but it does not allow us to make any statements about its running time. We hence stress that even termination is conjectural without assuming (2.3) or Conjecture 5.1.

Lemma 2.3 tells us that  $D_1 D_2 < 16p/3$  will always hold when  $j(\mathcal{O}) \in \mathbb{F}_p$ . As remarked before, by finding an element  $\pi \in \mathcal{O}$  such that  $\pi^2 = -p$ , we can tell if we are in the case when  $j(\mathcal{O}) \in \mathbb{F}_p$ . Hence, provided that it is computationally easier to determine the existence of such an element than to run the algorithm until  $n = 5$ , we could determine before running the algorithm if indeed  $j(\mathcal{O}) \in \mathbb{F}_p$ . Unfortunately, the number of supersingular  $j$ -invariants in  $\mathbb{F}_{p^2}$  is approximately  $p/12$ , and of these, only  $H(-4p) = O(\sqrt{p} \log p)$  lie in  $\mathbb{F}_p$ , where  $H(-4p)$  is the Hurwitz class number (see, for example, Cox [6, Theorem 14.18]). This shows that for a random maximal order  $\mathcal{O} \subset B_p$ , we definitely do not expect that  $j(\mathcal{O}) \in \mathbb{F}_p$ . On the other hand, if the order  $\mathcal{O}$  is input using the format in Ibukiyama [11] then we know  $\sqrt{-p} \in \mathcal{O}$  and so  $j(\mathcal{O}) \in \mathbb{F}_p$ .

## 5.2. Algorithm to match all supersingular $j$ -invariants with all maximal orders

In [4], Cerviño proposed an algorithm that, given a prime  $p$ , associates to every supersingular  $j$ -invariant of  $\mathbb{F}_{p^2}$  the corresponding maximal order type of  $B_p$ . This is different to Algorithm 1 in that it deals with all  $j$ -invariants at once. Cerviño states that his algorithm has running time  $\tilde{O}(p^{2.5})$  operations but no explanation for this is given in the paper and, as far as we can tell, the algorithm he presents is actually at best  $\tilde{O}(p^4)$  field operations. To recall, Cerviño computes, on one side, a list of all  $O(p)$  maximal orders and, for each such order  $\mathcal{O}$ , the set  $\Gamma(\mathcal{O}) = \{(\text{Tr}(\alpha), \text{Nr}(\alpha)) \mid \alpha \in \mathcal{O}, \text{Nr}(\alpha) = O(p)\}$ . On the other side he computes a list of all  $O(p)$  supersingular elliptic curves and, for each, the set  $\Delta(E) = \{(\text{Tr}(\phi), \deg(\phi)) \mid \phi \in \text{End}(E), \deg(\phi) = O(p)\}$ . Computing  $\Gamma(\mathcal{O})$  appears to require running over the  $O(p^2)$  elements in the  $\mathbb{Z}$ -module of rank 4, hence requiring  $O(p^2)$  work, at best. Cerviño suggests computing  $\Delta(E)$  using Vélú's formulae (and this seems to require  $O(p^{3+\varepsilon})$  field operations), but one can probably improve this to  $O(p^{2+\varepsilon})$  operations using evaluated modular polynomials  $\Phi_d(j(E), y) \in \mathbb{F}_p[x]$ , computed using Sutherland's algorithm [19]. Hence, it seems possible to improve Cerviño's algorithm so that it requires  $O(p^{3+\varepsilon})$  field operations.

We propose an alternative algorithm to solve this problem. The main idea of our method is to replace isogeny computations, for a very large set of isogenies, by gcds of Hilbert class polynomials. This leads to a complexity of  $O(p^{2.5+\varepsilon})$  field operations.

If we consider the sub-problem of matching supersingular curves over  $\mathbb{F}_p$  with their maximal orders, it seems that Cerviño's algorithm can be adapted to handle this case with complexity  $O(p^{2.5+\varepsilon})$  field operations. Our method for this case has the improved complexity  $O(p^{1.5+\varepsilon})$ . Note that, as would be expected, the complexities in both cases are just the complexity from §5.1 multiplied by the number of choices for  $\mathcal{O}$ .

Cerviño's proof that the algorithm halts within a bounded running time uses a result of Schiemann (Theorems 4.4 and 4.5 of [16]) that two ternary forms with equal theta series are equivalent. In our case, this translates to: if  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  represent the same integers with the same multiplicity, then it follows that  $\mathcal{O}^T \sim \mathcal{O}'^T$ , and hence by Lemma 3.3, we have that  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type. Furthermore, Schiemann gives a bound  $b$  in terms of the successive minima  $D_1$ ,  $D_2$  and  $D_3$  of  $\mathcal{O}^T$ , such that if  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  represent all integers  $k \leq b$  with the same multiplicity, then indeed  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type. For our purposes we may take  $b = 3D_3$ , which gives  $b \leq 6p$  using (A.2), although much better bounds are given in Schiemann's general result.

It is not difficult to see that  $\mathcal{O}^T$  and  $\mathcal{O}'^T$  represent the same integers with the same multiplicity if and only if they optimally represent the same integers with the same optimal multiplicity. This is because every representation  $x \in \mathcal{O}^T$  of  $k \in \mathbb{Z}$  can be decomposed uniquely as  $x = cy$ , where  $y \in \mathcal{O}^T$  is optimal and  $c$  is a positive integer. More specifically, we have the following lemma.

LEMMA 5.2. For any bound  $b > 0$ , it holds that  $\theta_{\mathcal{O}^T}(k) = \theta_{\mathcal{O}^T}(k)$  for all  $k \leq b$  if and only if  $\theta'_{\mathcal{O}^T}(k) = \theta'_{\mathcal{O}^T}(k)$  for all  $k \leq b$ .

