Geometry of Log-unit Lattices

Fernando Azpeitia Tellez and Christopher Powell [*][†]

Abstract

We address orthogonality of the log-unit lattice associated to real biquadratic number fields of the form $\mathbb{Q}\left(\sqrt{d_1}, \sqrt{d_2}\right)$, where d_1, d_2 are distinct primes. Based on data collected, we observed a pattern when (i) $d_1 = 2$ and $d_2 \equiv 3 \mod 4$; and (ii) $d_1 \equiv 1 \mod 4$ and $d_2 \not\equiv 3 \mod 4$ with exactly one fundamental unit of norm 1. For these cases, we prove that the associated log-unit lattice is orthogonal. Additionally, we provide a formula for the packing radius. In the case where both $d_1, d_2 \equiv 3 \mod 4$, we show that the log-unit lattice is not orthogonal. In all cases, we provide a formula for the co-volume, successive minima, and covering radius of the log-unit lattice.

1 Introduction

Fully homomorphic encryption (FHE) allows computations to be performed on a set of encrypted data such that the result of those computations, when decrypted, matches the result of operations performed on the corresponding set of unencrypted data. That is, given encryptions $E(p_1), \ldots, E(p_n)$ of plaintexts $p_1, \ldots, p_n$, one can compute a ciphertext of $\varphi(p_1, \ldots, p_n)$ for any polynomial function φ. Such an encryption scheme would be of immense utility in the world of IT security as it would allow the confidentiality of data to be preserved while being processed in untrusted computing environments. For example, FHE would allow cloud-based computing resources, such as online search engines, to be used without compromising user-privacy.

A practical FHE scheme has eluded cryptographers since 2009 when Craig Gentry, in [1], first demonstrated that such a cryptosystem could be realized in principle. Typical FHE cryptosystems are based on lattices, specifically *log-unit lattices* associated to number fields. The geometry of these lattices is crucial to the implementation of the associated cryptosystems. If the geometry of these lattices is too irregular, the resulting encryption and decryption algorithms either become too slow or fail to work altogether. Conversely, if the geometry is too well-behaved, the resulting algorithms fail to produce strong encryption. At present, the geometry of these lattices is not well-understood.

The goal of this project is to examine the geometry of log-unit lattices for special families of number fields. We prove that for every real biquadratic number field of the form $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, where d is prime and congruent to $3 \mod 4$, the associated log-unit lattice is orthogonal.

[*] Partially supported by NSF-DMS 1247679 grant, PUMP: Preparing Undergraduates through Mentoring towards PhDs.

[†] We would like to thank Dr. Shahed Sharif, our faculty advisor at California State University, San Marcos, for his tremendous patience in guiding us over the past year. This research would not have been possible without the time and knowledge he shared with us.

2 Background

Much of the mathematical background necessary for this research comes from the study of lattices and algebraic number theory. We begin by considering some preliminary definitions and results.

2.1 Lattices

Definition 1. A *lattice* $\mathcal{L}(b_1, \ldots, b_m)$ is a subgroup of $\mathbb{R}^n$ of the form

$$\mathcal{L}(b_1, \ldots, b_m) = \sum_{i=1}^{m} \mathbb{Z} b_i,$$

where $b_1, \ldots, b_m \in \mathbb{R}^n$ are linearly independent. The set $B = \{b_1, \ldots, b_m\}$ is called a *basis* for $\mathcal{L}$ and

$$\operatorname{span}(\mathcal{L}(B)) = \operatorname{span}(B) = \left\{ \sum_{i=1}^{m} x_i b_i \mid x_i \in \mathbb{R} \right\}.$$

Furthermore, the lattice is said to be *complete* or *full-rank* if $m = n$.

Definition 2. The *fundamental mesh* of $\mathcal{L}(B)$ is defined to be

$$\Phi(B) = \left\{ \sum\nolimits_{i=1}^{m} x_i b_i \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1 \right\}.$$

Geometrically, $\Phi(B)$ is a parallelepiped. The *volume* of $\Phi(B)$ is equal to the absolute value of the determinant of the matrix whose columns are given by b_i. [5].

