Structural results for maximal quaternion orders and connecting ideals of prime power norm in $B_{p,\infty}$

James Clements

University of Bristol

January 2025

Abstract. Fix odd primes p, ℓ with $p \equiv 3 \mod 4$ and $\ell \neq p$. Consider the rational quaternion algebra ramified at p and ∞ with a fixed maximal order $\mathcal{O}_{1728}$. We give explicit formulae for bases of all cyclic norm ℓ^n ideals of $\mathcal{O}_{1728}$ and their right orders, in Hermite Normal Form (HNF). Further, in the case $\ell \mid p+1$, or more generally, $-p$ is a square modulo ℓ, we derive a parametrization of these bases along paths of the ℓ-ideal graph, generalising the results of [1]. With such orders appearing as the endomorphism rings of supersingular elliptic curves defined over $\overline{\mathbb{F}_p}$, we note several potential applications to isogeny-based cryptography including fast ideal sampling algorithms. We also demonstrate how our findings may lead to further structural observations, by using them to prove a result on the successive minima of endomorphism rings of supersingular curves defined over $\mathbb{F}_p$.

1 Introduction

Take a prime $p \equiv 3 \mod 4$ and consider the quaternion algebra $B_{p,\infty} = \langle 1, i, j, k \rangle_{\mathbb{Q}}$ with $i^2 = -1$, $j^2 = -p$ and $k = ij = -ji$. For large p, the study of maximal orders and their connecting ideals in $B_{p,\infty}$ is particularly relevant to the field of isogeny-based cryptography. The security of every isogeny-based scheme relies on the assumption that computing the ring of endomorphisms of a random supersingular elliptic curve over $\overline{\mathbb{F}_p}$ is hard. Under the Deuring correspondence [10], such an endomorphism ring is isomorphic to a maximal quaternion order in $B_{p,\infty}$, with isogenies of degree N corresponding to left ideals of norm N. Hence the more we learn about these orders and ideals, the more we learn about security of isogeny-based schemes. Additionally under the correspondence, certain problems for elliptic curves can be translated to problems in quaternion algebras, where properties of quaternion algebras can make them easier to solve. This has led to several constructive applications leveraging quaternions such as the KLPT algorithm [13] used by the digital signature scheme SQISign [9].

In this work we give new structural results on the bases of maximal orders in $B_{p,\infty}$ and connecting ideals between them. We restrict to only consider ideals of odd prime power norm ℓ^n. This remains cryptographically relevant as: many isogeny-based schemes use isogenies of prime power degree, most famously SIDH

[12] (now broken [5, 14, 15]); and in general, any separable isogeny can be decomposed into a chain of isogenies of prime power degree. We also restrict to ideals with a specific left-order, corresponding to the endomorphism ring of the curve $E_{1728} : y^2 = x^3 + x$, with j-invariant 1728, which is often chosen as the starting curve for isogeny-based schemes.

The structure of maximal quaternion orders has been previously studied in depth, for instance see the results of Ibukiyama [11]. Only recently has their structure been considered in relation to isogeny paths. In [1], the authors made a first attempt to parametrize the bases of maximal orders along ℓ^n-isogeny paths from E_{1728}, through a connection to paths in Bruhat-Tits trees given in [2]. Essentially this means at each point in the walk, one may assign a direction $d_i \in \{0, ..., \ell\}$ for the next step. The basis of the resulting maximal order can then be determined simply from p, ℓ, n and the directions taken $(d_0, ..., d_{n-1})$. Their methods came with several restrictions however. They were limited to only use degree ℓ^n isogenies with kernels defined over $\mathbb{F}_{p^2}$, meaning for a prime $p = 4\ell^e f - 1$ the path length was restricted $n \leq e$. Combining this with the fact their paths must start from E_{1728}, when f is large the results only apply to a relatively small proportion of the isomorphism classes of maximal orders; those corresponding to curves close to E_{1728}.

Our findings include a generalisation of their result. While we will also work with ℓ^n isogenies from E_{1728}, we remove the restriction on n, and so cover all isomorphism classes of maximal quaternion orders. Also we do not require $\ell \mid p - 1$, only that $-p$ is a square mod ℓ. When $-p$ is not a square mod ℓ we do not achieve a parametrization, but still present new structural results for norm ℓ^n ideals and their right orders. We also briefly mention potential applications of these results, and use them to prove a statement regarding the successive minima of the endomorphism rings of curves defined over $\mathbb{F}_p$.

Some proofs are assisted using SageMath [16], with code available online at: `https://github.com/jtcc2/structural-results-for-quaternion-orders-and-ideals`.

Contributions

We now give a detailed summary of our findings.

Take odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$. Let $\mathcal{O}_{1728}$ be the maximal quaternion order in $B_{p,\infty}$,

$$\mathcal{O}_{1728} = \left\langle \frac{1+j}{2},\ \frac{i+k}{2},\ j,\ k \right\rangle_{\mathbb{Z}}$$

which is isomorphic to the endomorphism ring of the curve $E_{1728} : y^2 = x^3 + x$ over $\overline{\mathbb{F}_p}$, with j-invariant 1728. Let $\delta(P) = 1$ when a property P holds and 0 otherwise. We show (Theorem 1) for any integer $n \geq 1$, the set of $\mathbb{Z}$-lattices of the form,

$$\left\langle \begin{array}{rr} \frac{1}{2} + \frac{\ell^a}{2} j + \frac{C + \delta(2 \nmid C) \cdot \ell^{b+c}}{2\ell^c} k, & \frac{1}{2\ell^{a+b}} i + \frac{A}{\ell^n} j + \frac{B}{2\ell^b} k, \\ \ell^a j + \frac{C}{\ell^c} k, & \ell^b k \end{array} \right\rangle_{\mathbb{Z}} \qquad (*)$$

where $S = (A, B, C, a, b, c) \in \mathbb{Z}^6$ satisfy the conditions below, is exactly the set right orders of cyclic norm ℓ^n left $\mathcal{O}_{1728}$-ideals, and the basis above is in Hermite Normal Form.

Precisely the conditions on S are: (1) either, $0 \leq a, b \leq n$ with $a + b = n$, or $-n \leq a \leq 0$ and $b = n$; (2) $C \in \mathbb{Z}$ with $0 \leq C < \ell^{b+c}$, and $c = 0$ if $a \geq 0$ otherwise $c = -a$; (3) $0 \leq A < \ell^{n+a}$ and $0 \leq B < 2\ell^{2b}$; (4) B is odd, (5) $\alpha - 4A^2$ is divisible by $\ell^{2(n-b)}$, where α is the unique solution to $\alpha p \equiv -\ell^{2n-2a-2b}$ mod $2\ell^{2n}$; (6) $\frac{\alpha - 4A^2}{\ell^{2(n-b)}}$ is a square modulo $2\ell^{2b}$; (7) B is one of the square roots of $\frac{\alpha - 4A^2}{\ell^{2(n-b)}}$ modulo $2\ell^{2b}$; (8) $2A + BC \equiv 0 \mod \ell^{b+c}$; and (9) $\ell^{2c} \mid 1 + C^2$.

That is to say for any cyclic norm ℓ^n ideal from $\mathcal{O}_{1728}$, there is a unique tuple S satisfying the above conditions such that its right order equals (*). And conversely, for any tuple S satisfying the conditions, the $\mathbb{Z}$-lattice (*) is the right order of a cyclic norm ℓ^n ideal.

Furthermore we show (Theorem 2) for an order $\mathcal{O}$ defined by (*), the norm ℓ^n connecting ideal[1] from $\mathcal{O}_{1728}$ to $\mathcal{O}$ is,

$$\left\langle \begin{array}{rr} \frac{1}{2} - \frac{C}{2} i + \frac{B\ell^{a+c} - 2AC}{2\ell^c} j - \frac{2A + BC\ell^{a+c}}{2\ell^c} k, & \frac{\ell^{n-a-b}}{2} i + Aj + \frac{B\ell^{a+c}}{2} k, \\ \ell^{a+b} j + C\ell^{a+b} k, & \ell^n k \end{array} \right\rangle_{\mathbb{Z}}.$$

While these formula may seem complex, they simplify significantly in specific circumstances. We show (Proposition 1) when $\ell \equiv 3 \mod 4$ and p is a square mod ℓ, that we always have $(a, b, c) = (0, n, 0)$, and in the ideal result above, may set $C = 0$. As another example, we consider taking $n = 1$ (Theorem 4), and observe the set of left $\mathcal{O}_{1728}$-ideals of any odd prime norm ℓ, is exactly the disjoint union of 3 simpler sets,

$$\begin{aligned} &\{I_1(x) : 0 \leq x < \ell \text{ solves } x^2 \equiv -1 \mod \ell\} \\ \dot\cup\ &\{I_2(x) : 0 \leq x < \ell \text{ solves } 4px^2 \equiv -1 \mod \ell\} \\ \dot\cup\ &\left\{I_3(x, y) : 0 \leq x < \ell, 0 \leq y < 2\ell^2 \text{ solve } -py^2 \equiv 1 + 4px^2 \not\equiv \ell^2 \mod 2\ell^2\right\} \end{aligned}$$

where

$$\begin{aligned} I_1(x) &= \left\langle \frac{1}{2} + \frac{\ell - x}{2} i + \frac{1}{2} j + \frac{\ell + x}{2} k,\ \frac{\ell}{2} i + \frac{\ell}{2} k,\ j + xk,\ \ell k \right\rangle_{\mathbb{Z}}, \\ I_2(x) &= \left\langle \frac{1}{2} + \frac{\ell}{2} j + (\ell - x)k,\ \frac{1}{2} i + xj + \frac{\ell}{2} k,\ \ell j,\ \ell k \right\rangle_{\mathbb{Z}}, \\ I_3(x, y) &= \left\langle \frac{1}{2} + \frac{y}{2} j + (\ell - x)k,\ \frac{1}{2} i + xj + \frac{y}{2} k,\ \ell j,\ \ell k \right\rangle_{\mathbb{Z}}. \end{aligned}$$

[1] Warning. This basis is not necessarily in Hermite Normal Form.

And we obtain a similar result for their right orders (Theorem 3).

We now discuss our main theorem (Theorem 5), a parametrization result generalising that of [1]. Suppose ℓ is an odd prime such that $p \neq \ell$ and $-p$ is a square mod ℓ (e.g. take $\ell \mid p+1$). Again take an integer $n \geq 1$. We show how to derive all tuples $S = (A, B, C, a, b, c)$, satisfying the earlier conditions, from a single variable d. This means we derive bases of all cyclic norm ℓ^n ideals from $\mathcal{O}_{1728}$, and their right orders, from d. As a parametrization, the value d, through its base ℓ expansion, encodes the directions taken at each step in the ideal/isogeny walk. For $d = \sum_{r=0}^{n-1} d_r \ell^r$ giving rise to a norm ℓ^n ideal $I = I_1 I_2 ... I_n$, the direction taken by each ℓ-ideal I_r is encoded by $0 \leq d_r < \ell$. In the special case $p = 4\ell^e f - 1$ and $n \leq e$, we show our allocation of directions coincides with [1], and so the corresponding isogeny has kernel $\langle \ell^{e-n}(P + dQ) \rangle$ or $\langle \ell^{e-n}(dP + Q) \rangle$ for a particular basis P, Q of the ℓ^e-torsion on E_{1728}.

In the simpler case of $\ell \equiv 3 \mod 4$, we derive all cyclic norm ℓ^n ideals from $\mathcal{O}_{1728}$ as follows. First we fix r such that $r^2 \equiv -p \mod \ell^{2n}$. Then for every $0 \leq d \leq \ell^n - 1$ such that $\ell \nmid d^2 + 1$, define $a \leq n$ maximal such that $\ell^a \mid d$, and let $d' = \frac{d}{\ell^a}$. Let x, y, z be the unique solutions to $x \cdot 2r(d^2+1) \equiv d^2 - 1 \mod \ell^{2n}$, $y \cdot r(d^2+1) \equiv -d' \mod \ell^{2n-2a}$ and $z \cdot 2d' \equiv d^2 - 1 \mod \ell^{n-a}$. Then the following $\mathbb{Z}$-lattice is a norm ℓ^n ideal from $\mathcal{O}_{1728}$,

$$I_d = \left\langle \frac{1}{2} + \left(y\ell^a + \frac{\ell^n}{2} \right) j - xk, \;\; \frac{1}{2} i + xj + \left(y\ell^a + \frac{\ell^n}{2} \right) k, \;\; \ell^n j, \;\; \ell^n k \right\rangle_{\mathbb{Z}}.$$

And when $\ell \mid d$, so is,

$$J_d = \left\langle \frac{1}{2} + \left(y\ell^a + \frac{\ell^n}{2} \right) j + xk, \;\; \frac{1}{2} i - xj + \left(y\ell^a + \frac{\ell^n}{2} \right) k, \;\; \ell^n j, \;\; \ell^n k \right\rangle_{\mathbb{Z}}.$$

Varying d, the ideals I_d (and J_d when $\ell \mid d$) are all distinct. The right orders of I_d and J_d are simply the $\mathbb{Z}$-lattices of (*) from tuples $(x, 2y + \ell^{2n-2a}, z, a, n-a, 0)$ and $(-x, 2y + \ell^{2n-2a}, \ell^{n-2a} - z, a, n-a, 0)$ respectively. For the $\ell \equiv 1 \mod 4$ case, see Theorem 5 Part B..

Applications

We note the following direct applications of our results.

- *Investigating structural properties of maximal orders in special cases.* For example, in Section 7 we prove the following result. For a prime $p \equiv 3 \mod 4$ and $\mathcal{O} \subset B_{p,\infty}$ a maximal quaternion order for which there is a primitive embedding of $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, then the third successive minima of the Gross lattice $\mathcal{O}^T$ is exactly p. While this result is not entirely new, existing approaches to its proof are certainly non-trivial. Hence this showcases the applicability of our main theorems for proving similar claims.
- *Ideal sampling algorithms.* Our parametrization result (Theorem 5) gives an alternative polynomial time algorithm for uniformly sampling a random norm ℓ^n ideal of $\mathcal{O}_{1728}$. This can be applied to any maximal order $\mathcal{O}$ by

computing the connecting ideal J from $\mathcal{O}_{1728}$ to $\mathcal{O}$, sampling a random $\mathcal{O}_{1728}$-ideal I, then computing the push-forward of I through J. Similarly it can be repeatedly used to sample ideals of any fixed (odd) norm, although the more distinct factors of the norm, the slower the performance will be. It is also potentially implementable in constant-time.

For completeness we also restate the following applications suggested in [1], although provide no further advancement. The additional structure provided by a parametrization of the basis of norm ℓ^n ideals from $\mathcal{O}_{1728}$ and their right orders could aid in further study of finding optimal solutions the quaternion ℓ-isogeny problem [13]. Furthermore our parametrization is well suited for computing the norm forms (including trace-zero norm forms) of orders along an ℓ-isogeny path. Examining these parametrised norm forms, could aid our understanding of the degrees and traces which appear from endomorphisms of different supersingular elliptic curves.

Acknowledgements

This work was funded by EPSRC grant number EP/S022465/1.

2 Background

This section covers some prerequisites. For a more complete picture of quaternion algebras we recommend the book [17].

2.1 Quaternion Algebra $B_{p,\infty}$

The quaternion algebra $B = (a, b)_{\mathbb{Q}}$ with $a, b \in \mathbb{Q}$ is a 4 dimensional non-commutative algebra over $\mathbb{Q}$ with elements written $x = x_0 + x_1 i + x_2 j + x_3 ij$ for $x_r \in \mathbb{Q}$ and multiplication defined by $i^2 = a$, $j^2 = b$, and $ij = -ji$, often defining $k \coloneqq ij$ for simplicity. Each quaternion has a *conjugate* $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij$, a *(reduced) trace* $\mathrm{Tr}(x) = x + \overline{x} = 2x_0$, a *(reduced) norm* $\mathrm{nrd}(x) = x\overline{x}$, an inverse $x^{-1} = \frac{\overline{x}}{\mathrm{nrd}(x)}$, and each $x \notin \mathbb{Q}$ satisfies a quadratic minimal polynomial $x^2 - \mathrm{Tr}(x)x + \mathrm{nrd}(x) = 0$. Taking the norm of an arbitrary element gives a rational quadratic form $(x_0, x_1, x_2, x_3) \mapsto x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ called the *norm form* of B. For a prime p we denote by $B_{p,\infty}$ the quaternion algebra ramified at places p and ∞. We will only work in the case $p \equiv 3 \mod 4$ where we may explicitly define it as $B_{p,\infty} \cong (-1, -p)_{\mathbb{Q}}$.

2.2 $\mathbb{Z}$-Lattices

Take a $\mathbb{Z}$-lattice $L = \mathbb{Z}e_1 + ... + \mathbb{Z}e_n$ within a vector space V. Suppose V has a fixed basis $b_1, ..., b_m$ then each e_i may be written as a column vector,

$$e_i = e_{i1}b_1 + ... + e_{im}b_m \quad \longleftrightarrow \quad \begin{pmatrix} e_{i1} \\ e_{i2} \\ \cdots \\ e_{im} \end{pmatrix}.$$

A *basis matrix* of L is a matrix where columns correspond to a set of basis vectors by the above transformation. In a similar way, we may also use matrices representing a set of vectors spanning L, which may have additional columns. One may apply *unimodular* column operations to these matrices without changing the lattice they define. These consist of: adding an integral multiples of a column to another ($c_r \mapsto c_r + tc_s$); swapping columns ($c_r \leftrightarrow c_s$); or changing a sign ($c_r \mapsto -c_r$). Applying unimodular column operations amounts to multiplying on the right by a unimodular matrix. Under such operations a basis matrix can be put into a lower or upper triangular form, then further into a *lower/upper Hermite Normal Form (HNF)* by minimizing entries relative to the diagonal. This form is unique when there are at least as many columns as rows.

We will mainly work with full-rank $\mathbb{Z}$-lattices L within $B_{p,\infty}$ with the basis of $B_{p,\infty}$ fixed as $1, i, j, k$. Such a lattice then has an associated *norm form* with respect to a $\mathbb{Z}$-basis $e_1, ..., e_4$ as,

$$(x_1, x_2, x_3, x_4) \mapsto \mathrm{nrd}(x_1 e_1 + ... + x_4 e_4).$$

We restrict to integer inputs $x_i \in \mathbb{Z}$, so the form represents $n \in \mathbb{Q}$ if and only if there exists an element in L of reduced norm n. We say the *discriminant* of L, written $\mathrm{disc}(L)$, is the discriminant of its norm form. Lattices may be added $L_1 + L_2$, intersected $L_1 \cap L_2$, and within $B_{p,\infty}$, multiplied together $L_1 L_2$, or by a single element $\alpha \cdot L_1$. We also define the *Gross lattice* of L to be the set,

$$L^T = \{2x - \mathrm{Tr}(x) : x \in L\}.$$

When dealing with many lattice problems, it is often computationally easier to work with basis vectors which have smaller norms, and such elements can reveal structural properties of the lattice. One way to quantify this is using *successive minima.* For a lattice L with norm form (or vector space norm) f, the ith successive minima for $1 \leq i \leq rank(L)$ is defined to be the minimum value λ_i such that the rank of $\{v \in L : f(v) \leq \lambda_i\}$ is greater than or equal to i.