We now present our alternative to Cerviño’s algorithm in the general case of all supersingular curves over  $\mathbb{F}_{p^2}$ .

**Algorithm 2**

Input: Prime  $p$ .

Output: The list of pairs  $(\mathcal{O}_1, K_1(X)), \dots, (\mathcal{O}_{t_p}, K_{t_p}(X))$ , where  $t_p$  is the type number of  $B_p$ , and for all  $1 \leq i \leq t_p$ ,  $\mathcal{O}_i$  are representatives of the distinct maximal order types of  $B_p$ , and  $K_i(X)$  is the minimal polynomial of the supersingular  $j$ -invariant(s)  $j(\mathcal{O}_i)$ .

Procedure:

- (1) For all  $1 \leq i \leq t_p$ , compute a  $\mathbb{Z}$ -basis of  $\mathcal{O}_i$  and  $\mathcal{O}_i^T$ , run lattice reduction/enumeration on the bases to compute the successive minima  $D_1^i, D_2^i$  and  $D_3^i$  of  $\mathcal{O}_i^T$ , and set  $c_i = 0$ .
- (2) For every  $1 \leq i \leq t_p$  run Algorithm 1 on  $\mathcal{O}_i$  up until it either halts normally or until we reach  $n$  such that  $d_n > 6p$ . If Algorithm 1 halted normally, let  $K_i(X)$  be its output, store the pair  $(\mathcal{O}_i, K_i(X))$ , and set  $c_i = 1$ . Otherwise let  $G_i(X)$  be the current polynomial after Step (3) of Algorithm 1, and store the pair  $(\mathcal{O}_i, G_i(X))$ .
- (3) For all  $1 \leq i, j \leq t_p$  such that  $c_i = 0$  and  $c_j = 1$ , remove from  $G_i(X)$  all common factors with  $K_j(X)$ . If  $G_i(X)$  is now either linear, or quadratic and irreducible over  $\mathbb{F}_p$ , let  $K_i(X) = G_i(X)$  and store the pair  $(\mathcal{O}_i, K_i(X))$  and set  $c_i = 1$ .
- (4) Repeat Step (3) until  $c_i = 1$  for all  $1 \leq i \leq t_p$ . Output the list of pairs

$$(\mathcal{O}_1, K_1(X)), \dots, (\mathcal{O}_{t_p}, K_{t_p}(X)).$$

The correctness of Algorithm 2 is guaranteed by the correctness of Algorithm 1. Furthermore Algorithm 2 is always guaranteed to halt, which may seem surprising given that we do not know if the same is true for Algorithm 1 in the general case. To see that Algorithm 2 does always halt, we define a transitive order  $\preceq$  on the set of maximal order types as follows:  $\mathcal{O}_i \preceq \mathcal{O}_k$  if and only if  $\mathcal{O}_k$  optimally dominates  $\mathcal{O}_i$  up to  $6p$  (meaning that  $\theta'_{\mathcal{O}_i^T}(m) \leq \theta'_{\mathcal{O}_k^T}(m)$  for all  $1 \leq m \leq 6p$ ).

We observe that if  $\mathcal{O}_i \preceq \mathcal{O}_k$  and  $\mathcal{O}_k \preceq \mathcal{O}_i$ , then both orders  $\mathcal{O}_i$  and  $\mathcal{O}_k$  represent the same integers up to  $6p$  with the same optimal multiplicity, and so it follows by Schiemann [16] and Lemma 5.2 that they are of the same type, that is,  $\mathcal{O}_i = \mathcal{O}_k$ . Hence  $\preceq$  is a partial order on the set of maximal order types  $\{\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_{t_p}\}$ .

Now consider that we have just finished Step (2) of Algorithm 2 and consider  $1 \leq i \leq t_p$  such that  $c_i = 0$  (if  $c_i = 1$  for all  $1 \leq i \leq t_p$  then the algorithm clearly terminates without even performing Step (3)). Without loss of generality, assume  $i = 1$ . From the discussion following Algorithm 1, we know  $G_1(X)$  is square-free and so before performing Step (3) we can write

$$G_1(X) = (X - j_1)(X - j_2) \dots (X - j_k),$$

where the  $j$ -invariants  $j_1, j_2, \dots, j_k$  are all distinct and represent at least two different maximal orders, that is, we don’t have  $k = 1$ , nor do we have  $k = 2$  and  $j_1, j_2$  form a conjugate pair. Without loss of generality, assume that  $\mathcal{O}(j_1) = \mathcal{O}_1$  that is,  $j_1$  is the correct  $j$ -invariant associated with  $\mathcal{O}_1$ , and likewise that  $\mathcal{O}(j_2) = \mathcal{O}_2, \mathcal{O}(j_3) = \mathcal{O}_3$ , etc.

Since the roots  $j_2, j_3, \dots, j_k$  were not removed from  $G_1(X)$  when we ran Step (2), this implies that  $\mathcal{O}_2, \mathcal{O}_3, \dots, \mathcal{O}_k$  all optimally dominate  $\mathcal{O}_1$  up to  $6p$ , that is, we have  $\mathcal{O}_1 \prec \mathcal{O}_i$  (meaning that  $\mathcal{O}_1 \preceq \mathcal{O}_i$  and  $\mathcal{O}_1 \not\cong \mathcal{O}_i$ ) for all  $1 \leq i \leq k$ .

Now assume that  $c_1$  never becomes 1 after any number of repetitions of Step (3). This implies that one of  $c_2, c_3, \dots, c_k$  always remains 0 as well, since otherwise the roots  $j_2, j_3, \dots, j_k$  would ultimately be removed from  $G_1(X)$  with enough repetitions of Step (3). Without loss

of generality, assume that  $c_2$  always remains 0. But now the same argument applies to  $c_2$ , and there must exist another index  $1 \leq i \leq t_p$  such that  $\mathcal{O}_2 \prec \mathcal{O}_i$  and that  $c_i$  always remains 0.