Definition 3. Assume $\mathcal{L}(b_1, \ldots, b_m)$ is a lattice. If $\mathcal{L}$ is full-rank then *co-volume* of $\mathcal{L}(b_1, \ldots, b_m)$ is given by

$$\left| \det \left[b_1 \mid b_2 \mid \cdots \mid b_m \right] \right|.$$

Otherwise

$$\sqrt{\left| \det \left(\left[b_1 \mid b_2 \mid \cdots \mid b_m \right]^T \left[b_1 \mid b_2 \mid \cdots \mid b_m \right] \right) \right|}.$$

We denote the co-volume of $\mathcal{L}(b_1, \ldots, b_m)$ by $\operatorname{covol}(\mathcal{L}(b_1, \ldots, b_m))$.

Proposition 1. *Let $\mathcal{L}$ be a full-rank lattice in $\mathbb{R}^n$. Then $\operatorname{covol}(\mathcal{L})$ is independent of the choice of basis generating $\mathcal{L}$.*

Proof. Let $B = \{v_1, \ldots, v_n\}$ and $B' = \{w_1, \ldots, w_n\}$ be bases for $\mathcal{L}$. Then $w_1, \ldots, w_n \in \mathcal{L} = \sum_{i=1}^{n} \mathbb{Z} v_i$ which implies that

$$\begin{aligned} w_1 &= a_{11} v_1 + \ldots + a_{1n} v_n \\ &\vdots \\ w_n &= a_{n1} v_1 + \ldots + a_{nn} v_n \end{aligned}$$

where each $a_{ij} \in \mathbb{Z}$. This system corresponds to the matrix equation

$$\left[w_1 \ldots w_n \right] = \left[v_1 \ldots v_n \right] \cdot \left[a_{ij} \right]^T, \quad i, j \in \{1, \ldots, n\}. \tag{1}$$

Similarly, $v_1, \ldots, v_n \in \mathcal{L} = \sum_{i=1}^{n} \mathbb{Z}w_i$ implies that

$$\begin{aligned} v_1 &= b_{11}w_1 + \ldots + b_{1n}w_n \\ &\vdots \\ v_n &= b_{n1}w_1 + \ldots + b_{nn}w_n \end{aligned}$$

where each $b_{ij} \in \mathbb{Z}$. This system corresponds to the matrix equation

$$\begin{bmatrix} v_1 \ldots v_n \end{bmatrix} = \begin{bmatrix} w_1 \ldots w_n \end{bmatrix} \begin{bmatrix} b_{ij} \end{bmatrix}^T, \quad i, j \in \{1, \ldots, n\}. \tag{2}$$

By substituting (1) into (2), we obtain

$$\begin{bmatrix} v_1 \ldots v_n \end{bmatrix} = \left(\begin{bmatrix} v_1 \ldots v_n \end{bmatrix} \begin{bmatrix} a_{ij} \end{bmatrix}^T \right) \begin{bmatrix} b_{ij} \end{bmatrix}^T$$

which implies

$$\begin{bmatrix} a_{ij} \end{bmatrix}^T \begin{bmatrix} b_{ij} \end{bmatrix}^T = I.$$

This shows that these matrices are inverses of each other. Also, since their entries are integers, their determinants must be integers. But $\det(I) = 1$, so

$$\det \begin{bmatrix} a_{ij} \end{bmatrix}^T = \pm 1.$$

Hence, $\det \begin{bmatrix} v_1 \ldots v_n \end{bmatrix} = \pm \det \begin{bmatrix} w_1 \ldots w_n \end{bmatrix}$. By taking the absolute value of both sides we conclude that $\operatorname{covol}(\mathcal{L}(B)) = \operatorname{covol}(\mathcal{L}(B'))$. □

Definition 4. A lattice is *orthogonal* if there exists an orthogonal basis.

Proposition 2. *Let $\mathcal{L}(B)$ be a lattice with orthogonal basis $B = \{b_1, \ldots, b_m\}$. Then*

$$\operatorname{covol}(\mathcal{L}(B)) = \prod_{i=1}^{m} \|b_i\|.$$

Proof. Since B is orthogonal, $\Phi(B)$ is a hyperrectangle so

$$\operatorname{covol}(\mathcal{L}(B)) = \operatorname{volume}(\Phi(B)) = \prod_{i=1}^{m} \|b_i\|.$$

□

Definition 5. Let $\mathcal{L}(B)$ be a rank m lattice with basis B. Then for each $i \in \{1, \ldots, m\}$,

$$\lambda_i(\mathcal{L}) = \min\{r \mid \dim\left(\operatorname{span}(B) \cap \overline{\mathcal{B}}_r(0)\right) \geq i\},$$

where $\overline{\mathcal{B}}_r(0) = \{v \in \mathbb{R}^n \mid \|v\| \leq r\}$.