2.3 Quaternion Orders

For number fields, roots of monic polynomials with integer coefficients are called *algebraic integers.* Within quaternion algebras we call them *quaternion integers* and they are exactly the elements of integral norm and trace. A quaternion order in $B_{p,\infty}$ is a full-rank $\mathbb{Z}$-lattice which is a ring (containing 1). As lattices, they inherit the definitions of the previous section. As rings, they may only contain quaternion integers. While infinitely many orders exist we focus on *maximal orders*, up to (ring) isomorphisms, of which there are only finitely many classes. Maximal orders are those not contained in any larger order, or equivalently in $B_{p,\infty}$, those with discriminant p^2. Two orders $\mathcal{O}$, $\mathcal{O}'$ are isomorphic (as rings) if and only if they are conjugate, i.e. $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$ for some $\alpha \in B_{p,\infty}$.

For $p \equiv 3 \mod 4$ the following order in $B_{p,\infty}$, which we call $\mathcal{O}_{1728}$, is always maximal,

$$\mathcal{O}_{1728} = \mathbb{Z} \cdot \frac{1+j}{2} + \mathbb{Z} \cdot \frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k.$$

2.4 Integral Ideals

An (integral) left (or right) ideal of a quaternion order $\mathcal{O}$ is a full-rank $\mathbb{Z}$-lattice $I \subseteq \mathcal{O}$ such that $\mathcal{O}I \subseteq I$ (or $I\mathcal{O} \subseteq I$). As a lattice, it again inherits the previous definitions. We say $I = (x_1, ..., x_n)$ is *generated* by $x_1, ..., x_n$ if it is generated as a left (or right) $\mathcal{O}$-module, i.e. for left ideals $I = \sum_r \mathcal{O} \cdot x_r$. It is *principal* if generated by one element, and multiplying by a principal ideal is equivalent to multiplying by the generator, $I \cdot \alpha = I \cdot (\alpha)$. Two ideals I, J are *left (or right) equivalent* if they differ by a principal ideal on the right (or left), so $I = J\alpha$ (or $I = \alpha J$) for some non-zero $\alpha \in B_{p,\infty}$. We say a left (or right) $\mathcal{O}$-ideal I is *cyclic* (a.k.a. *primitive*) if for any $q \in \mathbb{Z}$ the set $\{\frac{x}{q} : x \in I\}$ is not a left (or right) $\mathcal{O}$-ideal. The size of an ideal is represented by the *ideal norm* $N(I) = \{\gcd(\mathrm{nrd}(x)) : x \in I\}$ and for cyclic left/right $\mathcal{O}$-ideals, $\mathrm{disc}(I) = N(I)^4 \cdot \mathrm{disc}(\mathcal{O})$. By definition $N(I)$ divides the reduced norm of every element in the ideal. Moreover, the ideal norm is contained in the ideal $N(I) \in I$, as is the reduced norm of every element in I. Every cyclic left $\mathcal{O}$-ideal may be written as $I = \mathcal{O} \cdot N(I) + \mathcal{O} \cdot \alpha$ for some quaternion integer $\alpha \in I$, and in $B_{p,\infty}$, for $N(I)$ coprime to p we have $I \cap \mathbb{Z} = \mathbb{Z} \cdot N(I)$. Also the *conjugate* of a left $\mathcal{O}$-ideal I is a right $\mathcal{O}$-ideal $\overline{I} = \{\overline{x} : x \in I\}$. The *left order* and *right order* of an quaternion ideal I are,

$$\mathcal{O}_{\mathrm{left}}(I) = \{\alpha \in B : \alpha I \subseteq I\} \quad \text{and} \quad \mathcal{O}_{\mathrm{right}}(I) = \{\alpha \in B : I\alpha \subseteq I\}$$

respectively, and they have the same discriminant. A cyclic left $\mathcal{O}$-ideal has left order $\mathcal{O}$ (similarly for right), and for the conjugate ideal, the left and right order switch. For any (integral) ideal I we have $N(I) \cdot \mathcal{O}_{\mathrm{left}}(I) \subseteq I \subseteq \mathcal{O}_{\mathrm{right}}(I)$ and $N(I) \cdot \mathcal{O}_{\mathrm{right}}(I) \subseteq I \subseteq \mathcal{O}_{\mathrm{left}}(I)$. For ideals I, J with $\mathcal{O}_{\mathrm{right}}(I) = \mathcal{O}_{\mathrm{left}}(J)$ the lattice IJ is an (integral) ideal with left order $\mathcal{O}_{\mathrm{left}}(I)$ and right order $\mathcal{O}_{\mathrm{right}}(J)$. The ideal norm is then multiplicative $N(IJ) = N(I)N(J)$, and for an $\mathcal{O}$-ideal I we have $I\overline{I} = N(I) \cdot \mathcal{O}$. For $N(I) = q_1...q_n$ with q_i prime, a cyclic ideal I can decomposed into a product of cyclic ideals $I = I_1...I_n$ with $N(I_r) = q_r$. Let $\mathcal{O}_1, \mathcal{O}_2$ be maximal orders, then we say an ideal I with $\mathcal{O}_{\mathrm{left}}(I) = \mathcal{O}_1$ and $\mathcal{O}_{\mathrm{right}}(I) = \mathcal{O}_2$ is a *connecting ideal* from $\mathcal{O}_1$ to $\mathcal{O}_2$. For any pair of maximal orders $\mathcal{O}_1, \mathcal{O}_2$, there exists a unique integer N such that $N\mathcal{O}_1\mathcal{O}_2$ is a cyclic (integral) connecting ideal. The norm of $N\mathcal{O}_1\mathcal{O}_2$ is N, and all connecting ideals from $\mathcal{O}_1$ to $\mathcal{O}_2$ are scalar multiples of it.

2.5 The Deuring Correspondence

For a prime p, the ring of endomorphisms of a supersingular elliptic curve over $\overline{\mathbb{F}_p}$, written $\mathrm{End}(E)$, is isomorphic to a maximal order in $B_{p,\infty}$. The Deuring correspondence [10] defines a correspondence between isomorphism classes of such curves, and isomorphism classes of maximal orders. It is one-to-one for $\mathbb{F}_p$-rational curves and maximal orders for which $\mathbb{Z}[\sqrt{-p}]$ embeds, and two-to-one otherwise. Ideals then naturally relate to isogenies. For a curve E_1 with a fixed isomorphism $\mathrm{End}(E_1) \cong \mathcal{O}_1 \subset B_{p,\infty}$, outgoing isogenies $\varphi_1 : E_1 \to E_2$ correspond to left $\mathcal{O}_1$-ideals I_{φ_1}, and $\mathrm{End}(E_2) \cong \mathcal{O}_2 := \mathcal{O}_{\mathrm{right}(I_{\varphi_1})}$. Moreover we have $N(I_{\varphi_1}) = \deg(\varphi_1)$, and φ_1 is an endomorphism $\varphi_1 \in \mathrm{End}(E)$ if and only if I is the principal ideal generated by the element of $\mathcal{O}$ corresponding to φ_1 under the isomorphism $\mathrm{End}(E_1) \cong \mathcal{O}_1$. Also the ideal I_{φ_1} is cyclic if and only if φ_1 is a *cyclic isogeny*, meaning an isogeny of cyclic kernel. We may then take a second isogeny $\varphi_2 : E_2 \to E_3$ which corresponds to a left $\mathcal{O}_2$-ideal I_{φ_2} in the same way. The composite isogeny $\varphi_2 \circ \varphi_1 : E_1 \to E_3$ then corresponds the left $\mathcal{O}_1$-ideal $I_{\varphi_1} I_{\varphi_2}$. Every isogeny φ_1 also has a dual $\hat{\varphi_1} : E_2 \to E_1$ of the same degree with $\hat{\varphi_1} \circ \varphi_1$ being the multiplication-by-$\deg(\varphi_1)$ endomorphism. Note that $\hat{\varphi_1}$ as an isogeny from E_2, corresponds to the conjugate ideal, i.e. the left $\mathcal{O}_2$-ideal $\overline{I_{\varphi_1}}$. Just as cyclic ideals decompose into the products of prime norm ideals, so do cyclic isogenies. Note that for a prime $\ell \neq p$, from any curve E there are $\ell + 1$ outgoing degree ℓ isogenies up to post-composition with isomorphism, and similarly there are $\ell + 1$ norm ℓ left-ideals of a fixed $\mathcal{O} \cong \mathrm{End}(E)$.

3 Structural result for right orders of ℓ^n ideals

In this section we prove our structural result on the bases of right orders of cyclic norm ℓ^n left-$\mathcal{O}_{1728}$ ideals. We express the bases of orders using the basis matrix notation defined in Section 2.2, and define $\delta(P) = 1$ when property P holds, and $\delta(P) = 0$ otherwise.

Definition 1. *For odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$ and $n \geq 1$, let $S_{p,\ell,n}$ denote the set of all basis matrices*

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\ell^{a+b}} & 0 & 0 \\ \frac{\ell^a}{2} & \frac{A}{\ell^n} & \ell^a & 0 \\ \frac{C+\delta(2\nmid C)\cdot\ell^{b+c}}{2\ell^c} & \frac{B}{2\ell^b} & \frac{C}{\ell^c} & \ell^b \end{pmatrix}$$

where,

- *either, $0 \leq a, b \leq n$ with $a + b = n$, or $-n \leq a \leq 0$ and $b = n$,*
- *$C \in \mathbb{Z}$ with $0 \leq C < \ell^{b+c}$, and $c = 0$ if $a \geq 0$ otherwise $c = -a$,*
- *$0 \leq A < \ell^{n+a}$ and $0 \leq B < 2\ell^{2b}$,*
- *B is odd,*
- *$\alpha - 4A^2$ is divisible by $\ell^{2(n-b)}$, where α is the unique solution to $\alpha p \equiv -\ell^{2n-2a-2b} \mod 2\ell^{2n}$,*
- *$\frac{\alpha-4A^2}{\ell^{2(n-b)}}$ is a square modulo $2\ell^{2b}$,*
- *B is one of the square roots of $\frac{\alpha-4A^2}{\ell^{2(n-b)}}$ modulo $2\ell^{2b}$,*
- *$2A + BC \equiv 0 \mod \ell^{b+c}$,*
- *and $\ell^{2c} \mid 1 + C^2$.*

The result can then be stated as follows.

Theorem 1. *Fix odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$ and an integer $n \geq 1$.*

A. All right orders $\mathcal{O}$ of cyclic left-ideals $I \subseteq \mathcal{O}_{1728}$ of norm ℓ^n have a HNF basis matrix in the set $S_{p,\ell,n}$.

B. *Every matrix in $S_{p,\ell,n}$ is the basis of a distinct maximal order $\mathcal{O}$ where the connecting ideal between $\mathcal{O}_{1728}$ and $\mathcal{O}$ has norm ℓ^n.*

Note in Part B., all the conditions of Definition 1 are necessary. While we won't prove it, upon removing any condition from the definition, counter-examples can be found.

The rest of this section is dedicated to proving the theorem. We will prove points A. and B. separately.

3.1 Proof of Theorem 1 Part A.

Take p, ℓ, n as in the Theorem. Let $\mathcal{O} \subset B_{p,\infty}$ be the right order of a cyclic norm ℓ^n left $\mathcal{O}_{1728}$ ideal I. We may represent $\mathcal{O}$ by a basis matrix in Hermite Normal Form (HNF), that is,

$$\begin{pmatrix} e_{00} & 0 & 0 & 0 \\ e_{01} & e_{11} & 0 & 0 \\ e_{02} & e_{12} & e_{22} & 0 \\ e_{03} & e_{13} & e_{23} & e_{33} \end{pmatrix}.$$

for $e_{ij} \in \mathbb{Q}$, with $e_{mn} \geq 0$ for all n, m. We will denote by $e_0, ..., e_3$ the basis elements of $\mathcal{O}$ arising from each column of the matrix.

Since the left and right orders of cyclic ideals have the same discriminant, we know $\mathcal{O}$ is maximal. We first obtain some information regarding e_{mn} from a previous result of [3].

Lemma 1. *Continuing from above, the following properties hold,*

1. *The denominators of each rational entry e_{mn}, when expressed in simplest form, divide $2 \cdot \ell^n$,*
2. *$e_{00} = \frac{1}{2}$,*
3. *$e_{11} = 1/(2e_{22}e_{33})$,*
4. *$e_{22}e_{33} \leq \ell^n$,*
5. *and $e_{01} = 0$ or $e_{01} = 1/(4e_{22}e_{33})$.*

Proof. From [3, Lemma 5.2] with $K = 2$ and $N(I) = \ell^n$, where point (2) comes from its proof.

Next we give initial results on entries e_{22}, e_{33} and e_{01}.

Lemma 2. *Continuing from above we have, $e_{22} = \ell^a$ and $e_{33} = \ell^b$ for some integers a, b with $-n \leq a \leq n$, $0 \leq b \leq n$ and $a + b \leq n$. Also $e_{01} = 0$.*

Proof. The last basis vector is $e_3 = e_{33}k$ and so $e_3 \cdot e_3 = -e_{33}^2 p \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. By Lemma 1 point (1) since p and ℓ are coprime it follows that $e_{33} \in \mathbb{Z}$. Since $k \in \mathcal{O}_{1728}$ and $N(I) \cdot \mathcal{O}_{1728} \subseteq \mathcal{O}$ we have $N(I) \cdot k \in \mathcal{O}$. This means $e_{33} \mid N(I) = \ell^n$ so we may write $e_{33} = \ell^b$ with $b \leq n$. The same argument shows $N(I) \cdot j \in \mathcal{O}$ and so we write $e_{22} = \ell^a$ with $a \leq n$. From $e_{33} \in \mathbb{Z}$ we get $b \geq 0$. From Lemma 1 point (1) we get $a \geq -n$. And applying the same result to $e_{11} = 1/(2e_{22}e_{33}) = 1/2\ell^{a+b}$ we get $a + b \leq n$.

By Lemma 1 point (5) $e_{01} = 0$ or $e_{01} = 1/(4\ell^{a+b})$. If however $e_{01} = 1/(4\ell^{a+b})$ since ℓ is odd this contradicts with Lemma 1 point (1) as 4 does not divide $2\ell^n$.

Next we prove entry e_{23} is in the given form.

Lemma 3. *Continuing from above, let $c = -a$ for $a \leq 0$ and $c = 0$ otherwise. Then there exists $C \in \mathbb{Z}$ such that $e_{23} = \frac{C}{\ell^c}$ and $0 \leq C \leq \ell^{b+c}$.*

Proof. Consider the basis vector $e_2 = e_{22}j + e_{23}k = \ell^a j + e_{23}k$. Every element of $\mathcal{O}$ is a quaternion integer which implies $\mathrm{nrd}(e_2) = p(\ell^{2a} + e_{23}^2) \in \mathbb{Z}$. If $a \geq 0$ then $pe_{23}^2 = \mathrm{nrd}(e_2) - p\ell^{2a} \in \mathbb{Z}$. By Lemma 1 point (1) and $\ell \neq p$, we get $e_{23} \in \mathbb{Z}$ so write $e_{23} = C = \frac{C}{1} = \frac{C}{\ell^c}$. If $a \leq 0$ then $p(\ell^c e_{23})^2 \in \mathbb{Z}$ so by the same argument $\ell^c e_{23} \in \mathbb{Z}$ and we may write $e_{23} = \frac{C}{\ell^c}$. The fact $0 \leq C$ comes from all entries being positive in HNF. And $C \leq \ell^{b+c}$ comes from the fact e_{23} is minimized relative to the diagonal entry e_{33} in HNF, so $\frac{C}{\ell^c} \leq e_{33} = \ell^b$.

We now return to address the first basis vector, recalling that $e_{00} = \frac{1}{2}$ and $e_{01} = 0$.

Lemma 4. *Continuing from above we have $e_{02} = \frac{\ell^a}{2}$ and $e_{03} = \frac{C+\delta(2\nmid C)\cdot\ell^{b+c}}{2\ell^c}$.*

Proof. For e_{02}, we know $1 \in \mathcal{O}$ and hence $2e_0 - 1 = 2e_{02}j + (*)k \in \mathcal{O}$. This means it must be a linear combination of the last two basis vectors, which implies $e_{22} = \ell^a \mid 2e_{02}$ so $e_{02} \in \frac{\ell^a}{2}\mathbb{Z}$. Since HNF minimizes entries relative to the diagonal we have $0 \leq e_{02} < e_{22} = \ell^a$, therefore $e_{02} = 0$ or $\frac{\ell^a}{2}$. Suppose for contradiction $e_{02} = 0$. Since $\frac{1+j}{2} \in \mathcal{O}_{1728}$ we have $\frac{\ell^n + \ell^n j}{2} \in \mathcal{O}$, so $\frac{\ell^n+\ell^n j}{2} - \ell^n e_0 = \frac{\ell^n}{2}j + (*)k \in \mathcal{O}$. This means $e_{22} = \ell^a \nmid \frac{\ell^n}{2}$ which is not possible. Hence by contradiction $e_{02} = \frac{\ell^a}{2}$.

Now consider e_{03}. We have $\mathrm{nrd}(e_0) = \frac{1+p\ell^{2a}}{4} + e_{03}^2 p \in \mathbb{Z}$. If $a \geq 0$ then $1 + p\ell^{2a} \equiv 1 + 3\cdot 1 \equiv 4 \equiv 0 \mod 4$ which implies $\frac{1+p\ell^{2a}}{4} \in \mathbb{Z}$ and so $e_{03}^2 p \in \mathbb{Z}$. By Lemma 1 point (1), this means $e_{03} \in \mathbb{Z}$. If instead $a < 0$ then $\mathrm{nrd}(e_0) = \frac{\ell^{-2a}+p}{4\ell^{-2a}} + e_{03}^2 p \in \mathbb{Z}$ and $\frac{\ell^{-2a}+p}{4\ell^{-2a}} \in \ell^{2a}\mathbb{Z}$ since modulo 4 we have $\ell^{-2a} + p \equiv 1 + 3 \equiv 0 \mod 4$. This implies $pe_{03}^2 \in \ell^{2a}\mathbb{Z}$ and so $e_{03} \in \ell^a\mathbb{Z}$.