Hence we can find an ascending chain  $\mathcal{O}_1 \prec \mathcal{O}_2 \prec \mathcal{O}_i \prec \dots$  such that  $c_1, c_2, c_i, \dots$  all remain 0. However every ascending chain clearly has an upper bound, so let us take  $\mathcal{O}_1 \prec \mathcal{O}_2 \prec \mathcal{O}_i \prec \dots \prec \mathcal{O}_n$ , where  $c_1, c_2, c_i, \dots, c_n$  all remain 0, and such that we cannot find another order  $\mathcal{O}_m$  such that  $\mathcal{O}_n \prec \mathcal{O}_m$  and  $c_m$  always remains 0. But this implies that  $c_n$  ultimately becomes 1 after a finite number of repetitions of Step (3), which clearly leads to a contradiction. It follows that eventually  $c_i$  becomes 1 for every  $1 \leq i \leq t_p$ , and so Algorithm 2 halts with the correct output.

To analyze the running time of Algorithm 2, we start by looking at Step (2). By the same argument as in the analysis of the running time of Algorithm 1 (there under Conjecture 5.2) we conclude that Step (2) can be done in time  $O(p^{1.5+\epsilon})$  for every  $1 \leq i \leq t_p$ . Since  $t_p$  is approximately  $p/24$ , Step (2) can be done overall in time  $O(p^{2.5+\epsilon})$ .

By earlier discussion and results from Cerviño [4], Steps (1), (3) and (4) can also be done within this running time. Hence the overall complexity of Algorithm 2 is  $O(p^{2.5+\epsilon})$ . We stress that in contrast to Algorithm 1, Algorithm 2 is guaranteed to always halt within this running time irrespective of Conjectures 5.1 and 5.2.

Finally, we remark that Algorithm 2 can be restricted to the case when  $j(\mathcal{O}) \in \mathbb{F}_p$ . It is possible to enumerate in Step (1) the maximal order types  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_{H(-4p)}$  whose  $j$ -invariants lie in  $\mathbb{F}_p$  in  $O(p^{0.5+\epsilon})$  field operations (from Kohel in a personal communication, 2012). From the analysis of Algorithm 1 under condition (2.3), we know that Step (2) of Algorithm 2 can be done in time  $O(p^{1+\epsilon})$  for every  $1 \leq i \leq H(-4p)$ . Since  $H(-4p) = O(p^{0.5+\epsilon})$ , this leads to a complexity of  $O(p^{1.5+\epsilon})$  in this restricted case.

### 6. Two examples

We give two examples of how Algorithm 1 runs, both constructed using Magma [3]; the code can be found on the second author’s webpage.

EXAMPLE 6.1. Let  $p = 61$ . The quaternion algebra  $B_{61}$  is spanned by  $\{1, i, j, k\}$  where  $i^2 = -61, j^2 = -7$  and  $k = ij = -ji$ . It can be checked that

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}(\frac{1}{2} + \frac{1}{2}j) + \mathbb{Z}(-\frac{1}{2} - \frac{1}{14}j + \frac{1}{7}k) + \mathbb{Z}(-\frac{1}{2} + \frac{1}{2}i - \frac{3}{14}j - \frac{1}{14}k)$$

is a maximal order of  $B_{61}$ .

We construct  $\mathcal{O}^T$  and find that its shortest element is  $y_1 = j$ . We set  $d_1 = \text{Nr}(y_1) = 7$ , and

$$G(X) = H_{-d_1}(X) = H_{-7}(X) = X - 41 \in \mathbb{F}_{61}[X].$$

We conclude that the  $j$ -invariant associated to the maximal order  $\mathcal{O}$  is  $j(\mathcal{O}) = 41 \in \mathbb{F}_p$ .

EXAMPLE 6.2. Let  $p = 20063$ . The quaternion algebra  $B_{20063}$  is spanned by  $\{1, i, j, k\}$  where  $i^2 = -20063, j^2 = -1$  and  $k = ij = -ij$ . We take  $\mathcal{O}$  as the maximal order in  $B_{20063}$  with  $\mathbb{Z}$ -basis

$$\begin{aligned} \mathcal{O} = & \mathbb{Z}(\frac{1}{2} + \frac{1}{16}j + \frac{13615}{16}k) + \mathbb{Z}(\frac{1}{512}i + \frac{151}{4096}j + \frac{1109113}{4096}k) \\ & + \mathbb{Z}(\frac{1}{8}j + \frac{13615}{8}k) + 2048\mathbb{Z}k. \end{aligned}$$

We construct  $\mathcal{O}^T$  and begin searching through its short elements. We find

$$y_1 = \frac{11}{64}i - \frac{8323}{512}j + \frac{51}{512}k,$$



which gives

$$d_1 = \text{Nr}(y_1) = 1056,$$

and

$$G_1(X) = H_{-d_1}(X) = H_{-1056}(X) \in \mathbb{F}_{20063}[X],$$

where  $\deg(H_{-1056}(X)) = 16$ .

Next we find

$$y_2 = \frac{67}{256}i + \frac{52101}{2048}j - \frac{85}{2048}k,$$

which gives

$$d_2 = \text{Nr}(y_2) = 2056,$$

and

$$G_2(X) = \text{gcd}(G_1(X), H_{-2056}(X)) = X^3 + 8728X^2 + 8070X + 5035 \in \mathbb{F}_{20063}[X],$$

where  $\deg(H_{-2056}(X)) = 16$ .