Proposition 3. *Let $\mathcal{L}(B)$ be a lattice with orthogonal basis $B = \{b_1, \ldots, b_m\}$ satisfying $\|b_i\| \leq \|b_{i+1}\|$, $i \in \{1, \ldots, m-1\}$. Then for each $i \in \{1, \ldots, m\}$, $\lambda_i(\mathcal{L}) = \|b_i\|$.*

Proof. For $i = 1$, suppose otherwise that there exists $v \in \mathcal{L}(B) \setminus \{0\}$ such that $\|v\| < \|b_1\|$. Then $v = \sum_{i=1}^{m} a_i b_i$, for some $a_i \in \mathbb{Z}$. So

$$\|v\|^2 = \langle v, v \rangle = \left\langle \sum_{i=1}^{m} a_i b_i, \sum_{i=1}^{m} a_i b_i \right\rangle .$$

Since B is orthogonal, we know $\langle b_i, b_j \rangle = 0$ for all $i \neq j$, so

$$\left\langle \sum_{i=1}^{m} a_i b_i, \sum_{i=1}^{m} a_i b_i \right\rangle = \sum_{i=1}^{m} a_i^2 \langle b_i, b_i \rangle .$$

Also, since $v \neq 0$, we know $a_i \neq 0$ for some $i \in \{1, \ldots, m\}$. Hence

$$\sum_{i=1}^{m} a_i^2 \langle b_i, b_i \rangle > \langle b_1, b_1 \rangle = \|b_1\|^2 .$$

But this contradicts our assumption that $\|v\| < \|b_1\|$. We now claim that for all $k \in \{1, \ldots, m-1\}$ and $v \in \mathcal{L}(B) \setminus \text{span}(b_1, \ldots, b_k)$, either $\|v\| \leq \|b_k\|$ or $\|v\| \geq \|b_{k+1}\|$. Suppose to the contrary that there is some $k \in \{1, \ldots, m-1\}$ and $v \in \mathcal{L}(B) \setminus \text{span}(b_1, \ldots, b_k)$ for which $\|b_k\| < \|v\| < \|b_{k+1}\|$. Then $v = \sum_{i=1}^{m} a_i b_i$ for some $a_i \in \mathbb{Z}$. So

$$\|v\|^2 = \sum_{i=1}^{m} a_i^2 \langle b_i, b_i \rangle .$$

Since $v \notin \text{span}(b_1, \ldots, b_k)$, we know $a_j \neq 0$ for some $j \in \{k+1, \ldots, m\}$. Thus

$$\sum_{i=1}^{m} a_i^2 \langle b_i, b_i \rangle \geq a_j^2 \|b_j\|^2 \geq \|b_j\|^2 \geq \|b_{k+1}\|^2 .$$

So we get $\|v\|^2 \geq \|b_{k+1}\|^2$, a contradiction. Thus we can find no $k \in \{1, \ldots, m-1\}$ and $v \in \mathcal{L}(B) \setminus \text{span}(b_1, \ldots, b_k)$ which satisfies $\|b_k\| < \|v\| < \|b_{k+1}\|$, as claimed. Now recall that B is a basis for $\mathcal{L}$, so $b_k \notin \text{span}(b_1, \ldots, b_{k-1})$ for all $k \in \{1, \ldots, m\}$. Note that $\|b_i\| = \|-b_i\|$. Thus $\dim\big(\text{span}(B) \cap \overline{B}_r(0)\big) \leq k$ if $r < \|b_{k+1}\|$, and $\dim\big(\text{span}(B) \cap \overline{B}_r(0)\big) \geq k+1$ if $r = \|b_{k+1}\|$. Hence $\lambda_i = \|b_i\|$ for all i.

□

Definition 6. Let $\mathcal{L}(B)$ be a lattice with basis B. Then the *packing radius* $\psi(\mathcal{L})$ is defined to be

$$\psi(\mathcal{L}) = \max\{r \mid \mathcal{B}_r(v) \cap \mathcal{B}_r(w) = \emptyset \ \forall v, w \in \mathcal{L}, v \neq w\}$$

where $\mathcal{B}_r(v) = \{x \in \mathbb{R}^n \mid \|x - v\| < r\}$.

Definition 7. Let $\mathcal{L}(B)$ be a lattice with basis B. Let $y \in \mathbb{R}^n$. Define

$$\|y - \mathcal{L}(B)\| = \min_{b \in \mathcal{L}(B)} \|y - b\| .$$

Then the *covering radius* $\rho(\mathcal{L})$ is given by

$$\rho(\mathcal{L}) = \max_{x \in \text{span}(B)} \|x - \mathcal{L}(B)\| .$$

Remark. A point $x \in \operatorname{span}(B)$ is called a *deep hole* if $\|x - \mathcal{L}(B)\| = \rho(\mathcal{L})$.