From $1 \in \mathcal{O}$ we know $1 - 2e_0 + e_2 = -2e_{03}k + e_{23}k \in \mathcal{O}$ which implies $e_{33} = \ell^b \mid (e_{23} - 2e_{03})$. Therefore there exist an integer r such that $-r\ell^b = e_{23} - 2e_{03}$. Rearranging this gives $e_{03} = \frac{e_{23}+r\ell^b}{2}$. By HNF minimizing entries we know $0 \leq e_{03}, e_{23} \leq \ell^b$ which means $r = 0$ or 1. If $a \geq 0$ then $e_{03}, e_{23} \in \mathbb{Z}$ so there is only one value of r for which this works, that is $r = \delta(2 \nmid e_{23})$ so that $e_{23} + r\ell^b$ is divisible by 2. This gives $e_{03} = \frac{e_{23}+\delta(2\nmid e_{23})\cdot\ell^b}{2}$. If $a < 0$ then $e_{03}, e_{23} \in \ell^a\mathbb{Z}$ and again there is only one value of r such that $e_{03} = \frac{\ell^{-a}e_{23}+r\ell^{b-a}}{2\ell^{-a}} \in \ell^a\mathbb{Z}$. This gives $e_{03} = \frac{\ell^{-a}e_{23}+\delta(2\nmid\ell^{-a}e_{23})\ell^{b-a}}{2\ell^{-a}}$. In both cases this can be written as $e_{03} = \frac{C+\delta(2\nmid C)\cdot\ell^{b+c}}{2\ell^c}$.

The last column to address is the second, where we know $e_{11} = \frac{1}{2\ell^{a+b}}$.

Lemma 5. *Continuing from above, $e_{12} = \frac{A}{\ell^n}$ and $e_{13} = \frac{B}{2\ell^b}$ with integers $0 \leq A < \ell^{n+a}$ and $0 \leq B < 2\ell^{2b}$.*

Proof. By Lemma 1 point (1), we can write $e_{12} = \frac{A'}{2\ell^n}$ and $e_{13} = \frac{B'}{2\ell^n}$ where $A', B' \in \mathbb{Z}$. Then $\frac{i+k}{2} \in \mathcal{O}_{1728}$ implies $\frac{\ell^n i + \ell^n k}{2} \in \mathcal{O}$, and so

$$\ell^{n+a+b}e_1 - \frac{\ell^n i + \ell^n k}{2} = \ell^{a+b}\frac{A'}{2}j + \left(\ell^{a+b}\frac{B'}{2} - \frac{\ell^n}{2}\right)k \in \mathcal{O}$$

which must be a linear combination of e_2 and e_3 so $e_{22} = \ell^a \mid \ell^{a+b}\frac{A'}{2}$, i.e. $\frac{A'\ell^b}{2} \in \mathbb{Z}$ so $2 \mid A'$. We then redefine $e_{12} = \frac{A}{\ell^n}$ for $A \in \mathbb{Z}$ and HNF minimization gives $0 \leq A < \ell^{n+a}$.

Also consider $e_1 \cdot e_3 \in \mathcal{O}$ which by previous results gives,

$$-\frac{pB'\ell^b}{2\ell^n} + \frac{A\ell^b p}{\ell^n}i - \frac{1}{2\ell^a}j \in \mathcal{O}.$$

Hence $e_{00} = \frac{1}{2} \mid \frac{pB'\ell^b}{2\ell^n}$ so $\ell^n \mid B'\ell^b$. Therefore $\ell^{n-b} \mid B'$ so we can redefine $e_{13} = \frac{B}{2\ell^b}$ for $B \in \mathbb{Z}$, and by minimizing HNF entries we get $0 \leq B < 2\ell^{2b}$.

The above results show the entries e_{nm} are all as stated, however it remains to prove the conditions relating the different variables. The conditions involving A, B, C are now given.

Lemma 6. *Continuing from the above,*

1. *B is odd,*
2. *$\alpha - 4A^2$ is divisible by $\ell^{2(n-b)}$, where α is the unique solution to $\alpha p \equiv -\ell^{2n-2a-2b} \mod 2\ell^{2n}$,*
3. *$\frac{\alpha - 4A^2}{\ell^{2(n-b)}}$ is a square modulo $2\ell^{2b}$,*
4. *B is one of the square roots of $\frac{\alpha - 4A^2}{\ell^{2(n-b)}}$ modulo $2\ell^{2b}$,*
5. *and $2A\ell^{a+b+c} + BC\ell^n \equiv 0 \mod \ell^{n+b+c}$,*
6. *$\ell^{n-a-2b} \mid A$,*
7. *$\ell^{2c} \mid 1 + C^2$.*

Proof. We build upon the statement of $\ell^{n+a+b}e_1 - \frac{\ell^n i + \ell^n k}{2} \in \mathcal{O}$ from the previous proof. We may subtract multiples of e_2 to remove the j term, leaving

$$\ell^{n+a+b}e_1 - \frac{\ell^n i + \ell^n k}{2} - A\ell^b e_2 = \left(\frac{B\ell^{n+a} - \ell^n}{2} - \frac{AC\ell^b}{\ell^c}\right)k \in \mathcal{O}.$$

This means $e_{33} = \ell^b \mid (\frac{B\ell^{n+a} - \ell^n}{2} - \frac{AC\ell^b}{\ell^c})$ which clearly requires B to be odd.

Now consider $\mathrm{nrd}(e_1) = \frac{\ell^{2n-2a-2b} + p(4A^2 + \ell^{2(n-b)}B^2)}{4\ell^{2n}}$ where $2n - 2a - 2b \geq 0$ from the inequality $a + b \leq n$. Since $\mathrm{nrd}(e_1) \in \mathbb{Z}$ there exists $r \in \mathbb{Z}$ such that $\ell^{2n-2a-2b} + p(4A^2 + \ell^{2(n-b)}B^2) = 4r\ell^{2n}$. Rearranging gives,

$$B^2 = \left(\frac{4r\ell^{2n} - \ell^{2n-2a-2b}}{p} - 4A^2\right)\frac{1}{\ell^{2(n-b)}}.$$

Since $B \in \mathbb{Z}$ the above expression implies $4r\ell^{2n} - \ell^{2n-2a-2b} \equiv 0 \mod p$. Let r_0 be the solution to this modulo p then $r = r_0 + r'p$ for some $r' \in \mathbb{Z}$. We get,

$$B^2 = \left(\alpha - 4A^2\right)\frac{1}{\ell^{2(n-b)}} + 4r'\ell^{2b} \quad \text{defining} \quad \alpha = \frac{4r_0\ell^{2n} - \ell^{2n-2a-2b}}{p}.$$

Since $B < 2\ell^{2b}$ we only need the value modulo $2\ell^{2b}$. We get $B^2 \equiv \frac{\alpha-4A^2}{\ell^{2(n-b)}} \mod 2\ell^{2b}$, hence B is a square root as claimed in the statement.

Notice the definition of α above is not the value given in the Lemma statement. In the formula for B however, we only need $\frac{\alpha-4A^2}{\ell^{2(n-b)}}$ modulo $2\ell^{2b}$ and hence we only need α and A modulo $2\ell^{2n}$. By the definition above α solves $\alpha p \equiv -\ell^{2n-2a-2b} \mod 2\ell^{2n}$. We argue however that this relation has at most one possible solution for α, and so we may redefine α to be this unique solution. Clearly the relation modulo ℓ^{2n} only has one solution for α by finite field arithmetic, denote it α_0. Lifting it modulo $2\ell^{2n}$ gives $p\alpha \equiv p(\alpha_0 + r\ell^{2n}) \equiv -\ell^{2n-2a-2b} \mod 2\ell^{2n}$ for $r = 0$ or 1. As the left-hand side takes on two different values, only one can be correct, so there is at most one solution modulo $2\ell^{2n}$.

For point (5) consider $e_1 \cdot e_2 \in \mathcal{O}$, which gives,

$$-p\left(\frac{A\ell^a}{\ell^n} + \frac{BC}{2\ell^{b+c}}\right) + (*)i + (*)j + (*)k \in \mathcal{O}$$

which means $e_{00} = \frac{1}{2} \mid \left(\frac{2A\ell^{a+b+c}+BC\ell^n}{2\ell^{n+b+c}}\right)$. This implies $\ell^{n+b+c} \mid p(2A\ell^{a+b+c} + BC\ell^n)$, or equivalently, since p, ℓ are coprime, $2A\ell^{a+b+c} + BC\ell^n \equiv 0 \mod \ell^{n+b+c}$.

Point (6) comes from $\mathcal{O} \ni e_1 \cdot e_3 + pBe_0 = p\ell^{b-n}Ai + (*)j + (*)k$, which to lie in $\mathcal{O}$ requires $e_{11} = \frac{1}{2\ell^{a+b}} \mid p\ell^{b-n}A$, hence $\ell^{a+2b-n}A \in \mathbb{Z}$.

Finally point (7) is trivial when $a \geq 0$ as $\ell^{2c} = 1$. For $a < 0$ we have $\mathrm{nrd}(e_2) = \mathrm{nrd}(\ell^a j + \frac{C}{\ell^c}k) = p(\frac{\ell^{2a+2c}+C^2}{\ell^{2c}}) \in \mathbb{Z}$. And $c = -a$ so this gives $\ell^{2c} \mid \ell^{2a+2c} + C^2 = 1 + C^2$.

The final conditions to prove are the relations between a and b.

Lemma 7. *Continuing from the above,*

1. *if $a \geq 0$ then $a + b = n$,*
2. *and if $a < 0$ then $b = n$.*

Hence $a + b + c - n = 0$ and so Lemma 6 point (5) becomes $2A + BC \equiv 0 \mod \ell^{b+c}$.

Proof. (1) Suppose for contradiction that $a \geq 0$ and $a + b < n$, so $c = 0$. We'll show that $\ell^{n-1}\mathcal{O}_{1728} \subseteq \mathcal{O}$ so that $N(I) = [\mathcal{O}_{1728} : \mathcal{O}_{1728} \cap \mathcal{O}] \leq \ell^{n-1}$ which is contradiction with the fact that I has norm ℓ^n.

To show $\ell^{n-1}\mathcal{O}_{1728} \subseteq \mathcal{O}$ it is enough to show $\frac{\ell^{n-1}+\ell^{n-1}j}{2}$, $\frac{\ell^{n-1}i+\ell^{n-1}k}{2}$, $\ell^{n-1}j$, $\ell^{n-1}k \in \mathcal{O}$. Let e_0, e_1, e_2, e_3 denote the basis vectors of $\mathcal{O}$ as given by the columns of the matrix in Theorem 1. One may check that,

$$\frac{\ell^{n-1} + \ell^{n-1}j}{2} = \ell^{n-1}e_0 + \frac{\ell^{n-1-a} - \ell^{n-1}}{2}e_2 - \frac{\ell^{n-1}\delta(2 \nmid C) + C\ell^{n-1-a-b}}{2}e_3,$$

$$\frac{\ell^{n-1}i + \ell^{n-1}k}{2} = \ell^{n+a+b-1}e_1 - \ell^{b-1}Ae_2 + \left(\frac{-\ell^{n+a-1-b}B + \ell^{n-1-b}}{2} + \frac{AC}{\ell}\right)e_3,$$

$$\ell^{n-1}j = \ell^{n-1-a}e_2 - C\ell^{n-1-a-b}e_3,$$

$$\text{and} \quad \ell^{n-1}k = \ell^{n-1-b}e_3.$$

Looking at the coefficients of the above expressions, since $a+b<n$ implies $n-1-a-b \geq 0$, and ℓ, B are odd and $C, \delta(2 \nmid C)$ have the same parity, it is clear most of the coefficients are integral. There are a few less obviously integral coefficients which we now address.

To prove $\ell^{b-1}A \in \mathbb{Z}$. It is clearly true if $b \geq 1$, so consider the case $b=0$. By Lemma 6 point (6) we have $\ell^{n-a} \mid A$ and as $n-1-a-b \geq 0$ we have $n-a \geq 1$ so $\ell \mid A$.

To prove $\frac{AC}{\ell} \in \mathbb{Z}$ from $2A\ell^{a+b} + BC\ell^n \equiv 0 \mod \ell^{n+b}$ we get $\frac{2A\ell^{a+b}+BC\ell^n}{\ell^{n+b}} \in \mathbb{Z}$ so $e_1 \cdot e_2 + p\frac{2A\ell^{a+b}+BC\ell^n}{\ell^{n+b}}e_0 \in \mathcal{O}$. This is equal to $\frac{-p\ell^{n+a}B+2p\ell^bAC}{2\ell^{n+b}}i + (*)j + (*)k$. To lie in $\mathcal{O}$ this means $e_{11} = \frac{1}{2\ell^{a+b}} \mid \frac{-p\ell^{n+a}B+2p\ell^bAC}{2\ell^{n+b}}$ so $-\ell^{2a}B + 2\ell^{a+b-n}AC \in \mathbb{Z}$ which implies $\frac{AC}{\ell^{n-a-b}} \in \mathbb{Z}$. Since $n-a-b \geq 1$ we have $\frac{AC}{\ell} \in \mathbb{Z}$.

Therefore the coefficients above are all integral so the elements all lie in $\mathcal{O}$.

(2) Fix $a<0$ so $c=-a>0$. Suppose $b<n$. We repeat the idea used to prove point (1), that $\ell^{n-1}\mathcal{O}_{1728} \subseteq \mathcal{O}$ will give a contradiction. We have,

$$\frac{\ell^{n-1} + \ell^{n-1}j}{2} = \ell^{n-1}e_0 - \frac{\ell^{n-1} - \ell^{n+c-1}}{2}e_2 - \frac{\ell^{n-1}\delta(2 \nmid C) + \ell^{n-1-b}C}{2}e_3,$$

$$\frac{\ell^{n-1}i + \ell^{n-1}k}{2} = \ell^{n+b-1-c}e_1 - A\ell^{b-1}e_2 + \left(\frac{2AC - \ell^{n-b}B}{2\ell^{1+c}} + \frac{\ell^{n-1-b}}{2}\right),$$

$$\ell^{n-1}j = \ell^{n+c-1}e_2 - C\ell^{n-1-b}e_3,$$

$$\text{and} \quad \ell^{n-1}k = \ell^{n-1-b}e_3.$$

And it is enough to show all coefficients of e_s's in the above expressions are integral. Almost all the exponents of ℓ are all non-negative from $b<n$ which implies $n-b-1 \geq 0$. And all fractions with denominator 2 have even numerator since ℓ, B are odd, and $C, \delta(2 \nmid C)$ have the same parity. The only non-obviously integral coefficients require us to show $A\ell^{b-1} \in \mathbb{Z}$, and $\frac{2AC-\ell^{n-b}B}{\ell^{1+c}}$ and $\ell^{n+b-1-c} \in \mathbb{Z}$.

We now show $A\ell^{b-1} \in \mathbb{Z}$. From the definition of α, we have $\alpha p \equiv -\ell^{2(n-b)+2c} \mod \ell^{2n}$ which means $\ell^{2\min(n-b+c,n)} \mid \alpha$ so certainly $\ell^{2(n-b+1)} \mid \alpha$. Since from the theorem $\ell^{2(n-b)} \mid \alpha - 4A^2$ we also have $\ell^{n-b} \mid A$. From $b<n$ we have $n-b>0$ so $\ell \mid A$ hence $A\ell^{b-1} \in \mathbb{Z}$.

Next we show $\frac{2AC-\ell^{n-b}B}{\ell^{1+c}} \in \mathbb{Z}$. From the Theorem we have $2A\ell^b + BC\ell^n \equiv 0 \mod \ell^{n+b+c}$ which implies $e_1 \cdot e_2 + (\frac{2p\ell^bA+p\ell^nBC}{\ell^{n+c+b}})e_0 \in \mathcal{O}$. The value of this expression is $(\frac{2p\ell^bAC-p\ell^nB}{2\ell^{n+b+c}})i + (*)j + (*)k$ which to lie in $\mathcal{O}$ implies $e_{11} = \frac{\ell^c}{2\ell^b} \mid \frac{2p\ell^bAC-p\ell^nB}{2\ell^{n+b+c}}$. Removing the factor of p by coprimality, this is means $\ell^{n+2c-b} \mid 2AC - \ell^{n-b}B$. Then as $b<n$ we have $n+2c-b > 1+c$ so we certainly have $\ell^{1+c} \mid 2AC - \ell^{n-b}B$ as required.

It remains to show $\ell^{n+b-1-c} \in \mathbb{Z}$. We have $n+b-1-c \geq n+0-1-n = -1$, so it is enough to show $n+b-1-c \neq -1$. Suppose for contradiction that $n+b-1-c = -1$ so $b = 0$ and $c = n$. Then by definition of α we have $\alpha p \equiv \ell^{4n} \mod 2\ell^{2n}$, so either $\alpha = 0$ or $\alpha = \ell^{2n}$. Clearly $\alpha \neq 0$ as otherwise B is not odd, hence $\alpha = \ell^{2n}$. By point (1) $\ell^{2n} \mid A$, but as $0 \leq A < \ell^{n+a} = \ell^{2n}$ we have $A = 0$. We also have $0 \leq B < 2\ell^0 = 2$ so $B = 0$ or $B = 1$. Since $B^2 \equiv \frac{\ell^{2n}-0}{\ell^{2n}} \mod 2\ell^{2b}$ we have $B = 1$. Then $2A + BC\ell^n \equiv 0 + C\ell^n \equiv 0 \mod \ell^{2n}$, so $C \equiv 0 \mod \ell^n$. From $C < \ell^{b+c} = \ell^n$ this implies $C = 0$. Then $e_2 = \frac{1}{\ell^n} j$ has non-integral norm. This is a contradiction so $n+b-1-c \geq 0$ so $\ell^{n+b-1-c} \in \mathbb{Z}$.

This completes the proof of Theorem 1 Part A..

3.2 Proof of Theorem 1 Part B.

We now prove Theorem 1 Part B., that every element of $S_{p,\ell,n}$ is the basis matrix of a distinct maximal order $\mathcal{O}$ where the connecting ideal from $\mathcal{O}_{1728}$ to $\mathcal{O}$ has norm ℓ^n. We will break this down into smaller results: showing $\mathcal{O}$ is an order; showing it is maximal; showing the cyclic connecting ideal from $\mathcal{O}_{1728}$ to $\mathcal{O}$ is of norm ℓ^n; and lastly showing every two orders from $S_{p,\ell,n}$ are distinct. We start with a technical result.