Next we find

$$y_3 = \frac{23}{256}i + \frac{85393}{2048}j - \frac{289}{2048}k$$

which gives

$$d_3 = \text{Nr}(y_3) = 2300,$$

and

$$G_3(X) = \text{gcd}(G_2(X), H_{-2300}(X)) = X^2 + 2748X + 6627 = (X - \alpha)(X - \bar{\alpha}) \in \mathbb{F}_{20063}[X],$$

where  $\deg(H_{-2300}(X)) = 18$  and  $\alpha, \bar{\alpha}$  form a conjugate pair.

Hence we conclude that  $\mathcal{O}$  corresponds to a conjugate pair of supersingular  $j$ -invariants,  $j(\mathcal{O}) = \alpha, \bar{\alpha}$  with minimal polynomial  $X^2 + 2748X + 6627$  over  $\mathbb{F}_{20063}$ .

Appendix. Proof of Theorem 2.2

We now describe the general strategy of the proof of Theorem 2.2. For further technical details see the full version of the paper (<http://arxiv.org/abs/1301.6875>).

As with Theorem 2.1, the first step is to take appropriate sublattices  $\langle x, y \rangle$  in  $\mathcal{O}^T$  and  $\langle x', y' \rangle$  in  $\mathcal{O}'^T$  and to show that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric. This is done by first proving that  $D'_1 = D_1$  and then that  $D'_2 = D_2$ . The final step is to extend to the full lattices  $\mathcal{O}^T$  and  $\mathcal{O}'^T$ .

A.1. Proving that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric

Since  $x$  and  $y$  represent the first two successive minima of  $\mathcal{O}^T$ , we have  $\text{Nr}(x + y) = \text{Nr}(x) + \text{Nr}(y) + \text{Tr}(x\bar{y}) \geq \text{Nr}(y)$  and likewise  $\text{Nr}(x - y) = \text{Nr}(x) + \text{Nr}(y) - \text{Tr}(x\bar{y}) \geq \text{Nr}(y)$ . It follows that  $|\text{Tr}(x\bar{y})| \leq \text{Nr}(x) = D_1$  as otherwise one of these two inequalities would not hold. We hence have  $\text{Tr}(x\bar{y}) = \mu D_1$  for some  $|\mu| \leq 1$ , and, without loss of generality, take  $-1 \leq \mu \leq 0$  (as otherwise we swap the sign of either  $x$  or  $y$ ). Similarly we will let  $\text{Tr}(x'\bar{y}') = \lambda D'_1$  with  $-1 \leq \lambda \leq 0$ .

LEMMA A.1. *Let notation be as above. Then  $-1 < \mu, \lambda \leq 0$  and  $D_1 \neq D_2$ .*

*Proof.* We first show that the cases  $\mu = -1$  and  $\lambda = -1$  are impossible. If  $\mu = -1$ , then  $\text{Nr}(y) = \text{Nr}(x + y)$ . Hence  $D_2$  would have two different optimal representations in  $\mathcal{O}^T$ , and so Kaneko [13, Theorem 2'] implies that  $D_2^2 \geq p^2$ . As  $D_3 \geq D_2$ , (4.1) would imply that  $D_1 D_2 D_3 \geq 15p^2 > 8p^2$ , which contradicts (4.3). So  $\mu = -1$  is indeed impossible. Similarly if  $\lambda = -1$ , then  $D_2'^2 \geq p^2$ . By (4.2) this would imply  $D_2 \geq p$ , and we again reach the same contradiction. The same application of Kaneko's result shows that  $D_1 \neq D_2$ .  $\square$



As shown in § 3,  $p \mid 4D_1D_2 - T^2$ . On [13, page 853], Kaneko obtains this result by writing  $\alpha_1 = (x + D_1)/2$  and  $\alpha_2 = (y + D_2)/2$ , defining  $s = \text{Tr}(\alpha_1\alpha_2)$ , and considering the quantity  $(D_1D_2 - (2s - D_1D_2)^2)/4$ . Note that  $2s - D_1D_2 = \text{Tr}(xy)/2 = -T/2$  so this is just  $(D_1D_2 - (T/2)^2)/4$ . It is straightforward to verify that

$$s = -\frac{\mu}{4}D_1 + \frac{1}{2}D_1D_2.$$

Substituting this value for  $s$ , we find that  $4p$  divides  $D_1(D_2 - \mu^2D_1/4)$ . The same result applies to  $\mathcal{O}^T$  (which is actually where we will use it), and so defining  $M := D'_1(D'_2 - \lambda^2D'_1/4)$ , it follows that

$$4p \leq M. \tag{A.1}$$

We remark that the above with (4.3) gives

$$4p \leq D_1D_2 \quad \text{and} \quad D_3 \leq 2p, \tag{A.2}$$

and in particular under conditions (4.1),

$$4p \leq D_1D_2 < \frac{16}{3}p \quad \text{and} \quad \frac{3}{4}p < D_3 \leq 2p. \tag{A.3}$$

We now begin to prove some technical lemmas. The following lemma will only be used in the context of maximal orders, but we remark that it can be readily generalized to all 2-dimensional lattices.

LEMMA A.2. *Under the condition  $\mu, \lambda \in (-1, 0]$ ,  $x + y$  is the next shortest element of  $\langle x, y \rangle$  after  $\pm y$  that is not in  $\langle x \rangle$ , and likewise  $x' + y'$  is the next shortest element of  $\langle x', y' \rangle$  after  $\pm y'$  that is not in  $\langle x' \rangle$ .*

*Proof.* One shows that  $\text{Nr}(ax + by) = a^2D_1 + b^2D_2 + ab\mu D_1$  will always exceed  $\text{Nr}(x + y) = D_1 + D_2 + \mu D_1$  for  $a, b \in \mathbb{Z}$  unless  $a = b = \pm 1$ . The details are omitted.  $\square$

The following lemma is the first of two technical lemmas, being Lemmas A.3 and A.4. In these lemmas we require bounds on  $D_1, D_1D_2$ , and sometimes on  $p$ , that we explicitly state. The bounds required by the following Lemma A.3 are the strictest and, unlike in Lemma A.4, we have not yet found a way to loosen them. If the bound on  $D_1D_2$  in the following lemma can be loosened, then the restriction imposed in Theorem 2.2 can be loosened as well.

LEMMA A.3. *Let notation be as in Notation 4.1. Assume  $D_1$  and  $D_2$  are both represented optimally by  $\mathcal{O}^T$ . Then  $D_1 = D'_1$  provided that*

$$D_1D_2 < \frac{16}{3}p \quad \text{and} \tag{A.4}$$

$$8 \leq D_1. \tag{A.5}$$

*Proof.* We first prove that the vectors of  $\mathcal{O}^T$  that optimally represent  $D_1$  and  $D_2$  lie in  $\langle x', y' \rangle$ . We recall that since  $D_1$  and  $D_2$  are represented optimally by  $\mathcal{O}'$ , we have (4.2). By (A.4) this implies  $D'_1D'_2 < 16p/3$ , and so from (4.3) we have

$$\frac{3}{4}p < \frac{4p^2}{D'_1D'_2} \leq D'_3.$$

Since the norm of the shortest element in  $\mathcal{O}^T$  outside  $\langle x', y' \rangle$  is  $D'_3$ , if  $D_2$  is represented outside  $\langle x', y' \rangle$  then  $3p/4 < D'_3 \leq D_2$  and hence

$$D_1 < \frac{16p}{3D_2} < \frac{64}{9} < 8,$$

which contradicts (A.5). So  $D_2$  cannot be represented outside  $\langle x', y' \rangle$ . Clearly  $D_1$  cannot be represented outside  $\langle x', y' \rangle$  either.

We now assume  $D_1 = \text{Nr}(ax' + by')$  with  $b \neq 0$ . This implies in particular that  $D'_2 \leq D_1$ , and so by (A.4) we have

$$D'_2 < \frac{4}{\sqrt{3}}\sqrt{p}. \tag{A.6}$$

From Lemma A.2, we know that  $x' + y'$  is the next shortest element after  $\pm y'$  in  $\langle x', y' \rangle \setminus \langle x' \rangle$ , and we recall from Lemma A.1 that  $\lambda \in (-1, 0]$  and  $D_1 \neq D_2$ . The latter implies that  $D_1$  and  $D_2$  must have different optimal representations in  $\mathcal{O}^T$ , and so it follows that  $\text{Nr}(x' + y') = D'_2 + (1 + \lambda)D'_1 \leq D_2$ . Combined with  $D'_2 \leq D_1$ , we have that

$$D'_2(D'_2 + (1 + \lambda)D'_1) \leq D_1D_2 < \frac{16}{3}p. \tag{A.7}$$

We recall the definition  $M = D'_1(D'_2 - \lambda^2 D'_1/4)$  and define

$$K = \frac{1}{1 + \lambda} \left( \frac{16p}{3D'_2} - D'_2 \right).$$

We will show that  $M < 4p$  under the constraints

$$D'_1 \leq \min\{D'_2, K\},$$

and this will be a contradiction to (A.1).

We consider two cases depending on whether or not  $D'_2 \leq K$ . Note that this happens exactly when  $(D'_2)^2(2 + \lambda) \leq 16p/3$ .

First note that  $M$  is maximized when  $D'_1$  is as large as possible. In the case  $(D'_2)^2(2 + \lambda) \leq 16p/3$  this means  $D'_1 = D'_2$  and so

$$M \leq D_2^2 \left( \frac{4 - \lambda^2}{4} \right) \leq \frac{16}{3}p \frac{1}{\lambda + 2} \left( \frac{4 - \lambda^2}{4} \right) < 4p.$$

In the case  $(D'_2)^2(2 + \lambda) > 16p/3$  we take  $D'_1 = K$ . Writing  $\gamma = (D'_2)^2$  we have

$$M \leq \frac{1}{4(1 + \lambda)^2\gamma} \left( \frac{16}{3}p - \gamma \right) \left( \gamma(\lambda + 2)^2 - \lambda^2 \frac{16}{3}p \right). \tag{A.8}$$

The right-hand side of (A.8) is subject to the constraints  $\gamma = D_2^2 \leq D_1^2 < 16p/3$  (which comes from (A.6)) and  $16p < 3(\lambda + 2)\gamma$ . It is then routine to verify that the right-hand side of (A.8) is maximized when  $\gamma$  is minimal, that is,  $\gamma = 16/(3(\lambda + 2))p$  (a simple way to verify this is to compute the partial derivative of the right-hand side of (A.8) with respect to  $\gamma$  and observe that it is negative when  $16|\lambda|p < 3(\lambda + 2)\gamma$ ). Substituting  $\gamma = 16/(3(\lambda + 2))p$  into the right-hand side of (A.8) reduces it to  $4(2 - \lambda)p/3$ , which for  $\lambda \in (-1, 0]$  is always less than  $4p$ .

Hence, in both cases, we obtain that  $M < 4p$ , which contradicts (A.1). In conclusion, if  $D_1$  and  $D_2$  are both represented optimally by  $\mathcal{O}^T$  with  $D_1 = \text{Nr}(ax' + by')$ , then we must have  $b = 0$  and it follows that  $a = 1$  and  $D_1 = D'_1$ .  $\square$

LEMMA A.4. *Let notation be as in Notation 4.1. Assume  $D_1 = D'_1$  and that  $D_2, \text{Nr}(x + y)$  and  $\text{Nr}(x - y)$  are all represented optimally by  $\mathcal{O}^T$ . Then  $x \sim x', y \sim y'$  and  $x + y \sim x' + y'$  (and so  $\langle x, y \rangle \sim \langle x', y' \rangle$  by Lemma 4.3) provided that*

$$D_1D_2 < 7p, \tag{A.9}$$

$$15 \leq D_1, \quad \text{and} \tag{A.10}$$

$$286 < p. \tag{A.11}$$

*Proof.* This is the longest proof in the paper. Due to lack of space, we refer to the full version of the paper for all details of the proof.