Lemma 8. *Take p, ℓ, n as before, and variables (a, b, c, A, B, C) satisfying the conditions of $S_{p,\ell,n}$. Then*

1. *the values $\omega_1 := \frac{p+1}{4}$, $\omega_2 := \frac{B+1}{2}$, and $\omega_3 := \frac{\delta+C}{2}$ are all integral,*
2. *if $a \geq 0$, the values $\mu_1 := \frac{2A+BC+B\ell^b\delta}{2\ell^b}$, $\mu_2 := \frac{p\ell^{2n}B^2+\ell^{2b}+4pA^2\ell^{2b}}{4\ell^{2n+2b}}$, $\mu_3 := \frac{\ell^n-\ell^b}{2\ell^b}$ and $\mu_4 := \frac{\ell^b+1}{2}$ are all integral,*
3. *if $a < 0$, the values $\lambda_1 := \frac{2A+BC+B\delta\ell^{n+c}}{2\ell^{n+c}}$, $\lambda_2 := \frac{pB^2+\ell^{2c}+4pA^2}{4\ell^{2n}}$, $\lambda_3 := \frac{C^2+1-\ell^{2c}(\delta+1)}{4\ell^{2c}}$, $\lambda_4 := \frac{B-2AC-\ell^{2c}}{2\ell^{2c}}$, $\lambda_5 := \frac{\delta(\delta-1)}{4}$, $\lambda_6 := \frac{\ell^n-\ell^c}{2\ell^c}$, and $\lambda_7 := \frac{\ell^n+1}{2}$ are all integral.*

where $\delta := \delta(2 \nmid C)$.

Proof. We know $\omega_2 \in \mathbb{Z}$ as B is odd, and $\omega_1 \in \mathbb{Z}$ as $p \equiv 3 \mod 4$. Also $\mu_4, \lambda_7 \in \mathbb{Z}$ as ℓ is odd, and $\mu_3 \in \mathbb{Z}$ as $b \leq n$. It is also clear from $0 \leq c \leq n$ that $\lambda_6 \in \mathbb{Z}$. By definition δ has the same parity as C, which shows $\omega_3 \in \mathbb{Z}$. Since $(\delta, \delta-1) = (0, -1)$ or $(1, 0)$ we know $\delta(\delta-1) = 0$ so $\lambda_5 \in \mathbb{Z}$.

From the condition $2A + BC \equiv 0 \mod \ell^{b+c}$ when $a \geq 0$ we have $c = 0$ so this gives $\frac{2A+BC}{\ell^b} \in \mathbb{Z}$. Noting that C and $\ell^b\delta$ have the same parity we have $2 \mid C + \ell^b\delta$ so $2\ell^b \mid 2A + B(C + \ell^b\delta)$ giving $\mu_1 \in \mathbb{Z}$. In the case $a < 0$ we instead have $b = n$ which by the same argument gives $\ell^{n+c} \mid 2A + BC$ so $\lambda_1 \in \mathbb{Z}$. We can also multiply $\ell^{n+c} \mid 2A + BC$ by C giving $\ell^{n+c} \mid 2AC + BC^2$ and since $c \leq n$ we certainly have $\ell^{2c} \mid 2AC + BC^2$. From the other condition that $\ell^{2c} \mid C^2 + 1$ we then get $\ell^{2c} \mid 2AC + B(C^2+1) - B = 2AC - B$. We also know B is odd so $B - \ell^{2c}$ is even, giving $2\ell^{2c} \mid 2AC - B - \ell^{2c}$ and hence $\lambda_4 \in \mathbb{Z}$.

Recall by definition of B we have $B^2\ell^{2n-2b} \equiv \alpha - 4A^2 \mod 2\ell^{2n}$ and by coprimality of p and the definition of α we get $pB^2\ell^{2n-2b} \equiv -\ell^{2n-2a-2b} - 4pA^2$

$\bmod 2\ell^{2n}$. When $a \geq 0$ and so $a + b = n$ we have $p\ell^{2n}B^2 + \ell^{2b} + 4pA^2\ell^{2b} \equiv 0 \mod 2\ell^{2n+2b}$ which gives $2\mu_2 \in \mathbb{Z}$. Then we get $\mu_2 \in \mathbb{Z}$ as on the numerator $p\ell^{2n}B^2 + \ell^{2b} \equiv 3 \cdot 1 \cdot 1 + \cdot 1 \equiv 0 \mod 4$. In the case of $a < 0$ we have $b = n$ and $a = -c$ so we instead have $pB^2 + \ell^{2c} + 4pA^2 \equiv 0 \mod 2\ell^{2n}$ and checking this modulo 4 we get $pB^2 + \ell^{2c} + 4pA^2 \equiv 3 \cdot 1 + 1 + 0 \equiv 0 \mod 4$ and so $\lambda_2 \in \mathbb{Z}$.

Finally we show $\lambda_3 \in \mathbb{Z}$. This comes from the condition $C^2 + 1 \equiv 0 \mod \ell^{2c}$ so ℓ^{2c} divides the numerator of λ_3. If C is even then $\delta = 0$ and the numerator is $C^2 + 1 - \ell^{2c} \equiv 0 + 1 - 1 \equiv 0 \mod 4$. If C is odd then $\delta = 1$ and the numerator is $C^2 + 1 - 2\ell^{2c} \equiv 1 + 1 - 2 \equiv 0 \mod 4$. Hence $4\ell^{2c}$ divides the numerator and so it is integral.

Next we show matrices in $S_{p,\ell,n}$ give rise to orders.

Lemma 9. *Continuing from above, take a basis matrix in $S_{p,\ell,n}$, and let $e_0, ..., e_3$ be the quaternions corresponding to the 4 columns. Then the $\mathbb{Z}$-lattice $\mathcal{O} = \langle e_0, ..., e_3 \rangle_{\mathbb{Z}}$ is an order.*

Proof. We have $1 \in \mathcal{O}$ as $1 = 2e_0 - e_2 - \delta(2 \nmid C)e_3$. Also $\mathcal{O}$ is clearly full-rank as a lattice, since the basis matrix in lower triangular form has all diagonal entries non-zero. Hence it is sufficient to show $\mathcal{O}$ is closed under multiplication, for which it is enough to prove $e_s \cdot e_t \in \mathcal{O}$ for all $0 \leq s, t \leq 3$. For ease of verification, the full proof is done symbolically in SageMath and can be found in file `prf_order.ipynb`. To give one example, in the case of $a < 0$ one may verify that,

$$e_2 \cdot e_3 = p(2\lambda_6 + 1)(-2Ce_0 + (4\lambda_6 + 2)e_1 + (-2A + C)e_2 + C\delta e_3) - (2\lambda_4 + 1)e_3,$$

and in the case $a \geq 0$,

$$e_2 \cdot e_3 = p(-2\ell^bCe_0 + 2\ell^{2n}e_1 + (-2\ell^bA + \ell^bC)e_2 + (\ell^bC\delta + 2AC - (2\mu_3 + 1)^2B)e_3),$$

where λ_4, λ_6 and μ_3 are integral values from the previous lemma, and $\delta \coloneqq \delta(2 \nmid C)$. The expressions on the right-hand side are clearly integral linear combinations of e_i and so $e_2 \cdot e_3 \in \mathcal{O}$.

And we also argue $\mathcal{O}$ is maximal.

Lemma 10. *Continuing from above, $\mathcal{O}$ is a maximal order.*

Proof. Consider the change of basis matrix T taking the basis of $\mathcal{O}_{1728}$ to the basis of $\mathcal{O}$. As matrices this is $M_{\mathcal{O}_{1728}} = M_{\mathcal{O}} \cdot T$. It is easy to see $\det(M_{\mathcal{O}_{1728}}) = \frac{1}{4}$ and $\det(M_{\mathcal{O}}) = \frac{1}{2} \cdot \frac{1}{2\ell^{a+b}} \cdot \ell^a \cdot \ell^b = \frac{1}{4}$ so $\det(T) = 1$. By [17, Lemma 15.2.5], $\det(T) = 1$ implies $\operatorname{disc}(\mathcal{O}) = \operatorname{disc}(\mathcal{O}_{1728})$. As all maximal orders in $B_{p,\infty}$ have the same discriminant and $\mathcal{O}_{1728}$ is maximal, this implies $\mathcal{O}$ is maximal.

Now consider connecting ideals from $\mathcal{O}_{1728}$ to $\mathcal{O}$, which certainly exist as both $\mathcal{O}_{1728}$ and $\mathcal{O}$ are maximal. Recall connecting ideals between two orders are all equal up to scaling by elements of $\mathbb{Q}$ (see [13, Lemma 8]). Hence there is exactly one such connecting ideal which is cyclic (and integral) which we call I. Equivalently, I is the smallest norm (integral) connecting ideal from $\mathcal{O}_{1728}$ to $\mathcal{O}$. We now show I has norm ℓ^n.

Lemma 11. *Continuing from above, the cyclic connecting ideal I from $\mathcal{O}_{1728}$ to $\mathcal{O}$, has norm ℓ^n.*

Proof. First we show $N(I) \geq \ell^n$. In the case $a \leq 0$ we have $b = n$ so the smallest multiple of k in the order is $\ell^n k$. This means for any $r < \ell^n$ we have $rk \notin \mathcal{O}$. Since $N(I) \cdot \mathcal{O}_{1728} \subseteq \mathcal{O}$ and $k \in \mathcal{O}_{1728}$, we must have $N(I) \cdot k \in \mathcal{O}$, which implies $N(I) \geq \ell^n$. In the case $a > 0$, we have $a + b = n$ so $e_{11} = \frac{1}{2\ell^n}$. As in the previous section, we again use the result of [3, Lemma 5.2], which states for the right order $\mathcal{O}$ of an $\mathcal{O}_{1728}$-ideal I, the denominators of the basis coefficients of $\mathcal{O}$ all divide $2 \cdot N(I)$. Applied to e_{11} we get $\ell^n \mid N(I)$ and hence $N(I) \geq \ell^n$.

We now prove $\ell^n \mathcal{O}_{1728} \subseteq \mathcal{O}$ by showing ℓ^n multiples of each of the 4 basis vectors of $\mathcal{O}_{1728}$ lie in $\mathcal{O}$. For the first of these we get,

$$\frac{\ell^n + \ell^n j}{2} = \begin{cases} \ell^n e_0 + \ell^n(-\ell^c \lambda_6 + \lambda_7 - 1)e_2 - (\ell^n \omega_3 - C(\lambda_7 - 1))e_3 & \text{when } a < 0 \\ \ell^n e_0 - \mu_3 \ell^b e_2 - (\ell^n \omega_3 - C(\ell^b \mu_3 + \mu_4 - 1))e_3 & \text{when } a \geq 0 \end{cases}$$

where in the relevant case $\lambda_6, \lambda_7, \omega_3, \mu_3, \mu_4$ are integral by Lemma 8. This shows $\frac{\ell^n + \ell^n j}{2}$ can be written as an integral linear combination of e_t so it lies in $\mathcal{O}$. We address the remaining cases in the SageMath code file `prf_int.ipynb`. Having shown $\ell^n \mathcal{O}_{1728} \subseteq \mathcal{O}$ we must have $\mathcal{O}_{1728} \cap \mathcal{O} \subseteq \ell^n \mathcal{O}_{1728}$ and hence by [13, Lemma 8] $N(I) \leq \ell^n$. This proves $N(I) = \ell^n$.

It remains to show each matrix in $S_{p,\ell,n}$ arises from a distinct maximal order. To be clear, distinct means they are different as lattices, and does not mean non-isomorphic.

Lemma 12. *Every matrix in $S_{p,\ell,n}$ arises from a distinct maximal order.*

Proof. From the ranges of A, B, C it is clear that $0 \leq e_{st} < e_{tt}$ for all $0 \leq s, t \leq 3$. This means the matrices are all in lower triangular Hermite Normal Form which is unique for every quaternion order. Hence two distinct matrices cannot give the same order.

This completes the proof of Theorem 1.

4 Structural result for ℓ^n ideals

In this section we prove the following result, again using the basis matrix notation of Section 2.2.

Theorem 2. *Take odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$ and an integer $n \geq 1$. Then the set of cyclic left-ideals $I \subseteq \mathcal{O}_{1728}$ of norm ℓ^n is exactly given by the set of basis matrices,*

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ -\frac{C}{2} & \frac{\ell^{n-a-b}}{2} & 0 & 0 \\ \frac{B\ell^{a+c} - 2AC}{2\ell^c} & A & \ell^{a+b} & 0 \\ -\frac{2A + BC\ell^{a+c}}{2\ell^c} & \frac{B\ell^{a+c}}{2} & C\ell^{a+b} & \ell^n \end{pmatrix}$$

where (a, b, c, A, B, C) satisfy the conditions given in the previous section (see Definition 1). The right order of each ideal I is the order with the basis matrix as stated in Theorem 1.

We start by fixing odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$ and an integer $n \geq 1$ as in the statement. Take an arbitrary cyclic left $\mathcal{O}_{1728}$-ideal J of norm ℓ^n and its right order $\mathcal{O}$. By Theorem 1 there is a unique tuple (a, b, c, A, B, C) from the HNF basis of $\mathcal{O}$, satisfying the conditions of Definition 1. Moreover the theorem states by varying J (or equivalently $\mathcal{O}$) we obtain all possible tuples satisfying these conditions. Hence taking I to be $\mathbb{Z}$-lattice defined by the basis matrix in the statement of Theorem 2, to prove Theorem 2, it is enough to show $I = J$. We first show I is a left $\mathcal{O}_{1728}$-ideal and right $\mathcal{O}$-ideal.

Lemma 13. *Continuing from above, I is an (integral) left-ideal of $\mathcal{O}_{1728}$.*

Proof. Let e_0, e_1, e_2, e_3 denote the 4 basis vectors corresponding to the columns of the basis matrix defining I. Let f_0, f_1, f_2, f_3 denote the basis vectors $\frac{1+j}{2}$, $\frac{i+k}{2}$, j, k of $\mathcal{O}_{1728}$. To show I is integral we show $I \subseteq \mathcal{O}_{1728}$ which amounts to showing $e_t \in \mathcal{O}_{1728}$ for $t = 0, 1, 2, 3$. To do this, one may write each e_t as a linear combination of $f_0, ..., f_3$. This is made easier using the integral values of $\omega_i, \lambda_i, \mu_i$ from Lemma 8. We only give one example here, however all the cases are given in SageMath code file `prf_left_ideal.ipynb` for easy verification. To show $e_0 \in \mathcal{O}_{1728}$, for $a < 0$ we have,

$$e_0 = f_0 - Cf_1 + (\ell^c\lambda_4 - \ell^c\lambda_6 + \lambda_7 - 1)f_2 + (\omega_3 - \ell^n\lambda_1 + \delta(2\omega_2\lambda_7 - \omega_2 - \lambda_7))f_3$$

and when $a \geq 0$,

$$e_0 = f_0 - Cf_1 + (\omega_2 + \mu_3 B - AC - 1)f_2 - (\mu_3 BC + A + C(\omega_2 - 1))f_3,$$

where all coefficients are integral.

As I has a basis matrix in lower-triangular form with non-zero diagonal entries, it is clearly full-rank. To complete the proof it remains to show for every $\alpha \in \mathcal{O}_{1728}$ and $\beta \in I$, we have $\alpha\beta \in I$. Since α and β can be written as a linear combination of f_s and e_t respectively, it is enough to show $f_s \cdot e_t \in I$ for $s, t \in \{0, 1, 2, 3\}$. We do this by writing $f_s \cdot e_t$ as integral linear combinations of e_t. Again, see the SageMath code file `prf_left_ideal.ipynb` for the complete list of relations.

Lemma 14. *Continuing from above, I is an (integral) right-ideal of $\mathcal{O}$.*

Proof. We follow the same structure as the precious proof. Let g_0, g_1, g_2, g_3 be the basis vectors $\mathcal{O}$, from the columns of the basis matrix given in Theorem 1. To show $I \subseteq \mathcal{O}$ we must write e_t as linear combinations of g_s. Then to show I is a right-ideal of $\mathcal{O}$ we must show $e_t \cdot g_s \in I$ by writing the 16 combinations of $e_t \cdot g_s$ as linear combinations of e_t. See SageMath file `prf_right_ideal.ipynb` for verification.

We can now complete the proof.

Proof. Proof of Theorem 2 Continuing from above, recall we must argue $I = J$. Since I is a left $\mathcal{O}_{1728}$-ideal and right $\mathcal{O}$-ideal with $\mathcal{O}_{1728}$ and $\mathcal{O}$ maximal, this means $\mathcal{O}_{\text{left}}(I) = \mathcal{O}_{1728}$ and $\mathcal{O}_{\text{right}}(I) = \mathcal{O}$. Hence I is a connecting ideal from $\mathcal{O}_{1728}$ to $\mathcal{O}$. We also know J is a cyclic connecting ideal from $\mathcal{O}_{1728}$ to $\mathcal{O}$, and by [13, Lemma 8] there is only one connecting ideal which is cyclic. Therefore to show $I = J$ we must show I is cyclic. This is obvious from the first column of the basis matrix of I, as it corresponds to a quaternion integer $e_0 \in I$ with reduced trace $\mathrm{Tr}(e_0) = 1$. For I to be non-cyclic, $\frac{I}{g}$ would have to be an integral ideal for some integer $g \geq 2$, so $\frac{e_0}{g} \in \frac{I}{g}$ is a quaternion integer, so $\mathrm{Tr}(\frac{e_0}{g}) = \frac{1}{g}$ is integral, which is a contradiction. Hence I is cyclic.

5 Special Cases

We now give some further results and special cases of the structural results of the previous two sections.

In Section 5.1 we discuss how the results simplify when $\ell \equiv 3 \mod 4$ and additionally when p is a square modulo ℓ. In Section 5.2 we give simplified results for the case $n = 1$, i.e. considering the bases of ideals of a prime norm ℓ, and their right orders. In Section 5.3 we briefly discuss how to obtain upper triangular basis matrices instead of lower triangular. And in Section 5.4 we explain how the previous results can apply to all norm ℓ^n left $\mathcal{O}_{1728}$-ideals and their right orders, not just cyclic ideals.

5.1 Case $\ell \equiv 3 \mod 4$

When $\ell \equiv 3 \mod 4$ we obtain the following simplifications of Theorems 1, 2.

Proposition 1. *Let $p \neq \ell$ be odd primes with $p \equiv 3 \mod 4$ and take n an integer with $n \geq 1$. Let (A, B, C, a, b, c) satisfy the conditions of Definition 1. Also suppose $\ell \equiv 3 \mod 4$, then,*

1. *$a \geq 0$ and $c = 0$,*
2. *in Theorem 2 (but not Theorem 1) we may replace C with 0,*
3. *and if p is a square modulo ℓ, then $(a, b, c) = (0, n, 0)$.*

Proof. (1) Suppose for contradiction $a < 0$. Then $c > 0$ so $\ell^{2c} \mid C^2 + 1$ implies $C^2 \equiv -1 \mod \ell$ and so -1 is a square mod ℓ. This is a contradiction as -1 is a square mod ℓ if and only if $\ell \equiv 1 \mod 4$.