In light of Lemma 3.2, it suffices to prove that  $D_2 = D'_2$  and  $\text{Nr}(x + y) = \text{Nr}(x' + y')$  since all vectors in question have zero trace.

Recall that  $\text{Nr}(x + y) = (1 + \mu)D_1 + D_2$  and  $\text{Nr}(x' + y') = (1 + \lambda)D'_1 + D'_2$  where  $-1 < \mu, \lambda \leq 0$ . To avoid trivial cases later on, one can check (details omitted) that  $\mu, \lambda \neq 0$ .

One can also check (details omitted) that the vectors in  $\mathcal{O}^T$  that represent  $\text{Nr}(x)$ ,  $\text{Nr}(y)$ ,  $\text{Nr}(x + y)$  and  $\text{Nr}(x - y)$  all lie in  $\langle x', y' \rangle$ .

Hence assume  $D_2 = \text{Nr}(ax' + by')$  for some  $a, b \in \mathbb{Z}$ . Remarking that  $a(a + b\lambda) \geq -(\lambda b/2)^2$ , and recalling that  $D_1 = D'_1$  by assumption, we obtain

$$D_2 = a^2D'_1 + b^2D'_2 + ab\lambda D'_1 = aD'_1(a + b\lambda) + b^2D'_2 \geq b^2D'_2 - \left(\frac{\lambda b}{2}\right)^2 D_1,$$

which implies  $D'_2 \leq D_2/b^2 + \lambda^2 D_1/4$ . Hence by (A.9), for  $|b| \geq 2$  we have

$$M = D'_1D'_2 - \frac{\lambda^2}{4}D_1^2 \leq D_1\left(\frac{1}{b^2}D_2 + \frac{\lambda^2}{4}D_1\right) - \frac{\lambda^2}{4}D_1^2 = \frac{D_1D_2}{b^2} < 4p,$$

which contradicts (A.1), and so we must have  $|b| = 1$ . Without loss of generality, (changing the sign of  $a$  if necessary), we can take  $b = 1$ .

Now let  $\text{Nr}(x + y) = (1 + \mu)D_1 + D_2 = \text{Nr}(cx' + dy') = c^2D'_1 + d^2D'_2 + cd\lambda D'_1$ . Remarking as before that  $c(c + d\lambda) \geq -(\lambda d/2)^2$ , we obtain

$$\text{Nr}(x + y) = D_1(1 + \mu) + D_2 \geq d^2D'_2 - \left(\frac{\lambda d}{2}\right)^2 D_1.$$

This with (A.9) implies that, for  $|d| \geq 2$ , we have

$$M = D'_1D'_2 - \frac{\lambda^2}{4}D_1^2 \leq D_1\frac{D_1(1 + \mu) + D_2 + (\lambda^2d^2/4)D_1}{d^2} - \frac{\lambda^2}{4}D_1^2 \leq \frac{2D_1D_2}{d^2} < 4p,$$

which again contradicts (A.1), and so we must have  $|d| = 1$ . Without loss of generality, (changing the sign of  $c$  if necessary), we can take  $d = 1$ .

Since  $D_1 = D'_1$  and  $b = d = 1$ , we have

$$D_2 = a(a + \lambda)D_1 + D'_2 \quad \text{and} \tag{A.12}$$

$$D_1(1 + \mu) + D_2 = c(c + \lambda)D_1 + D'_2. \tag{A.13}$$

We observe that  $a \neq c$  since otherwise  $\mu = -1$ , which is impossible from before. So subtracting (A.12) from (A.13), factorizing and dividing, gives us

$$\frac{1 + \mu}{c - a} = a + c + \lambda. \tag{A.14}$$

We observe that if  $a = 0$  then  $1 + \mu = c(c + \lambda)$ , where the left-hand side is in  $(0, 1)$ , which implies from the right-hand side that  $c = 1$ . But this implies that  $D_2 = D'_2$  and  $\text{Nr}(x + y) = \text{Nr}(x' + y')$  as desired, and we conclude by Lemma 3.2.

So we assume now that  $a \neq 0$ . We note that if  $a = 1$ , then (A.14) becomes  $1 + \mu = c(c + \lambda) - 1 - \lambda$ , from which we see that the only possible solution (since the left-hand side is again in  $(0, 1)$ ) is  $c = -1$  and  $\lambda = -(1 + \mu)/2 \in (-1/2, 0)$ .

We now claim that

$$D_2 < \frac{7}{4}D'_2. \tag{A.15}$$

Indeed, if this was not the case, by (A.9) we would have

$$M \leq D'_1 D'_2 \leq \frac{4}{7} D_1 D_2 < 4p,$$

which contradicts (A.1).

Now (A.15) and (A.12) imply that  $a(a + \lambda)D_1 + D'_2 = D_2 \leq 7D'_2/4$ . We remark that  $a(a + \lambda) > 0$  for all integers  $a \neq 0$ . Hence we have

$$D_1 \leq \frac{3D'_2}{4a(a + \lambda)}. \tag{A.16}$$

Now let  $\text{Nr}(x - y) = (1 - \mu)D_1 + D_2 = \text{Nr}(ex' + fy') = e^2D'_1 + f^2D'_2 + e f \lambda D'_1$ . We remark that  $e^2 + \lambda e f \geq -(\lambda f/2)^2$ , and so with (A.16), we have

$$\begin{aligned} D_2 &\geq f^2 D'_2 + \left( -\left(\frac{\lambda f}{2}\right)^2 - (1 - \mu) \right) D_1 \geq D'_2 \left( f^2 - \frac{3}{4a(a + \lambda)} \left( 1 - \mu + \frac{\lambda^2 f^2}{4} \right) \right) \\ &= D'_2 \left( f^2 \left( 1 - \frac{3\lambda^2}{16a(a + \lambda)} \right) - \frac{3(1 - \mu)}{4a(a + \lambda)} \right). \end{aligned} \tag{A.17}$$

We observe that for all  $\lambda \in (-1, 0)$  and  $a \in \mathbb{Z}$ , with  $a \neq 0$ , and with  $\lambda \in (-\frac{1}{2}, 0)$  when  $a = 1$ , it holds that

$$\delta = 1 - \frac{3\lambda^2}{16a(a + \lambda)} > 0.$$

Hence for all  $|f| \geq 2$ , it holds that

$$D_2 \geq D'_2 \left( 4\delta - \frac{3(1 - \mu)}{4a(a + \lambda)} \right) \geq D'_2 \left( 4 - \frac{3(1 - \mu + \lambda^2)}{4a(a + \lambda)} \right). \tag{A.18}$$

By separating into the cases  $a \leq -2, a = -1, a = 1$  and  $a \geq 2$ , it can be readily checked that for  $\lambda, \mu \in (-1, 0)$  and  $a \in \mathbb{Z}$ , with  $a \neq 0$ , and with  $\lambda = -(1 + \mu)/2$  when  $a = 1$ , it holds that

$$\frac{1 - \mu + \lambda^2}{a(a + \lambda)} \leq \frac{5}{2},$$

with equality only in the case that  $a = 1$  and  $\mu = 0, \lambda = -\frac{1}{2}$ . As a result,

$$D_2 \geq D'_2 \left( 4 - \frac{15}{8} \right) > \frac{7}{4} D'_2,$$

which contradicts (A.15). We conclude that  $|f| \geq 2$  is impossible, and hence, without loss of generality, we take  $f = 1$ .

We now have

$$D_1(1 - \mu) + D_2 = eD_1(e + \lambda) + D'_2. \tag{A.19}$$

Viewing (A.12) and (A.19), we observe that  $e \neq a$ , as otherwise we would have  $\mu = 1$ , which is impossible. Hence subtracting (A.12) from (A.19) we obtain

$$\frac{1 - \mu}{e - a} = a + e + \lambda. \tag{A.20}$$

Viewing this in conjunction with (A.14), it remains to find the possible solutions to (A.14) and (A.20) with  $a, c, e \in \mathbb{Z}, a \neq 0$ , and  $\lambda, \mu \in (-1, 0)$ . We omit the elementary calculations. The conclusion is that the only possible solution to  $D_2 = \text{Nr}(ax' + by')$ ,  $\text{Nr}(x + y) = \text{Nr}(cx' + dy')$  and  $\text{Nr}(x - y) = \text{Nr}(ex' + fy')$  is  $a = 0, b = 1, c = 1, d = 1, e = -1, f = 1$  (and the corresponding negative solutions if we wish to change signs). This implies by Lemma 3.2 that  $y \sim y'$  and  $x + y \sim x' + y'$  as desired.  $\square$

A.2. *Completing the proof*

We have shown that  $\langle x, y \rangle$  and  $\langle x', y' \rangle$  are isometric. Hence, by Lemma 4.3, we can conjugate  $\mathcal{O}$  by an appropriate element  $c \in B_p$  and hence assume that  $\langle x, y \rangle = \langle x', y' \rangle$ . It remains to deal with  $D_3$ . After conjugation, we have that  $\mathcal{O}^T = \langle x, y, z \rangle$  and  $\mathcal{O}'^T = \langle x, y, z' \rangle$  where  $\text{Nr}(z) = D_3$  and  $\text{Nr}(z') = D'_3$ . Since  $z, z' \notin \langle x, y \rangle$  and  $\theta'_{\mathcal{O}^T}(D_3) \leq \theta'_{\mathcal{O}'^T}(D_3)$  it follows that  $D'_3 \leq D_3$ . The next result shows that we may assume  $D'_3 = D_3$ , in which case the proof will follow from the argument used to prove Theorem 2.1.

LEMMA A.5. *Let notation be as in Notation 4.1. Suppose that  $\langle x, y \rangle = \langle x', y' \rangle$ . Suppose furthermore that there exists  $w \in \mathcal{O}^T$ ,  $w \notin \langle x, y \rangle$ , such that  $\text{Nr}(w) = D_3$ . It holds that  $w = \pm z'$ .*

*Proof of Lemma A.5.* As in Lemma 4.5 we let  $u$  and  $u'$  be the projections of  $z$  and  $z'$  to  $\langle x, y \rangle^\perp$ . We want to show that  $u' = \pm u$ . Lemma 4.4 shows that

$$\det(\mathcal{O}^T) \leq \det(\langle x, y \rangle) \text{Nr}(z) \leq D_1 D_2 D_3 \leq 2 \det(\mathcal{O}^T),$$

from which it follows that

$$\text{Nr}(z) = D_3 \leq \frac{2 \det(\mathcal{O}^T)}{\det(\langle x, y \rangle)}. \tag{A.21}$$