(2) For $a \geq 0$ we have $a + b = n$ so in Theorem 2 we may subtract C multiples of the 4th column from the 3rd. This replaces the C in the 3rd column with 0. Similarly add C multiples of the 2nd column to the 1st column, which is equivalent to replacing C in the first column with 0.

(3) By point (1) $a \geq 0$, $c = 0$ and $a + b = n$. Assume for contradiction that $a > 0$ so $n - b \geq 1$. By definition of α we have $\alpha p \equiv -1 \mod 2\ell^n$. Then $\ell^{n-b}B$ being a square root of $\alpha - 4A^2$ modulo $2\ell^{2n}$ means $\ell^{2(n-b)}B^2 p \equiv \alpha p - 4A^2 p \equiv -1 - 4A^2 p \mod 2\ell^n$. As $\ell \mid \ell^{2(n-b)}$, this reduces to $4A^2 p \equiv -1 \mod \ell$, where on

the left-hand side 4, p and A^2 are all squares modulo ℓ hence $4A^2p$ is a square mod ℓ, whereas on the right, -1 is not a square. This is a contradiction. To conclude we therefore have $a = 0$ and $a + b = n$ so $b = n$.

5.2 Case $n = 1$ - Prime norm ideals

As before take odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$. We now give HNF basis matrices for the set of right orders of left $\mathcal{O}_{1728}$-ideals of norm ℓ, followed by basis matrices of the norm ℓ ideals themselves.

Theorem 3. *Take odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$. Define $\mathbb{Z}$-lattices $\mathcal{O}_1(x)$, $\mathcal{O}_2(x)$, and $\mathcal{O}_3(x, y, z)$ from basis matrices*

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2\ell} & 0 & \frac{1}{\ell} & 0 \\ \frac{x+\delta(2\nmid x)\cdot\ell^2}{2\ell} & \frac{\ell}{2} & \frac{x}{\ell} & \ell \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\ell} & 0 & 0 \\ \frac{\ell}{2} & \frac{x}{\ell} & \ell & 0 \\ 0 & \frac{1}{2} & 0 & 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\ell} & 0 & 0 \\ \frac{1}{2} & \frac{x}{\ell} & 1 & 0 \\ \frac{z+\delta(2\nmid z)\cdot\ell}{2} & \frac{y}{2\ell} & z & \ell \end{pmatrix}.$$

Then the set of maximal orders $\mathcal{O}$ such that $\mathcal{O}$ is the right order of a left-ideal $I \subseteq \mathcal{O}_{1728}$ of norm ℓ, is exactly given by the disjoint union of basis matrices: $\mathcal{O}_1(x)$ for $0 \leq x < \ell^2$ with $x^2 \equiv -1 \mod \ell^2$; $\mathcal{O}_2(x)$ for $0 \leq x < \ell^2$ with $4p \cdot x^2 \equiv -1 \mod \ell^2$; and $\mathcal{O}_3(x, y, z)$ for $0 \leq x < \ell$, $0 \leq y < 2\ell^2$ with $1 + 4px^2 \equiv -py^2 \not\equiv \ell^2 \mod 2\ell^2$ and $0 \leq z < \ell$ is the unique solution to $2x + y \cdot z \equiv 0 \mod \ell$.

Proof. Follows from Theorem 1. Take (A, B, C, a, b, c) satisfying the conditions, then for $n = 1$ we have either $(a, b, c) = (-1, 1, 1), (1, 0, 0)$ or $(0, 1, 0)$.

When $(a, b, c) = (-1, 1, 1)$ we have $0 \leq A < \ell^{n+a} = \ell^{1-1} = 1$ so $A = 0$. Also $\ell^2 = \ell^{2c} \mid C^2 + 1$ and $0 \leq C < \ell^{b+c} = \ell^2$. From $2A + BC \equiv 0 \mod \ell^{b+c} = \ell^2$ we get $2 \cdot 0 + B(-1) \equiv 0 \mod \ell^2$ so $\ell^2 \mid B$. Since $0 \leq B < 2\ell^{2b} = 2\ell^2$ and B is odd we have $B = \ell^2$. Relabelling C with x, the basis matrices from Theorem 1 with $(a, b, c) = (-1, 1, 1)$ are exactly the basis matrices $\mathcal{O}_1(x)$ for the conditions on x in the statement.

For $(a, b, c) = (1, 0, 0)$ we have $0 \leq C < \ell^{b+c} = 1$ so $C = 0$. Also $0 \leq B < 2\ell^{2b} = 2$ and B odd implies $B = 1$. The range on A becomes $0 \leq A < \ell^2$ and we know $\ell^2 = \ell^{2(n-b)} \mid \alpha - 4A^2$ so solving $\alpha - 4A^2 \equiv 0 \mod \ell^2$ is enough to determine the values of A. Multiplying through by p yields $p\alpha - 4pA^2 \equiv 0 \mod \ell^2$ and by the definition of α we have $\alpha p \equiv -1 \mod 2\ell^2$ so certainly $4pA^2 \equiv -1 \mod \ell^2$. Relabelling A with x gives exactly the basis matrices $\mathcal{O}_2(x)$ for the conditions on x in the statement.

Lastly, for $(a, b, c) = (0, 1, 0)$, relabelling A, B, C with x, y, z gives exactly the basis matrices $\mathcal{O}_3(x, y, z)$ in the statement. One must carefully check the conditions on A, B, C align with the conditions given above on x, y, z. The condition that B is a square root of $\alpha - 4A^2$ modulo $2\ell^{2n} = 2\ell^2$ is equivalent to $y^2 \equiv \alpha - 4x^2 \mod 2\ell^2$. Then multiplying by p and using the definition of α gives $1 + 4px^2 \equiv -py^2 \mod 2\ell^2$. This relation also forces y to be odd, and hence B to be odd, as is required. The relation $\ell^{2c} \mid 1 + C^2$ is also trivially true with $c = 0$.

We included the condition $y^2 \not\equiv \ell^2 \mod 2\ell^2$ as then z is uniquely defined by x and y. Removing it and replacing 'the unique solution' with 'a solution' yields an equivalent statement.

Theorem 4. *Take odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$. Define $\mathbb{Z}$-lattices $I_1(x)$, $I_2(x)$, and $I_3(x,y)$ from basis matrices*

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ \frac{\ell-x}{2} & \frac{\ell}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 1 & 0 \\ \frac{\ell+x}{2} & \frac{\ell}{2} & x & \ell \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \frac{\ell}{2} & x & \ell & 0 \\ \ell - x & \frac{\ell}{2} & 0 & \ell \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \frac{y}{2} & x & \ell & 0 \\ \ell - x & \frac{y}{2} & 0 & \ell \end{pmatrix}.$$

Then the set of left $\mathcal{O}_{1728}$-ideals of norm ℓ is exactly given by the disjoint union of basis matrices: $I_1(x)$ for $0 \leq x < \ell$ with $x^2 \equiv -1 \mod \ell$; $I_2(x)$ for $0 \leq x < \ell$ with $4px^2 \equiv -1 \mod \ell$; and $I_3(x,y)$ for $0 \leq x < \ell$, $0 \leq y < 2\ell^2$ with $1 + 4px^2 \equiv -py^2 \not\equiv \ell^2 \mod 2\ell^2$. For orders $\mathcal{O}_1(x)$, $\mathcal{O}_2(x)$, and $\mathcal{O}_3(x,y,z)$ from Theorem 3, the connecting ideals of norm ℓ from $\mathcal{O}_{1728}$ are $I_1(x)$, $I_2(x)$, and $I_3(x,y)$ respectively.

Proof. From the previous proof there are 3 cases with $(a,b) = (-1,1), (1,0)$ or $(0,1)$. For $(a,b) = (-1,1)$, the right orders of norm ℓ ideals were exactly the lattices $\mathcal{O}_1(x)$ for the values of x given, with the tuples (A,B,C,a,b,c) from Theorem 3 corresponding to $(0, \ell^2, x, -1, 1, 1)$. We simply substitute these values into Theorem 2 to achieve the result. The same applies to cases $(a,b) = (1,0)$ and $(0,1)$.

We also apply some further steps to simplify the results. Suppose the resulting basis matrix has columns c_1, c_2, c_3, c_4. In case $(a,b) = (-1,1)$ we apply column operations $c_2 \mapsto c_2 - \frac{\ell-1}{2}c_4$ and $c_1 \mapsto c_1 + c_2 - \frac{\ell-1}{2}c_3 + (x - \frac{\ell-1}{2})c_4$. In case $(a,b) = (1,0)$ we apply $c_1 \mapsto c_1 + c_4$. In case $(a,b) = (0,1)$ we apply $e_3' \mapsto c_3 - zc_4$ then $c_1' \mapsto c_1 + zc_2 + c_4$, and variable z can be removed. Lastly we observe in all cases, by applying column operations, the conditions on x (and y, z) can be taken with smaller moduli. For instance in the case of I_1, x need only be defined modulo ℓ, as we can add multiples of column 4 to column 3, and multiples of column 2 to column 1.

Remark 1. By Proposition 1 when $\ell \equiv 3 \mod 4$ cases $\mathcal{O}_1(x)$ and $I_1(x)$ never occur in Theorems 3, 4. Similarly when p is a square modulo ℓ the relation $4px^2 \equiv -1 \mod \ell$ has no solutions as -1 is a non-square, so cases $\mathcal{O}_2(x)$ and $I_2(x)$ never occur. Combining these, when both $\ell \equiv 3 \mod 4$ and p is a square mod ℓ, only cases $\mathcal{O}_3(x,y,z)$ and $I_3(x,y)$ occur.

5.3 Upper triangular basis matrices

In Theorem 1 and subsequent results we only gave ideal and order basis matrices in a lower triangular form. One may also wish to consider basis matrices in upper triangular form. It is possible to transform the lower triangular matrices into upper triangular using matrix operations. We now give one example of this.

Proposition 2. *The basis matrix of Theorem 1, i.e. of right orders of cyclic norm ℓ^n left $\mathcal{O}_{1728}$-ideals, can be replaced with the following upper triangular matrix in the case $a \geq 0$,*

$$\begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{-p(2A+BC)}{2\ell^{n+c}} \\ 0 & \ell^{n-c} & -pA & \frac{p(2AC-B)}{2\ell^{n+c}} \\ 0 & 0 & \frac{\ell^c}{2} & -\frac{C}{2\ell^n} \\ 0 & 0 & 0 & \frac{1}{2\ell^n} \end{pmatrix}.$$

Proof. Fix an order $\mathcal{O}$ given by the basis matrix in Definition 1 for which $a \geq 0$ and let (e_t) denote it's basis. As $\mathcal{O}$ is an order we know $1 \in \mathcal{O}$ and since $i \in \mathcal{O}_{1728}$ and the connecting ideal to $\mathcal{O}_0$ has norm ℓ^n, we have $\ell^n i \in \mathcal{O}$. Also as a ring we have $e_1e_2, e_1e_3, e_2e_3 \in \mathcal{O}$. Hence, we may extend the basis matrix of $\mathcal{O}$ to the spanning set $1, \ell^n i, e_1e_2, e_1e_3, e_2e_3$. This corresponding 4×8 matrix can then be reduced to a 4×4 matrix followed by columns of 0s via integral column operations. We do this in such a way that yields the upper triangular matrix given above, using Lemma 8 to ensure the column operations are integral. The reduction is given in SageMath code file `prf_up_tri.ipynb`.

5.4 Non-cyclic ideals

Next we consider the requirement of ideals to be cyclic in Theorems 1, 2. In particular, upon removing the cyclic condition, how would the result, and the relations on variables (A, B, C, a, b, c) change? One immediate consequence is the proof of Lemma 7 would not hold, so we would not necessarily have either $a + b = n$ or $b = n$. In turn, this would have broken the proof of Lemma 11 for which a fix is not obvious. There is however a simple observation that addresses the bases of non-cyclic ideals, which we now give.

Remark 2 (Non-cyclic ideals). Suppose we want to describe the basis of the right order of an arbitrary norm ℓ^m (integral) left $\mathcal{O}_{1728}$-ideal which may or may not be cyclic. Let I denote such an ideal. There exists some integer $g \geq 1$ such that $\frac{I}{g}$ is a cyclic left $\mathcal{O}_{1728}$-ideal, and $N(\frac{I}{g}) = N(I)/g^2 \in \mathbb{Z}$. Hence we may write $g = \ell^r$ for some $r \geq 0$. Since $\frac{I}{\ell^r}$ is a cyclic left $\mathcal{O}_{1728}$-ideal of norm ℓ^{m-2r}, its right order is of the form in Theorem 1 with $n = m - 2r$. In the definition of right order, scalars don't change anything, meaning the right order $\mathcal{O}_{\text{right}}(I)$ is equal to the right order $\mathcal{O}_{\text{right}}(\frac{I}{\ell^r} I)$. In other words, to obtain all possible right orders of norm ℓ^m left $\mathcal{O}_0$-ideals, we use Theorem 1 for each $r \geq 0$ such that $m - 2r \geq 0$. The same argument applies to the bases of all ideals I of norm ℓ^m; we use Theorem 2 with $n = m - 2r \geq 0$ for each $r \geq 0$, although in this case we must multiply the ideal basis by ℓ^r.

6 Parametrization Results

Recall in Theorems 1, 2, we gave basis matrices of all cyclic norm ℓ^n ideals I from $\mathcal{O}_{1728}$ and their right orders $\mathcal{O}$, in terms of variables (A, B, C, a, b, c) satisfying a set of conditions. The basis matrices of $\mathcal{O}$ and I were precisely,

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\ell^{a+b}} & 0 & 0 \\ \frac{\ell^a}{2} & \frac{A}{\ell^n} & \ell^a & 0 \\ \frac{C+\delta(2\nmid C)\cdot\ell^{b+c}}{2\ell^c} & \frac{B}{2\ell^b} & \frac{C}{\ell^c} & \ell^b \end{pmatrix} \text{ and } \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ -\frac{C}{2} & \frac{\ell^{n-a-b}}{2} & 0 & 0 \\ \frac{B\ell^{a+c}-2AC}{2\ell^c} & A & \ell^{a+b} & 0 \\ -\frac{2A+BC\ell^{a+c}}{2\ell^c} & \frac{B\ell^{a+c}}{2} & C\ell^{a+b} & \ell^n \end{pmatrix}.$$

We will denote these $\mathbb{Z}$-lattices as $\mathcal{O}(A, B, C, a, b, c)$ and $I(A, B, C, a, b, c)$ respectively.

We now show in the case that $-p$ is a square modulo ℓ, these variables can essentially all be written in terms of a single variable d. Also the base ℓ expansion of d specifies 'directions' at each step along the walk in the quaternion ℓ-ideal graph. Our result can be stated as follows.

Theorem 5. *Fix odd primes $p \neq \ell$ with $p \equiv 3 \mod 4$ and $-p$ a square modulo ℓ. Take an integer $n \geq 1$. Also fix an r such that $r^2 \equiv -p \mod \ell^{2n}$. All ideals below are cyclic norm ℓ^n left $\mathcal{O}_{1728}$-ideals.*

A. *We generate distinct ideals I and their right orders $\mathcal{O}$, with $a \geq 0$, as follows. For every $0 \leq d \leq \ell^n - 1$ such that $\ell \nmid d^2 + 1$, define $a \leq n$ maximal such that $\ell^a \mid d$, and let $d' = \frac{d}{\ell^a}$. Let x, y, z be the unique solutions to $x \cdot 2r(d^2+1) \equiv d^2 - 1 \mod \ell^{2n}$, $y \cdot r(d^2+1) \equiv -d' \mod \ell^{2n-2a}$ and $z \cdot 2d' \equiv d^2 - 1 \mod \ell^{n-a}$. Then (Case 1), $I(x, 2y + \ell^{2n-2a}, z, a, n-a, 0)$ and $\mathcal{O}(x, 2y + \ell^{2n-2a}, z, a, n-a, 0)$ are norm ℓ^n ideals and their right orders. Also when $a > 0$ we obtain additional distinct ideals and orders from (Case 2), $I(-x, 2y + \ell^{2n-a}, \ell^{n-a} - z, a, n-a, 0)$ and $\mathcal{O}(-x, 2y + \ell^{2n-2a}, \ell^{n-2a} - z, a, n-a, 0)$.*

B. *We generate distinct ideals I and their right orders $\mathcal{O}$ with $a < 0$ as follows. For this we must have $\ell \equiv 1 \mod 4$ (by Proposition 1) so fix an r_{-1} with $r_{-1}^2 \equiv -1 \mod \ell^{2n}$. For every $0 \leq d \leq \ell^n - 1$ with $\ell \mid d$ define $c \leq n$ maximal such that $\ell^c \mid d$. If $d = 0$ set $d' = 1$, otherwise set $d' = \frac{d}{\ell^c}$. Let x, y, z be the unique solutions to $x \cdot 4rd' \equiv d^2 + 1 \mod \ell^{2n}$, $y \cdot 4rd' \equiv r_{-1}(d^2 - 1) \mod \ell^{2n}$ and $z \cdot (d^2 - 1) \equiv r_{-1}(d^2 + 1) \mod \ell^{n+c}$. Then (Case 1) $I(x, 2y + \ell^{2n}, z, -c, n, c)$ and $\mathcal{O}(x, 2y + \ell^{2n}, z, -c, n, c)$ are norm ℓ^n ideals and their right orders. And (Case 2) so are $I(-x, 2y + \ell^{2n}, \ell^{n+c} - z, -c, n, c)$ and $\mathcal{O}(-x, 2y + \ell^{2n}, \ell^{n+c} - z, -c, n, c)$.*

C. *Every norm ℓ^n cyclic ideal from $\mathcal{O}_{1728}$ is generated by either point A or point B. And hence so are all right orders of such ideals.*

D. *Let I be an ideal generated from Part A. or B. from value d. Consider the base ℓ expansion $d = \sum_{r=0}^{n-1} d_r \ell^r$. Viewing I as an ℓ-isogeny walk, the values d_r can be considered a choice of direction at each step. This means for any decomposition $I = I_1 I_2$ with $N(I_1) = \ell^m$ and $N(I_2) = \ell^{n-m}$, the ideal I_1 arises from the same construction (Part A. or B., Case 1 or 2) replacing n with m, and d with $\sum_{r=0}^{m-1} d_r \ell^r$.*

This result is a generalisation of the results of [1].