On the other hand, as  $D_3$  is represented by  $w \in \mathcal{O}'^T = \langle x, y, z' \rangle$  outside of  $\langle x, y \rangle$ , we have that  $w = ax + by + cz'$  for some  $a, b, c \in \mathbb{Z}$ ,  $c \neq 0$ . Therefore

$$D_3 = \text{Nr}(w) = \text{Nr}(ax + by + cz') \geq c^2 \text{Nr}(u') = c^2 \frac{\det(\mathcal{O}^T)}{\det(\langle x, y \rangle)},$$

where the last equality comes from (4.8). Hence  $c = \pm 1$  as required. □

*Proof of Theorem 2.2.* Assume that  $D_1, D_2, \text{Nr}(x + y), \text{Nr}(x - y)$  and  $D_3$  are all optimally represented in  $\mathcal{O}'^T$  and that  $\theta'_{\mathcal{O}^T}(D_3) \leq \theta'_{\mathcal{O}'^T}(D_3)$ . The case  $D_1 < 15$  is treated by Lemma 4.1 so we assume conditions (4.1). From Lemma A.2, we know that  $D'_1 = D_1$ . Hence, from Lemma A.4, we have that  $y \sim y'$  and  $x + y \sim x' + y'$ . By Lemma 4.3, conjugating  $\mathcal{O}'$  by an appropriate element  $c \in B_p$ , we can assume that  $\langle x, y \rangle = \langle x', y' \rangle$ . Now, in order that  $\theta'_{\mathcal{O}^T}(D_3) \leq \theta'_{\mathcal{O}'^T}(D_3)$ , we require that  $D_3$  is represented in  $\mathcal{O}'^T$  outside of  $\langle x, y \rangle$ . Hence, by Lemma A.5 we may assume that  $D'_3 = D_3$ . Lemma 4.5 then implies  $\mathcal{O}^T = \mathcal{O}'^T$ . Lemma 3.3 implies that  $\mathcal{O}$  and  $\mathcal{O}'$  are of the same type as desired. This completes the proof. □

*Acknowledgements.* We are very grateful to David Kohel for answering our questions about quaternion algebras and to John Voight for his helpful discussions.

References

1. A. V. AHO, J. E. HOPCROFT and J. D. ULLMAN, *The design and analysis of computer algorithms* (Addison-Wesley, Reading, MA, 1974).
2. J. BELDING, R. BRÖKER, A. ENGE and K. LAUTER, ‘Computing Hilbert class polynomials’, *ANTS-VIII*, Lecture Notes in Computer Science 5011 (eds A. J. van der Poorten and A. Stein; Springer, 2008) 282–295.
3. W. BOSMA, J. CANNON and C. PLAYOUST, ‘The Magma algebra system I: the user language’, *J. Symbolic Comput.* 24 (1997) 235–265.
4. J. M. CERVIÑO, ‘On the correspondence between supersingular elliptic curves and maximal quaternionic orders’, *Mathematisches Institut Georg-August-Universität Göttingen Seminars Summer Term 2004* (Universitätsverlag Göttingen, 2004) 53–60.
5. D. X. CHARLES, K. E. LAUTER and E. Z. GOREN, ‘Cryptographic hash functions from expander graphs’, *J. Cryptology* 22 (2009) no. 1, 93–113.

6. D. A. COX, *Primes of the form  $x^2 + ny^2$*  (Wiley, 1989).
7. N. ELKIES, K. ONO and T. YANG, 'Reduction of CM elliptic curves and modular function congruences', *Int. Math. Res. Not. IMRN* 44 (2005) 2695–2707.
8. J. VON ZUR GATHEN and J. GERHARD, *Modern computer algebra* (Cambridge University Press, 1999).
9. S. GOLDWASSER and D. MICCIANCIO, *Complexity of lattice problems: a cryptographic perspective* (Kluwer, 2002).
10. M. HENK, 'Successive minima and lattice points', *Rend. Circ. Mat. Palermo (2) Suppl.* (2002) 377–384.
11. T. IBUKIYAMA, 'On maximal orders of division quaternion algebra over the rational number field with certain optimal embeddings', *Nagoya Math. J.* 88 (1982) 181–195.
12. B. KANE, 'Representations of integers by ternary quadratic forms and CM liftings of supersingular elliptic curves', PhD Thesis, University of Wisconsin-Madison, 2006.
13. M. KANEKO, 'Supersingular  $j$ -invariants as singular moduli mod  $p$ ', *Osaka J. Math.* 26 (1989) 849–855.
14. D. KOHEL, 'Endomorphism rings of elliptic curves over finite fields', PhD Thesis, University of California at Berkeley, 1996.
15. A. PIZER, 'An algorithm for computing modular forms on  $\Gamma_0(N)$ ', *J. Algebra* 64 (1980) no. 2, 340–390.
16. A. SCHIEMANN, 'Ternary positive definite quadratic forms are determined by their theta series', *Math. Ann.* 308 (1997) 507–517.
17. C. L. SIEGEL, *Lectures on the geometry of numbers* (Springer, 1989).
18. A. V. SUTHERLAND, 'Computing Hilbert class polynomials using the Chinese remainder theorem', *Math. Comp.* 80 (2011) 501–538.
19. A. V. SUTHERLAND, 'On the evaluation of modular polynomials', *Algorithmic Number Theory 10th International Symposium (ANTS X)*, Open Book Series 1 (eds E. W. Howe and K. S. Kedlaya; Mathematical Sciences Publishers, 2013) 531–555.
20. A. V. SUTHERLAND, 'Isogeny volcanoes', *Algorithmic Number Theory 10th International Symposium (ANTS X)*, Open Book Series 1 (eds E. W. Howe and K. S. Kedlaya; Mathematical Sciences Publishers, 2013) 507–530.
21. M.-F. VIGNÉRAS, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics 800 (Springer, 1980).
22. T. YANG, 'Minimal CM liftings of supersingular elliptic curves', *Pure Appl. Math. Q.* 4 (2008) no. 4, 1317–1326.

Ilya Chevyrev  
 Mathematical Institute  
 University of Oxford  
 United Kingdom

[ilya.chevyrev@maths.ox.ac.uk](mailto:ilya.chevyrev@maths.ox.ac.uk)

Steven D. Galbraith  
 Mathematics Department  
 University of Auckland  
 New Zealand

[S.Galbraith@math.auckland.ac.nz](mailto:S.Galbraith@math.auckland.ac.nz)