Remark 3. Take odd primes $p \neq \ell$, and an integer $n \geq 1$. Suppose we are in the special case of $\ell \equiv 3 \mod 4$ and $p = 4\ell^e f - 1$ where $e \geq 1$ and $n \leq e$. Then the parametrization of ideals in Theorem 5 is the same as [1, Proposition 3.3] using the same value d. Although note the definitions of $\mathcal{O}_{1728}$ differ, by switching the roles of j and k. Our Case 1 and Case 2 correspond to their "$d_0 \neq \infty$" and "$d_0 = \infty$" cases. Our variables A, B, C correspond to their variables α, β with $A \equiv \alpha \mod \ell^n$ and $\frac{B\ell^a}{2} \equiv \beta \mod \ell^n$, and $C \equiv 0 \mod \ell^n$ (recall Proposition 1 point (2)). Using their results, the directions represented by values $d_0, ..., d_{n-1}$ in the ℓ expansion of d, can be interpreted as 2×2 matrix multiplications in a Bruhat-Tits tree Also the kernel generator of the corresponding ℓ^n-isogeny can be expressed in terms of d and a special choice of ℓ^e-torsion basis of E_{1728}.

The remainder of this section is dedicated to proving Theorem 5.

6.1 Proof of Theorem 5 Part A..

Throughout this section we will take (A, B, C, a, b, c) to be a tuple generated by Theorem 5 Part A. using an integer $0 \leq d \leq \ell^n - 1$, so $a \geq 0$. This is either (Case 1) $(x, 2y + \ell^{2n-2a}, z, a, n-a, 0)$ or (Case 2) $(-x, 2y + \ell^{2n-a}, \ell^{n-a} - z, a, n-a, 0)$. First notice that A and B are not necessarily in the ranges needed to apply Theorem 5, as for instance for $A = x$ (in Case 1) we have $0 \leq A \leq \ell^{2n}$ when we need $0 \leq A < \ell^{n+a}$ for the theorem. We use the following observation to address this.

Lemma 15. *For any $k_1, k_2 \in \mathbb{Z}$, let $A' = A + k_1\ell^{n+a}$ and $B' = B + k_1 2C\ell^{b-c} + k_2 2\ell^{2b}$ then, $\mathcal{O}(A, B, C, a, b, c) = \mathcal{O}(A', B', C, a, b, c)$, and $I(A, B, C, a, b, c) = I(A', B', C, a, b, c)$, providing $\ell^{2c} \mid C^2 + 1$.*

Proof. See code file `prf_AB_prime.ipynb` for verification. The first relation comes from examining the basis matrix of $\mathcal{O}(A, B, C, a, b, c)$ and applying the unimodular column operation $c_2' = c_2 + k_1 c_3 + k_2 c_4$. The second comes from the basis matrix of $I(A, B, C, a, b, c)$ applying $c_2' = c_2 + k_1\ell^{n-b}c_3 + (k_1 C\frac{1-\ell^{a+c}}{\ell^c} + k_2\ell^b)c_4$ and $c_1' = c_1 + (k_1 C\frac{1-\ell^{a+c}}{\ell^c} + k_2\ell^b)c_3 + (k_1\frac{C^2+1}{\ell^{2c}}(\ell^{a+c} - 2) - 2k_1\frac{1-\ell^{a+c}}{\ell^{2c}} - 2k_2 C\ell^{b-c})c_4$, where $\frac{1-\ell^{a+c}}{\ell^c}$ and $\frac{1-\ell^{a+c}}{\ell^{2c}}$ are integral in both cases $a \geq 0, c = 0$ and $a < 0, c = -a$.

In Part A., with $a \geq 0$, since $c = 0$ the condition $\ell^{2c} \mid C^2 + 1$ is trivially true. From now on we fix k_1 such that $0 \leq A' < \ell^{n+a}$, and k_2 such that $0 \leq B' < 2\ell^{2b}$ so A' and B' are within the desired ranges. To prove Theorem 5 Part A., we will show the tuple (A', B', C, a, b, c) satisfies all the conditions of Definition 1 so we may apply Theorems 5 and 2.

Lemma 16. *Continuing from above we have:*
1. *B' is odd,*
2. *$2A' + B'C \equiv 0 \mod \ell^{n-a}$,*
3. *and $pB'^2\ell^{2a} \equiv -1 - 4pA'^2 \mod 2\ell^{2n}$.*

Proof. Since $B = 2y + \ell^{2n-2a}$ and $B' = B + k_1 2C\ell^{n-a} + k_2 2\ell^{2n-2a}$, both are clearly odd.

Now we prove $A + yC \equiv 0 \mod \ell^{n-a}$. Recall we have either $(A, C) = (x, z)$ (Case 1) or $(A, C) = (-x, \ell^{n-a} - z)$ (Case 2). It is sufficient to prove this relation for $(A, C) = (x, z)$ as Case 2 holds by multiplying by -1. Since $\ell \nmid d^2 + 1$ the claim is equivalently, $2r(d^2 + 1)x + r(d^2 + 1)y \cdot 2z \equiv 0 \mod \ell^{n-a}$. By definition of x and y the left-hand side is equivalent to $(d^2 - 1) - 2d'z \mod \ell^{n-a}$ and applying the definition of z we get zero.

Point (2) then follows from using the definitions of A', B' and B, and subtracting the relation $A+yC \equiv 0 \mod \ell^{n-a}$. The relation then becomes $2k_1\ell^{n+a} + (\ell^{2n-2a} + k_1 2C\ell^{n-a} + k_2 2\ell^{2n-2a})C \equiv 0 \mod \ell^{n-a}$, which is clearly true.

Next we prove $pB^2\ell^{2a} \equiv -1 - 4pA^2 \mod \ell^{2n}$. In either case of $A = \pm x$ we have $A^2 = x^2$. Also $B^2\ell^{2a} = (2y + \ell^{2n-2a})^2\ell^{2a} \equiv 4y^2\ell^{2a} \mod \ell^{2n}$. Multiplying through by $(d^2 + 1)^2$ and noting $r^2 \equiv -p$, the claim can then be rewritten as $-4(r(d^2+1)y)^2\ell^{2a} \equiv -(d^2+1)^2 + (2r(d^2+1)x)^2 \mod \ell^{2n}$. Using the definitions of x, y and d' this is equivalent to $-4d^2 \equiv -(d^2+1)^2 + (d^2-1)^2 \mod \ell^{2n}$, which clearly holds.

Finally we prove point (3). Since B' is odd the result is trivially true modulo 2, and so by Chinese Remainder Theorem it is then sufficient to prove it modulo ℓ^{2n}. Using the definitions of A', B' the statement may be written as,

$$p(B\ell^a + k_1 2C\ell^n + k_2 2\ell^{2n-a})^2 \equiv -1 - 4p(A + k_1\ell^{n+a})^2 \mod 2\ell^{2n}$$

expanding the brackets gives,

$$p(B^2\ell^{2a} + 4k_1 BC\ell^{n+a}) \equiv -1 - 4p(A^2 + 2k_1 A\ell^{n+a}) \mod 2\ell^{2n}.$$

Since we proved the same statement above for A, B we may subtract it, reducing proving point (3) to showing,

$$4pk_1 BC\ell^{n+a} \equiv -8pk_1 A\ell^{n+a} \mod \ell^{2n}.$$

Using the definition of B, and dividing through this is equivalent to $k_1(A+Cy) \equiv 0 \mod \ell^{n-a}$, which we previously showed was true.

Corollary 1. *The $\mathbb{Z}$-lattice $I(A, B, C, a, b, c)$ is a cyclic norm ℓ^n left $\mathcal{O}_{1728}$-ideal with right order $\mathcal{O}(A, B, C, a, b, c)$.*

Proof. The construction of (A', B', C, a, b, c), together with the previous lemma shows it satisfies all the conditions of Definition 1. Hence by Theorem 5, $\mathcal{O}(A', B', C, a, b, c)$ is the right order of a norm ℓ^n ideal from $\mathcal{O}_{1728}$. And by Theorem 2, $I(A', B', C, a, b, c)$ is the connecting ideal. Then Lemma 15 shows we can replace A', B' with A, B.

We now complete the proof of Theorem 5 Part A..

Lemma 17. *The ideals/orders generated in the statement of Theorem 5 Part A..*

Proof. Suppose from the statement of Part A. we generate two tuples $(A_i, B_i, C_i, a_i, n - a_i, 0)$ from integers d_i for $i = 1, 2$ which result in the same order. Also note for each i we are either in Case 1, with $A_i = x_i$, $C_i = z_i$, or Case 2, with $A_i = -x_i$,

$C_i = \ell^{n-a_i} - z_i$. Now use Lemma 15 to reduce them to $(A_i', B_i', C_i, a_i, n - a_i, 0)$ with A_i', B_i' in the correct ranges as we did previously. We've already shown these tuples satisfy the conditions to apply Theorem 1. And recall the theorem states a bijection between such tuples and orders, hence since the orders are equal, the tuples are equal, i.e. $A_1' = A_2'$, $B_1' = B_2'$, $C \coloneqq C_1 = C_2$, $a \coloneqq a_1 = a_2$. Without loss of generality we may consider three cases: for $i = 1, 2$ we are in Case 1; for $i = 1, 2$ we are in Case 2; or for $i = 1$ we are in Case 1, and for $i = 2$ are in Case 2. In each case we prove the result by obtaining a contradiction from $d_1 \neq d_2$.

For both in Case 1, we have $A_i' \equiv x_i \mod \ell^{n+a}$ so $x_1 \equiv x_2 \mod \ell^{n+a}$. By definition of x_i this means $(d_2^2 + 1)(d_1^2 - 1) \equiv (d_1^2 + 1)(d_2^2 - 1) \mod \ell^{n+a}$ which expanded gives $d_1^2 \equiv d_2^2 \mod \ell^{n+a}$. Also note $d_1, d_2 \neq 0$ since if one is zero we have $a = n$ so $a_1 = n$ and $a_2 = n$ which is only possible if $d_1 = d_2 = 0$. Hence there are exactly two square roots of d_2^2 modulo ℓ^{n+a} and these are $d_1 \equiv \pm d_i \mod \ell^{n+a}$. Since $0 \leq d_i \leq \ell^n - 1$, $a \geq 0$, and $d_1 \neq d_2$ we have $d_1 = -d_2$. From $z_1 = C_1 = C_2 = z_2$ we get $(d_1^2 - 1)\frac{d_2}{\ell^a} \equiv (d_2^2 - 1)\frac{d_1}{\ell^a} \mod \ell^{n-a}$. Substituting in $d_1 = -d_2$ gives $(d_2^2 - 1)d_2 \equiv -(d_2^2 - 1)d_2 \mod \ell^n$ implying $d_2 \equiv 0 \mod \ell^n$ which by the range on d_2 gives $d_2 = 0$ which is a contradiction.

For the ideals generated from $i = 1, 2$ both in Case 2, we have $-x_1 \equiv A_1' = A_2' \equiv -x_2 \mod \ell^{n+a}$ and $\ell^{n-a} - z_1 = C_1' = C_2' = \ell^{n-a} - z_2$. This means we still have $x_1 \equiv x_2 \mod \ell^{n-a}$ and $z_1 = z_2$, so a contradiction arises from exactly the same method as Case 1.

Finally for $i = 1$ in Case 1, and $i = 2$ in Case 2 we get $x_1 \equiv -x_2 \mod \ell^{n+a}$. Hence $(d_2^2 + 1)(d_1^2 - 1) \equiv -(d_1^2 + 1)(d_2^2 - 1) \mod \ell^{n+a}$ which expanded gives $d_1^2 d_2^2 \equiv 1 \mod \ell^{n+a}$. This means $\ell \nmid d_1$ and $\ell \nmid d_2$ so $a = 0$. This is a contradiction as in the statement of Theorem 5 Part A. we only generate ideals/orders in Case 2 when $a > 0$.

6.2 Proof of Theorem 5 Part B..

To prove Part B. we follow the same approach as the previous section. Take (A, B, C, a, b, c) to be a tuple generated by Theorem 5 Part B. using an integer $0 \leq d \leq \ell^n - 1$, so $a = -c < 0$. This is either (Case 1) $(x, 2y + \ell^{2n}, z, -c, n, c)$ or (Case 2) $(-x, 2y + \ell^{2n}, \ell^{n+c} - z, -c, n, c)$. First we check the following condition on C.

Lemma 18. *Following from above,* $\ell^{2c} \mid C^2 + 1$.

Proof. With either $C = z$ or $C = \ell^{n+c} - z$ we have $C^2 \cong z^2 \mod \ell^{2c}$. Then by definition of z, $C^2 \cdot (d^2 - 1)^2 \equiv (z(d^2 - 1))^2 \equiv (r_{-1}(d^2 + 1))^2 \mod \ell^{2c}$. Rearranging this is $(C^2 + 1)(d^2 + 1)^2 - 4d^2C^2 \equiv 0 \mod \ell^{2c}$. Noting that $\ell^{2c} \mid d^2$ by construction, and dividing by $(d^2 + 1)^2$ which is coprime to ℓ, gives the result.

Similarly to before, A and B are not within the correct ranges to meet the criteria to apply Theorem 1. However we may again apply Lemma 15, whose proof remains the same for $a < 0$, and the condition $\ell^{2c} \mid C^2 + 1$ holds. This means defining $A' = A + k_1\ell^{n+a}$ with k_1 chosen such that $0 \leq A' < \ell^{n+a}$ and $B' = B + k_1 2C\ell^{b-c} + k_2 2\ell^{2b}$ with k_2 chosen so $0 \leq B' < 2\ell^{2b}$, we have that,

$$\begin{aligned} \mathcal{O}(A,B,C,a,b,c) &= \mathcal{O}(A',B',C,a,b,c) \\ \text{and} \quad I(A,B,C,a,b,c) &= I(A',B',C,a,b,c). \end{aligned}$$

The following conditions then hold.

Lemma 19. *Following from above,*

- *B' is odd,*
- $2A' + B'C \equiv 0 \mod \ell^{n+c}$,
- *and $pB'^2 \equiv -\ell^{2c} - 4pA'^2 \mod 2\ell^{2n}$.*

Proof. Clearly $B = 2y + \ell^{2n}$ is odd, and so $B' = B + k_1 2C\ell^{n-c} + k_2 2\ell^{2n}$ is odd.

For point (2), with (Case 1) $A = x$ and $C = z$, expanding definitions we have

$$\begin{aligned} (2rd')(2A + BC) &\equiv 4rd'x + 4rd'yz \mod \ell^{n+c} \\ &\equiv (d^2+1) + r_{-1}(d^2-1)z \mod \ell^{n+c} \\ &\equiv (d^2+1) - (d^2+1) \equiv 0 \mod \ell^{n+c}. \end{aligned}$$

An the same holds for (Case 2) $A = -x$ and $C = \ell^{n+c} - z$, hence $2A + BC \equiv 0 \mod \ell^{n+c}$. Then we have $2A' + B'C \equiv 2(A + k_1\ell^{n-c}) + (B + k_1 2C\ell^{n-c})C \mod \ell^{n+c}$. Subtracting the relation for A, B gives, $2A' + B'C \equiv (C^2+1)2k_1\ell^{n-c} \mod \ell^{n+c}$ which is zero by the previous Lemma.

For point (3) we have in both cases,

$$\begin{aligned} 4d'^2(pB^2 + \ell^{2c} + 4pA^2) &\equiv -(4d'ry)^2 + 4d'^2\ell^{2c} - (4rd'x)^2 \mod \ell^{2n} \\ &\equiv (d^2-1)^2 + 4d^2 - (d^2+1)^2 \equiv 0 \mod \ell^{2n}. \end{aligned}$$

Hence $pB^2 + \ell^{2c} + 4pA^2 \equiv 0 \mod \ell^{2n}$. Then using the definitions of A', B' we expand $4d'^2(pB'^2 + \ell^{2c} + 4pA'^2)$ and subtract the above relation leaving,

$$4pk_1\ell^{n-c}(2A + BC + (C^2+1)k_1\ell^{n-c}) \equiv 0 \mod \ell^{2n},$$

where we use the previous Lemma, and relation $2A + BC \equiv 0 \mod \ell^{n+c}$. This relation also holds modulo 2, hence by Chinese Remainder Theorem point (3) holds.

Combining all these results we have the following.

Corollary 2. *The $\mathbb{Z}$-lattice $I(A,B,C,a,b,c)$ is a cyclic norm ℓ^n left $\mathcal{O}_{1728}$-ideal with right order $\mathcal{O}(A,B,C,a,b,c)$.*

Proof. The previous results show (A', B', C, a, b, c) satisfies the conditions of Definition 1. Hence by Theorems 5 and 2, and Lemma 15 the result holds.

Just like the previous section, the following observation completes the proof of Theorem 5 Part B..

Lemma 20. *The ideals/orders generated in the statement of Theorem 5 Part B. are all distinct.*

Proof. Similar to Lemma 17. Suppose from the statement of Part B. we generate two tuples $(A_i, B_i, C_i, -c_i, n, c_i)$ from integers d_i for $i = 1, 2$ which result in the same order. For each i, we have (Case 1) $A_i = x_i, C_i = z_i$ or (Case 2) $A_i = -x_i, C_i = \ell^{n+c_i} - z_i$. Reduce A_i, B_i to A'_i, B'_i in the correct ranges as above. Then by the bijection of Theorem 1 we have $A'_1 = A'_2$, $B'_1 = B'_2$, $C \coloneqq C_1 = C_2$ and $c \coloneqq c_1 = c_2$.

For both tuples from Case 1, or both from Case 2, $A'_1 = A'_2$ and $C_1 = C_2$ give $x_1 \equiv x_2 \mod \ell^{n-c}$ and $z_1 \equiv z_2 \ell^n$. Using the definitions of x_i and z_i these relations give $d_2(d_1^2 + 1) \equiv d_1(d_2^2 + 1) \mod \ell^n$ and $d_1^2 \equiv d_2^2 \mod \ell^n$ respectively. Since $d_1 \neq d_2$, the second of these implies $d_1 \equiv -d_2 \mod \ell^n$, which substituted into the first gives $d_2(d_2^2 + 1) \equiv 0 \mod \ell^n$. Since $c > 0$ we know $\ell \mod d_2$ so $\ell \nmid d_2^2 + 1$, hence $\ell^n \mid d_2$. This implies $d_2 = 0$ so $c = n$. This is a contradiction as the only value d_1 can take such that $\ell^c \mid d_1$ is $d_1 = 0$, but $d_1 \neq d_2$.

For the $i = 1$ tuple from Case 1, and $i = 2$ from Case 2, we have $z_1 \equiv -z_2 \mod \ell^n$. By definition of z_i this gives, $d_1^2 d_2^2 \equiv 1 \mod \ell^n$. By construction $c > 0$ so $\ell \mid d_i$ for $i = 1, 2$ which gives a contradiction.

6.3 Proof of Theorem 5 Part C..

We've previously shown the ideals generated by Part A. are all distinct, as are those generated by Part B.. These two sets are also distinct from each other, by the bijection of Theorem 1, since the sets contain ideals with $a < 0$ and $a \geq 0$ respectively. We may then prove the claim that Parts A. and B. give all cyclic norm ℓ^n ideals from $\mathcal{O}_{1728}$ by a counting argument, showing the sum of the sizes of the two sets equals the total number of cyclic ℓ^n isogenies. This total number is now given.

Lemma 21. *For odd primes $\ell \neq p$ with $p \equiv 3 \mod 4$ there are $\ell^n + \ell^{n-1}$ cyclic left-ideals of $\mathcal{O}_{1728}$ of norm ℓ^n.*

Proof. We consider an ℓ^n isogeny as a decomposed chain of n ℓ-isogenies. From [7, Proposition 1] it follows that an ℓ^n-isogeny is cyclic if and only if there is no immediate backtracking in any decomposition. In the first step there are $\ell + 1$ choices of ℓ-isogeny, and in subsequent steps there only ℓ as one direction is the dual of the previous isogeny in the chain, i.e. immediately backtracking. In total this gives $(\ell + 1)\ell^{n-1}$ options.

We now count the number of ideals from Part A..

Lemma 22. *Take p, ℓ, n as in Theorem 5. The number of ideals generated by Part A. of the Theorem is,*

- *$\ell^n + \ell^{n-1}$ when $\ell \equiv 3 \mod 4$, consisting of ℓ^n in Case 1 and ℓ^{n-1} in Case 2,*
- *And $\ell^n - \ell^{n-1}$ when $\ell \equiv 1 \mod 4$, consisting of $\ell^n - 2\ell^{n-1}$ in Case 1 and ℓ^{n-1} in Case 2.*

Proof. For Case 1 we simply count the number of $0 \leq d \leq \ell^n - 1$ with $\ell \nmid d^2 + 1$. For $\ell \equiv 3 \mod 4$, -1 is not a square, so this is all ℓ^n of them, since if $\ell \mid d^2 + 1$ we'd have $d^2 \equiv -1 \mod \ell$ which is impossible.

For $\ell \equiv 1 \mod 4$, we exclude the values of d where $d^2 \equiv -1 \mod \ell$, which are all values of d which are equal to one of the two square roots of -1 modulo ℓ, call them r_{-1} and $\ell - r_{-1}$. That means excluding values $d = r_{-1} + k\ell$ and $\ell - r_{-1} + k\ell$ for $0 \leq k < \ell^{n-1}$, which is $2\ell^{n-1}$ values. This means we have $\ell^n - 2\ell^{n-1}$ distinct ideals.

For Case 2 we count all $0 \leq d \leq \ell^n - 1$ with $\ell \mid d$ and $\ell \nmid d^2 + 1$. Since the second condition is implied by the first we just count d with $\ell \mid d$ and there are always ℓ^{n-1} of them.

The number of ideals from Part B. is then as follows.

Lemma 23. *Take p, ℓ, n as in Theorem 5. The number of ideals generated by Part B. of the Theorem is $2\ell^{n-1}$ when $\ell \equiv 1 \mod 4$ and 0 otherwise.*

Proof. By the statement of Theorem 5 Part B. we require $\ell \equiv 1 \mod 4$ for r_{-1} to exist. For each $0 \leq d < \ell^n$ with $\ell \mid d$ we generate two ideals, one in Case 1, and one in Case 2. This gives a total of $2\ell^{n-1}$.

This completes the proof as the counts of Lemmas 22 and 23 sum to that of Lemma 21.

6.4 Proof of Theorem 5 Part D..

We first give a classical result on cyclic ideal decomposition.

Lemma 24. *Let I be a cyclic integral left $\mathcal{O}$-ideal for a quaternion order $\mathcal{O}$, with $N(I) = N_1 N_2$. Let $I_1 = I + \mathcal{O}N_1$ and $I_2 = \frac{\overline{I_1} I}{N_1} = I + \mathcal{O}_{\text{right}}(I)N_2$. Then $I = I_1 I_2$, and I_1, I_2 are cyclic integral ideals of norms N_1 and N_2 respectively.*

Proof. Expanding definitions one can check $I = I_1 I_2$ holds. The ideals are integral as $I_1 \subseteq \mathcal{O}$ and $I_2 \subseteq \mathcal{O}_{\text{right}}(I)$, and cyclic as I is cyclic. To show their norms are as claimed, note that for any cyclic integral ideal J we have $\mathbb{Z} \cap J = N(J) \cdot \mathbb{Z}$.

We can now prove Part D. of the Theorem.

Proof of Theorem 5 Part D.. We prove the result for ideals generated by Part B. first. Take some integer $0 \leq d < \ell^n$ with ℓ-expansion $d = \sum_{r=0}^{n-1} d_r \ell^r$, and let $\tilde{d} = \sum_{r=0}^{m-1} d_r \ell^r$. By Part B. of the Theorem, generate values c, x, y, z from d and $\tilde{c}, \tilde{x}, \tilde{y}, \tilde{z}$ from $\tilde{d}$. Then (in Case 1 or 2) we obtain tuples (A, B, C, a, b, c) and $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{a}, \tilde{b}, \tilde{c})$ from d and $\tilde{d}$ respectively, which give norm ℓ^n and ℓ^m ideals I and I_1. By Lemma 24 we know that $I + \mathcal{O}_{1728}\ell^m$ is a cyclic integral ideal of $\mathcal{O}_{1728}$ of norm ℓ^m such that $I = (I + \mathcal{O}_{1728}\ell^m) \cdot I_2$ for some cyclic integral ideal I_2. Hence to prove the result we must show $I_1 = I + \mathcal{O}_{1728}\ell^m$, and since they have the same norm it is sufficient to show the single inclusion $I + \mathcal{O}_{1728}\ell^m \subseteq I_1$. By noting $a = -c$ and $b = n$, the ideal $I + \mathcal{O}_{1728}\ell^m$ can be represented by the following matrix, with columns representing the concatenation of the bases of I and $\mathcal{O}_{1728}\ell^m$,

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 & \frac{\ell^m}{2} & 0 & 0 & 0 \\ -\frac{C}{2} & \frac{\ell^c}{2} & 0 & 0 & 0 & \frac{\ell^m}{2} & 0 & 0 \\ \frac{B-2AC}{2\ell^c} & A & \ell^{n-c} & 0 & \frac{\ell^m}{2} & 0 & \ell^m & 0 \\ -\frac{2A+BC}{2\ell^c} & \frac{B}{2} & C\ell^{n-c} & \ell^n & 0 & \frac{\ell^m}{2} & 0 & \ell^m \end{pmatrix}.$$

We refer to these spanning vectors (columns) as $e_0, ..., e_7$. As I_1 is a norm ℓ^m ideal, it also contains $\mathcal{O}_{1728}\ell^m$, hence we can represent it with the following matrix,

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ -\frac{\tilde{C}}{2} & \frac{\ell^{\tilde{c}}}{2} & 0 & 0 & \frac{\ell^m}{2} & 0 \\ \frac{\tilde{B}-2\tilde{A}\tilde{C}}{2\ell^{\tilde{c}}} & \tilde{A} & \ell^{m-\tilde{c}} & 0 & 0 & \ell^m \\ -\frac{2\tilde{A}+\tilde{B}\tilde{C}}{2\ell^{\tilde{c}}} & \frac{\tilde{B}}{2} & \tilde{C}\ell^{m-\tilde{c}} & \ell^m & \frac{\ell^m}{2} & 0 \end{pmatrix}$$

consisting of the basis of I with additional vectors from $\mathcal{O}_{1728}\ell^m \in I$. We refer to these vectors (columns) as $f_0, ..., f_5$. We'll show $I + \mathcal{O}_{1728}\ell^m \subseteq I_1$ by proving each vector $e_i \in I_1$ for each i. Clearly $e_i \in I_1$ for $i = 4, ...7$ as $\mathcal{O}_{1728}\ell^m \subseteq I_1$. Also $e_3 = \ell^{n-m} f_3 \in I_1$. For the remaining vectors note by definition of c and $\tilde{c}$ we have $\tilde{c} = \min(c, m)$. Also as $d \equiv \tilde{d} \mod \ell^m$ we have

$$\tilde{x} \cdot 4r\tilde{d}\ell^{c-\tilde{c}} \equiv \ell^c(\tilde{d}^2 + 1) \equiv \ell^c(d^2 + 1) \equiv x \cdot 4rd \mod \ell^m$$

so (in both Cases) $\tilde{A} \cdot \ell^{c-\tilde{c}} \equiv A \mod \ell^m$. We similarly obtain $\tilde{B} \cdot \ell^{c-\tilde{c}} \equiv B \mod 2\ell^m$, and $\tilde{C} \equiv C \mod \ell^m$. We may then define integers k_A, k_B, k_C such that $A = \tilde{A}\ell^{c-\tilde{c}} + k_A\ell^m$, $B = \tilde{B}\ell^{c-\tilde{c}} + 2k_B\ell^m$ and $C = \tilde{C} + k_C\ell^m$. We then have $e_2 = \ell^{(n-c)-(m-\tilde{c})}(f_2 + k_C\ell^{m-\tilde{c}}f_3) \in I_1$ where $m - \tilde{c} < n - c$ so the exponents are integral. This gives $e_1 = \ell^{c-\tilde{c}}f_1 + k_A f_5 + k_B f_3 \in I_1$. Next, one can show from expanding definitions that there exists k_1 such that $(\frac{B-2AC}{2\ell^c}) = (\frac{\tilde{B}-2\tilde{A}\tilde{C}}{2\ell^{\tilde{c}}}) + k_1\ell^m$. And from the property $2A+BC \equiv 0 \mod \ell^{n+c}$, since B is odd this lifts to $2A+BC \equiv \delta(2 \nmid C)\ell^{n+c} \mod 2\ell^{n+c}$. Applying the same to $\tilde{A}, \tilde{B}, \tilde{C}$, there exists some integer k_2 such that $\frac{2\tilde{A}+\tilde{B}\tilde{C}}{\ell^{\tilde{c}}} + k_C\ell^m = \frac{2A+BC}{\ell^c} + 2k_2\ell^m$, since $k_C \equiv \delta(2 \nmid C) - \delta(2 \nmid \tilde{C}) \mod 2$. Then $e_0 = f_0 - k_C f_4 + k_1 f_5 + k_2 f_3 \in I$ and so $I + \mathcal{O}_{1728}\ell^m \subseteq I_1$.

Prove the result for ideals constructed from Part A. is much simpler. Using the same notation as above, note that $c = 0$, $b = n - a$ and we may replace C and $\tilde{C}$ with 0 by Proposition 1. The matrices representing $I + \mathcal{O}_{1728}$ and I_1 are then,

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 & \frac{\ell^m}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & \frac{\ell^m}{2} & 0 & 0 \\ \frac{B\ell^a}{2} & A & \ell^n & 0 & \frac{\ell^m}{2} & 0 & \ell^e & 0 \\ -A & \frac{B\ell^a}{2} & 0 & \ell^n & 0 & \frac{\ell^m}{2} & 0 & \ell^e \end{pmatrix} \text{ and } \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \frac{\tilde{B}\ell^{\tilde{a}}}{2} & \tilde{A} & \ell^m & 0 \\ -\tilde{A} & \frac{\tilde{B}\ell^{\tilde{a}}}{2} & 0 & \ell^m \end{pmatrix}.$$

The inclusion is easy to see from checking $\tilde{a} = \min(a, m)$, $A \equiv \tilde{A} \mod \ell^m$ and $B\ell^a \equiv \tilde{B}\ell^{\tilde{a}} \mod \ell^m$.

7 Application to Successive Minima of $\mathbb{F}_p$ curves

In this section we will apply our structural results to prove Proposition 3. This is not an entirely new result. It was originally noted during a workshop brainstorming session[2], with the suggestion it could be proven from the results of [11]. To demonstrate the applicability of our structural results however, we give our own proof with the main new insight being the proof of Lemma 27.

Proposition 3. *Fix a prime $p \equiv 3 \mod 4$ and let $\mathcal{O} \subseteq B_{p,\infty}$ be a maximal quaternion order for which there is a primitive embedding of $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, then the third successive minima of the Gross lattice $\mathcal{O}^T$ is exactly p, where $\mathcal{O}^T = \{2x - \mathrm{Tr}(x) : x \in \mathcal{O}\}$.*

We prove it in three steps. The first step is to show such an order $\mathcal{O}$ is isomorphic to an order to which we can apply our structural results. This mainly comes down to considering the behaviour of a certain group action. See Appendix A for prerequisite results.

Lemma 25. *For $p \equiv 3 \mod 4$ and a maximal quaternion order $\mathcal{O} \subset B_{p,\infty}$, with a primitive embedding of $\mathfrak{O} = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, and $\mathcal{O} \ncong \mathcal{O}_{1728}$, there exists an isomorphic quaternion order $\mathcal{O}' \cong \mathcal{O}$ which is the right order of cyclic (integral) left $\mathcal{O}_{1728}$-ideal of odd prime norm ℓ, with $\frac{1+j}{2} \in \mathcal{O}'$.*

Proof. Let E be an $\mathbb{F}_p$-rational supersingular elliptic curve with endomorphism ring isomorphic to $\mathcal{O}$, which exists under the Deuring correspondence. We know E admits an $\mathfrak{O}$-orientation so we may consider the group action of $\mathrm{Cl}(\mathfrak{O})$ on the set of supersingular elliptic curves orientable by $\mathfrak{O}$. This is the group action used by the CSIDH key exchange [6], although we work with $\mathfrak{O}$-oriented curves instead of $\mathbb{Z}[\sqrt{-p}]$-oriented curves. Let E_{1728} be the $\mathbb{F}_p$-rational curve $y^2 = x^3 + x$ which is supersingular for $p \equiv 3 \mod 4$, with $\mathrm{End}(E_{1728}) \cong \mathcal{O}_{1728}$ (as defined earlier), and an $\mathfrak{O}$-orientation $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E_{1728})$ mapping 1 to $[1]$ and $\sqrt{-p}$ to the Frobenius endomorphism. As the group action is transitive (see [6, Theorem 7]) there exists an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ such that $E_{1728} * [\mathfrak{a}] = E' \cong E$. Moreover we can assume $N(\mathfrak{a}) = \ell$ is an odd prime, since every ideal class in $\mathrm{Cl}(\mathfrak{O})$ contains infinitely many ideals of prime norm (see Lemma 29). Precisely this means there is an isogeny $\varphi : E_{1728} \to E'$ with kernel $\cap_{x \in \mathfrak{a}} \ker(\iota(x))$ and $N(\mathfrak{a}) = \ell = \deg(\varphi)$. By Deuring correspondence there is a quaternion left $\mathcal{O}_{1728}$-ideal I corresponding to φ (see Lemma 30), with $N(I) = N(\mathfrak{a})$ and $\frac{1+j}{2} \in \mathcal{O}_{\mathrm{right}}(I)$. As $N(I)$ contains no square factors, I is cyclic. Taking $\mathcal{O}' = \mathcal{O}_{\mathrm{right}}(I)$ we have $\mathcal{O}' \cong \mathrm{End}(E') \cong \mathrm{End}(E) \cong \mathcal{O}$.

Now we use our structural results to show such an order $\mathcal{O}'$ admits a basis of a certain form. We use the following technical Lemma.

[2] From the Leuven Isogeny Days 5 workshop at K.U. Leuven (September 2024), with credit going to the organisers and a large group of participants.

Lemma 26. *Let p be prime, and $K = \mathbb{Q}(\sqrt{-p})$ with field norm $n(\cdot)$. Let L be a rank 2 $\mathbb{Z}$-lattice in K, where all non-zero elements of L have norm ≥ 2. Let* $\det(L)$ *denote the determinant of the basis matrix of L with respect to basis $1, \sqrt{-p}$ of K. Then there exists a basis b_1, b_2 of L with $n(b_i) \leq p \cdot \det(L)^2$ for $i = 1, 2$.*

Proof. Embed K into $\mathbb{C}$ by $\sqrt{-p} \mapsto \sqrt{p} \cdot i$, and then into $\mathbb{R}^2$ by $i \mapsto (0, 1)$, and observe the norm of an element in K equals the square of the Euclidean norm $|| \cdot ||$ of the element mapped into $\mathbb{R}^2$. Under this embedding L becomes a lattice $L' \subset \mathbb{R}^2$. Let λ_1, λ_2 be the successive minima of L' with respect to $|| \cdot ||$, so L has successive minima λ_1^2, λ_2^2. By Minkowski's second theorem (see [4, Chapter 8]) applied to L' with the unit ball in $\mathbb{R}^2$ we get $\lambda_1 \lambda_2 \leq \frac{4}{\pi} \det(L')$ where $\det(L')$ is the determinant of the matrix with columns as the basis of L'. Since λ_1^2 is the norm of the smallest non-zero element in L we have $\lambda_1^2 \geq 2 > \frac{16}{\pi^2} \approx 1.62$. Hence $\frac{16}{\pi^2}\lambda_2^2 < \lambda_1^2 \lambda_2^2 \leq \frac{16}{\pi^2} \det(L')^2$, so $\lambda_2^2 < \det(L')^2$. The result follows by definition of 2nd successive minima, and noting $\det(L') = \sqrt{p} \cdot \det(L)$.

Lemma 27. *Let $\mathcal{O}$ be a maximal quaternion order which is the right order of a cyclic left $\mathcal{O}_{1728}$-ideal of prime norm ℓ, with $\frac{1+j}{2} \in \mathcal{O}$. Suppose $\mathcal{O} \ncong \mathcal{O}_{1728}$. Then $\mathcal{O}$ admits a basis of the form $e_0, e_1, e_2, e_3 \in B_{p,\infty}$ with $e_0 = 1, e_1 = \frac{1+j}{2}$ and $e_2, e_3 \in \mathbb{Q}i + \mathbb{Q}k$ with* $\operatorname{nrd}(e_2), \operatorname{nrd}(e_3) \leq \frac{p}{4}$.

Proof. We know $\mathcal{O}$ is of the form given in Theorem 1 with $n = 1$. We also know $\frac{1+j}{2} \in \mathcal{O}$, which is only possible if it is a linear combination of the basis vectors, i.e. there exists $x_i \in \mathbb{Z}$ such that,

$$\begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{\ell^a}{2} \\ \frac{C+\delta(2\nmid C)\cdot \ell^{b+c}}{2\ell^c} \end{pmatrix} + x_1 \begin{pmatrix} 0 \\ 0 \\ \ell^a \\ \frac{C}{\ell^c} \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ \ell^b \end{pmatrix}.$$

From the conditions on a we have $a = -1, 0$ or 1, which from the 3rd row gives $\frac{1}{2} = \frac{1}{2\ell} + \frac{x_1}{\ell}$, or $\frac{1}{2} = \frac{1}{2} + x_1$ or $\frac{1}{2} = \frac{\ell}{2} + x_1 \ell$ respectively. Clearly the last of these is impossible.

Consider the first case of $a = -1$, so $b = 1$ and $c = 1$. Then the above relation becomes $\ell = 1 + 2x_1$ so $x_1 = \frac{\ell - 1}{2}$. Then in the 4th entry we get $0 = \frac{C+\delta(2\nmid C)\cdot\ell^2}{2\ell} + \frac{C(\ell-1)}{2\ell} + x_2 \ell$ so $0 = \delta(2 \nmid C) \cdot \ell^2 + C\ell + x_2 2\ell^2$. This gives $C\ell \equiv 0 \mod \ell^2$ so $\ell \mid C$. This is impossible as the last condition in the theorem of $\ell^{2c} = \ell^2 \mid 1 + C^2$ cannot be satisfied.

Hence we must have $a = 0$ as it is the only possible case. It then follows that $b = 1$ and $c = 0$. Also by the relation above we have $x_1 = 0$ and so from the 4th row obtain $C + \delta(2 \nmid C)\ell + x_2 2\ell = 0$ hence $C \equiv 0 \mod \ell$. From the bounds on C we have $0 \leq C < \ell$ so clearly $C = 0$. Finally considering the relation $2A + BC \equiv 0 \mod \ell^{b+c}$ we have $2A \equiv 0 \mod \ell$ and from the bounds on A we have $0 \leq A < \ell$ so also have $A = 0$. Substituting these values into the basis matrix and conditions of Theorem 1 tells us that $\mathcal{O}$ admits a basis in the matrix form,

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\ell} & 0 & 0 \\ \frac{1}{2} & 0 & 1 & 0 \\ 0 & \frac{B}{2\ell} & 0 & \ell \end{pmatrix}.$$

where $0 \leq B < 2\ell^2$ is an odd solution to $B^2 \cdot p \equiv -1 \mod 2\ell^2$.

Applying unimodular column operations $c_3 \mapsto c_3 - 2c_1$ and $c_3 \mapsto -c_3$, then reordering the columns and we get a basis matrix,

$$\begin{pmatrix} 1 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2\ell} & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{B}{2\ell} & \ell \end{pmatrix}.$$

This is almost the basis claimed, however we must minimize the norms of the last two columns. To that end, we find a short basis of the 2-dimensional quadratic lattice L with basis matrix,

$$\begin{pmatrix} \frac{1}{2\ell} & 0 \\ \frac{B}{2\ell} & \ell \end{pmatrix}, \qquad \text{with respect to the norm} \qquad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x^2 + py^2.$$

As the 2D basis reduction can be expressed as a 2×2 unimodular matrix, it's easy to check one may reconstruct a basis of $\mathcal{O}$ from,

$$\text{basis matrix } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ of } L \quad \longmapsto \quad \text{basis matrix } \begin{pmatrix} 1 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & a & b \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & c & d \end{pmatrix} \text{ of } \mathcal{O},$$

since the change of the $\mathcal{O}$ basis can be expressed as a 4×4 unimodular matrix. Note this 2-dimensional lattice L may be viewed as lying within the quadratic field $K = \mathbb{Q}(\sqrt{-p})$. Also observe $\det(L) = \frac{1}{2\ell} \cdot \ell - 0 \cdot \frac{B}{2\ell} = \frac{1}{2}$ and the norms of all elements in $L \subset K$ are integral as it embeds into $\mathcal{O}$ which consists of algebraic integers. Hence if no elements in L have norm 1, we are done by Lemma 26. This can be seen by instead supposing there exists $\alpha \in \mathcal{O}$ of trace zero and norm 1, then one may show an embedding of $\mathcal{O}_{1728} \hookrightarrow \mathcal{O}$ exists by taking $\frac{1+j}{2} \mapsto \frac{1+j}{2}$ and $i \mapsto \alpha$, which since $\mathcal{O}_{1728}$ is maximal, is an isomorphism. This is a contradiction under the assumption $\mathcal{O} \not\cong \mathcal{O}_{1728}$.

And finally we show an order with a basis in this form must satisfy the successive minima claim.

Lemma 28. *Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal quaternion order. Suppose $\mathcal{O}$ has a basis $e_0, e_1, e_2, e_3 \in B_{p,\infty}$ with $e_0 = 1, e_1 = \frac{1+j}{2}$ and $e_2, e_3 \in \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}k$ with* $\mathrm{nrd}(e_2), \mathrm{nrd}(e_3) \leq \frac{p}{4}$. *Then the 3rd successive minima of $\mathcal{O}^T$, denoted λ_3, is exactly p.*

Proof. Since e_0, e_1, e_2, e_3 linearly span $\mathcal{O}$ we know $\{2e_r - \mathrm{Tr}(e_r) : r = 0, ..., 3\}$ linearly span $\mathcal{O}^T$. For $r = 0$ note that $2e_0 - \mathrm{Tr}(e_0) = 0$ so we may exclude it, which means $\{2e_r - \mathrm{Tr}(e_r) : r = 1, 2, 3\}$ span $\mathcal{O}^T$, which implies they have rank 3. Then by definition we have $\lambda_3 \leq \max(\{\mathrm{nrd}(2e_r - \mathrm{Tr}(e_r)) : r = 1, 2, 3\})$. For $r = 1$ this norm is exactly p. For $r = 2, 3$ we get the upper bound $\mathrm{nrd}(2e_r - \mathrm{Tr}(e_r)) \leq \mathrm{nrd}(2e_r) = 4\,\mathrm{nrd}(e_r) \leq 4 \cdot \frac{p}{4} = p$. Therefore $\lambda_3 \leq p$.

For equality, the set $\{2e_r - \mathrm{Tr}(e_r) : r = 1, 2, 3\}$ doesn't just span a sublattice of $\mathcal{O}^T$, but spans all of $\mathcal{O}^T$, so is a basis of it. Write $e_i = \frac{\mathrm{Tr}(e_i)}{2} + e_{i1}i + e_{i2}k$ for $i = 2, 3$ The norm form of $\mathcal{O}^T$ with respect to this basis is then,

$$(x_1, x_2, x_3) \mapsto \mathrm{nrd}(x_1 j + x_2(2e_{21}i + 2e_{22}k) + x_3(2e_{31}i + 2e_{32}k)).$$

By collecting the terms with coefficients of $1, i, j, k$ then using the usual formula for reduced norm, this can be written as,

$$(x_1, x_2, x_3) \mapsto (2x_2e_{21} + 2x_3e_{31})^2 + px_1^2 + p(2x_2e_{22} + 2x_3e_{32})^2,$$

which is clearly positive definite. Now consider the contributions of the term px_1^2. If the form represents an element of norm strictly less than p, we must have $x_1 = 0$ as otherwise the term px_1^2 contributes too much. Therefore all elements in the Gross lattice with norm less than p are contained in the rank 2 sublattice $(2e_{21}i + 2e_{22}k)\mathbb{Z} + (2e_{31}i + 2e_{32}k)\mathbb{Z}$. Hence supposing if $\lambda_3 < p$, the set $\{v \in \mathcal{O}^T : n(v) \leq \lambda_3\}$ is a subset of this sublattice so has rank 2, which contradicts the definition of λ_3.

We may then prove the proposition.

Proof of Proposition 3. Clearly isomorphic orders have the same successive minima, and successive minima of their Gross lattices. If $\mathcal{O} \cong \mathcal{O}_{1728}$ we are immediately done as the result holds for $\mathcal{O}_{1728}$. Instead suppose $\mathcal{O} \ncong \mathcal{O}_{1728}$. Invoke Lemma 25 to find an isomorphic order $\mathcal{O}'$, then apply Lemma 27 to $\mathcal{O}'$, giving a basis in the required form, then apply Lemma 28 to show the third successive minima of the Gross lattice of $\mathcal{O}'$ is p.

References

[1] Laia Amorós, James Clements, and Chloe Martindale. *Parametrizing Maximal Orders Along Supersingular ℓ-Isogeny Paths.* Cryptology ePrint Archive, Paper 2025/033. 2025. URL: https://eprint.iacr.org/2025/033.

[2] Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. "Explicit connections between supersingular isogeny graphs and Bruhat-Tits trees". In: *Women in numbers Europe III—research directions in number theory.* Vol. 24. Assoc. Women Math. Ser. Springer, Cham, 2021, pp. 39–73. ISBN: 978-3-030-77699-2; 978-3-030-77700-5. DOI: 10.1007/978-3-030-77700-5_2. URL: https://doi.org/10.1007/978-3-030-77700-5_2.

[3] Sarah Arpin, James Clements, Pierrick Dartois, Jonathan Komada Eriksen, Péter Kutas, and Benjamin Wesolowski. "Finding orientations of supersingular elliptic curves and quaternion orders". In: *Designs, Codes and Cryptography* (2024). ISSN: 1573-7586. DOI: `10.1007/s10623-024-01435-5`. URL: `https://doi.org/10.1007/s10623-024-01435-5`.

[4] John William Scott Cassels. *An introduction to the geometry of numbers*. Second. Springer Science & Business Media, 1997. ISBN: 978-3-540-61788-4. DOI: `10.1007/978-3-642-62035-5`. URL: `https://doi.org/10.1007/978-3-642-62035-5`.

[5] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, Apr. 2023, pp. 423–447. DOI: `10.1007/978-3-031-30589-4_15`.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology – ASIACRYPT 2018, Part III*. Vol. 11274. Lecture Notes in Computer Science. Brisbane, Queensland, Australia: Springer, Cham, Switzerland, Dec. 2018, pp. 395–427. DOI: `10.1007/978-3-030-03332-3_15`.

[7] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22.1 (Jan. 2009), pp. 93–113. DOI: `10.1007/s00145-007-9002-x`.

[8] David A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*. Third. With contributions by Roger Lipsett. AMS Chelsea Publishing, Providence, RI, 2022. ISBN: [9781470470289]; [9781470471835].

[9] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *Advances in Cryptology – ASIACRYPT 2020, Part I*. Vol. 12491. Lecture Notes in Computer Science. Daejeon, South Korea: Springer, Cham, Switzerland, Dec. 2020, pp. 64–93. DOI: `10.1007/978-3-030-64837-4_3`.

[10] Max Deuring. "Die typen der multiplikatorenringe elliptischer funktionenkörper". In: *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*. Vol. 14. 1. Springer. 1941, pp. 197–272.

[11] Tomoyoshi Ibukiyama. "On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings". In: *Nagoya Mathematical Journal* 88 (1982), pp. 181–195.

[12] David Jao and Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*. Tapei, Taiwan: Springer, Berlin, Heidelberg, Germany, Nov. 2011, pp. 19–34. DOI: `10.1007/978-3-642-25405-5_2`.

[13] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion ℓ-isogeny path problem". In: *LMS J. Comput. Math.* 17 (2014), pp. 418–432. ISSN: 1461-1570. DOI: 10.1112/S1461157014000151. URL: https://doi.org/10.1112/S1461157014000151.

[14] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, Apr. 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16.

[15] Damien Robert. "Breaking SIDH in Polynomial Time". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, Apr. 2023, pp. 472–503. DOI: 10.1007/978-3-031-30589-4_17.

[16] SageMath Developers. *SageMath, the Sage Mathematics Software System (Version 10.1)*. https://www.sagemath.org. 2024.

[17] John Voight. *Quaternion algebras*. Vol. 288. Graduate Texts in Mathematics. Springer, Cham, [2021] ©2021, pp. xxiii+885. ISBN: 978-3-030-56692-0; 978-3-030-56694-4. DOI: 10.1007/978-3-030-56694-4. URL: https://doi.org/10.1007/978-3-030-56694-4.

Appendix A Properties of $\mathbb{F}_p$ group action

We now prove some facts regarding the class group action used in Section 7.

Lemma 29. *Let $\mathfrak{O}$ be an order in an imaginary quadratic field K, and let I be an $\mathfrak{O}$-ideal with $N(I)$ coprime to $f = \operatorname{cond}(\mathfrak{O})$. Suppose no scalar factors divide I, i.e. $(q) \nmid I$ for all primes q. Then there exists infinitely many equivalent ideals $J \sim I$ of prime norm.*

Proof. If I is the unit ideal we are done, so assume $I \neq (1)$. Let $N = N(I)$ and write $I = \mathbb{Z}N + \mathbb{Z}\alpha$ with $N \mid n(\alpha)$. The norm form of I with respect to this basis is,

$$g : (x, y) \mapsto \frac{n(xN + y\alpha)}{N} = Nx^2 + t(\alpha)xy + \frac{n(\alpha)}{N}y^2$$

which has integral coefficients. The form is positive definite as the field norm n on K is positive definite. The form is primitive as otherwise $N \mid t(\alpha)$ and $N^2 \mid n(\alpha)$ which implies $\frac{\alpha}{N} \in \mathfrak{O}_K$ is a quadratic integer. This implies $\frac{f}{N}\alpha \in f \cdot \mathfrak{O}_K \subseteq \mathfrak{O}$ and multiplying by $f^{-1} \in \mathbb{Z}$ such that $f^{-1}f \equiv 1 \mod N$ gives $\frac{\alpha}{N} \in \mathfrak{O}$, which is a contradiction as I has no scalar factors. By [8, Chapter 2.9C], g represents infinitely many primes, so there are infinitely many $\beta = xN + y\alpha$ with $x, y \in \mathbb{Z}$ such that $n(\beta) = Nq$ for q prime. Moreover if $N \neq q$ then $N \nmid y$, so there are infinitely many β with $N \nmid y$. Clearly for $I' = \mathbb{Z}N + \mathbb{N}\beta$ we have $I = I'$, as $I' \subseteq I$ follows from $\beta \in I$, and $I \subseteq I'$ follows from $N\alpha \in I'$ as I' is an ideal, and $y\alpha = \beta - xN \in I'$, so $\alpha = \gcd(N, y)\alpha \in I'$. Setting $J = I'\frac{\overline{\beta}}{N} = \mathbb{Z}\overline{\beta} + \mathbb{Z}q$ we have $I \sim J$ and $N(J) = q$.

Take a prime $p \geq 5$ with $p \equiv 3 \mod 4$ and define $\mathfrak{O} = \mathbb{Z}[g]$ with $g = \frac{1+\sqrt{-p}}{2}$. The class group action from [6] of the order $\mathfrak{O}$ is defined as follows. Let $SS_{\mathfrak{O}}$ be the isomorphism classes of supersingular elliptic curves E over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathfrak{O}$. Fix isomorphism $\Phi : \mathfrak{O} \to \mathrm{End}_{\mathbb{F}_p}(E)$. Take $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ and assume $\mathfrak{a}$ has factors of $\mathfrak{p}$ removed, where $\mathfrak{p}$ is the ideal above p in $\mathfrak{O}$. Let φ be the separable isogeny from E with kernel $\bigcap_{x \in \mathfrak{a}} \ker(\Phi(x))$. Note for any $\mathbb{Z}$-basis $x_1, ..., x_n$ of $\mathfrak{a}$ this kernel is equal to $\bigcap_i \ker(\Phi(x_i))$. Let $E/\mathfrak{a}$ denote the codomain of φ. Then the map $* : SS_{\mathfrak{O}} \times \mathrm{Cl}(\mathfrak{O})$ defined by $E * \mathfrak{a} = E/\mathfrak{a}$ is well-defined and is a group action. Furthermore when $\mathfrak{a}$ contains no scalar factors we have $\deg(\varphi) = N(\mathfrak{a})$.

Lemma 30. *Following from above, fix a maximal quaternion order $\mathcal{O} \cong \mathrm{End}(E)$, elements i, j, k as the usual basis of $B_{p,\infty}$, and an isomorphism $\lambda : \mathcal{O} \to \mathrm{End}(E)$ taking $\sqrt{-p}$ to j. Suppose $\mathfrak{a}$ has no scalar factors and norm coprime to p. Then writing $\mathfrak{a} = \langle N(\mathfrak{a}), x \rangle_{\mathbb{Z}}$ for some $x \in \mathfrak{O}$,*

$$I = \mathcal{O} \cdot N(\mathfrak{a}) + \mathcal{O} \cdot \lambda^{-1}(\Phi(x)),$$

is a left quaternion $\mathcal{O}$-ideal which corresponds to φ under the Deuring correspondence. This means $N(I) = N(\mathfrak{a})$, $\mathrm{End}(E/\mathfrak{a}) \cong \mathcal{O}_{\mathrm{right}}(I)$, and we have $\lambda^{-1}(\Phi(g)) \in \mathcal{O}_{\mathrm{right}}(I)$.

Proof. By Deuring correspondence, the $\mathcal{O}$-ideal J corresponding to φ is,

$$J = \lambda^{-1}(\{\theta \in \mathrm{End}(E) : \ker(\varphi) \subseteq \ker(\theta)\}).$$

Given $I = \mathcal{O} \cdot N(\mathfrak{a}) + \mathcal{O} \cdot \lambda^{-1}(\Phi(x))$, our aim is to show $I = J$. From the definition of φ we have $\ker(\varphi) = \ker([N(\mathfrak{a})]) \cap \ker(\Phi(x))$, so $\ker(\varphi) \subseteq \ker([N(\mathfrak{a})])$ and $\ker(\varphi) \subseteq \ker(\Phi(x))$. By pre-composing these maps by an endomorphism $\theta \in \mathcal{O}$, we only make the kernel larger, hence $\ker(\varphi) \subseteq \ker(\lambda(\theta) \circ [N(\mathfrak{a})])$ and $\ker(\varphi) \subseteq \ker(\lambda(\theta) \circ \Phi(x))$. This shows $\theta \cdot N(\mathfrak{a}) \in J$ and $\theta \cdot \lambda^{-1}(\Phi(x)) \in J$. Since θ was arbitrary, $\mathcal{O} \cdot N(\mathfrak{a}) \subseteq J$ and $\mathcal{O} \cdot \lambda^{-1}(\Phi(x)) \subseteq J$. As J is closed under addition $I \subseteq J$. It is then sufficient to show $N(I) = N(J)$, or more precisely that $N(I) \leq N(J)$. From the Deuring correspondence $N(J) = \deg(\varphi)$, and from the group action $\deg(\varphi) = N(\mathfrak{a})$, so $N(J) = N(\mathfrak{a})$. As $\mathfrak{a}$ contains no scalar factors, I is cyclic. It is a well known fact that for cyclic quaternion ideals I we have $I \cap \mathbb{Z} = N(I) \cdot \mathbb{Z}$. Then as $N(\mathfrak{a}) \in I$, we have $N(I) \leq N(\mathfrak{a})$.

Finally, to show $\lambda^{-1}(\Phi(g)) \in \mathcal{O}_{\mathrm{right}}(I)$, by definition of right order one must show $\mathcal{O} \cdot N(\mathfrak{a})\lambda^{-1}(\Phi(g)) + \mathcal{O} \cdot \lambda^{-1}(\Phi(x))\lambda^{-1}(\Phi(g)) \subset I$. This is trivial from linearity of λ^{-1} and Φ, commutativity of multiplication in $\mathfrak{O}$, and the closure of $\mathcal{O}$.