Definition 8. Define $\lfloor \rceil : \mathbb{R} \to \mathbb{Z}$ by

$$\lfloor x \rceil = \begin{cases} \lceil x \rceil & \text{if } \lceil x \rceil - x \leq \frac{1}{2} \\ \lfloor x \rfloor & \text{if } \lceil x \rceil - x > \frac{1}{2}. \end{cases}$$

Lemma 1. Suppose $\mathcal{L}(B)$ is a lattice with orthogonal basis $B = \{b_1, \dots, b_m\}$. Let $x = \sum_{i=1}^m a_i b_i \in \operatorname{span}(B)$. Then

$$\|x - \mathcal{L}(B)\|^2 = \sum_{i=1}^m (a_i - \lfloor a_i \rceil)^2 \|b_i\|^2 .$$

Proof. Let $v, w \in \mathcal{L}(B)$ be such that $\|x - v\| \leq \|x - w\|$. We know $w = \sum_{i=1}^m c_i b_i$ for some $c_i \in \mathbb{Z}$. Consider $v = \sum_{i=1}^m \lfloor a_i \rceil b_i$. Recall that B is orthogonal, so $\langle b_i, b_j \rangle = 0$ for all $i \neq j$. Then

$$\|x - v\|^2 = \sum_{i=1}^m (a_i - \lfloor a_i \rceil)^2 \|b_i\|^2 \quad \text{and} \quad \|x - w\|^2 = \sum_{i=1}^m (a_i - c_i)^2 \|b_i\|^2 .$$

We claim that $(a_i - \lfloor a_i \rceil)^2 \leq (a_i - c_i)^2$ for all $i \in \{1, \dots, m\}$. Suppose otherwise, i.e., $(a_i - c_i)^2 < (a_i - \lfloor a_i \rceil)^2$. Note that $-\frac{1}{2} \leq a_i - \lfloor a_i \rceil < \frac{1}{2}$. So $(a_i - \lfloor a_i \rceil)^2 \leq \frac{1}{4}$. This implies that $(a_i - c_i)^2 < \frac{1}{4}$. In other words, $-\frac{1}{2} < a_i - c_i < \frac{1}{2}$. Since $c_i \in \mathbb{Z}$, it follows that $c_i = \lfloor a_i \rceil$. But this implies $(a_i - \lfloor a_i \rceil)^2 = (a_i - c_i)^2$, a contradiction. Thus $(a_i - \lfloor a_i \rceil)^2 \leq (a_i - c_i)^2$ for every i, as claimed. The result follows. □

Proposition 4. *Suppose $\mathcal{L}(B)$ is a lattice with orthogonal basis $B = \{b_1, \dots, b_m\}$. Then the center $c = \frac{1}{2}\sum_{i=1}^m b_i$ of $\Phi(B)$ is a deep hole.*

Proof. Let $x \in \operatorname{span}(B)$. So $x = \sum_{i=1}^m a_i b_i$ for some $a_i \in \mathbb{R}$. Then, by Lemma 1,

$$\|x - \mathcal{L}(B)\|^2 = \sum_{i=1}^m (a_i - \lfloor a_i \rceil)^2 \|b_i\|^2 .$$

Note that $\lfloor a_i \rfloor \leq a_i < \lfloor a_i \rfloor + \frac{1}{2}$ and $\lceil a_i \rceil - \frac{1}{2} \leq a_i < \lceil a_i \rceil$, so $(a_i - \lfloor a_i \rceil)^2 \leq \frac{1}{4}$. Hence

$$\sum_{i=1}^m (a_i - \lfloor a_i \rceil)^2 \|b_i\|^2 \leq \sum_{i=1}^m \tfrac{1}{4} \|b_i\|^2 .$$

Recall that B is orthogonal, so $\langle b_i, b_j \rangle = 0$ for all $i \neq j$. Thus

$$\sum_{i=1}^m \tfrac{1}{4} \|b_i\|^2 = \tfrac{1}{4} \sum_{i=1}^m \langle b_i, b_i \rangle = \tfrac{1}{4} \left\langle \sum_{i=1}^m b_i, \sum_{i=1}^m b_i \right\rangle = \|c\|^2 .$$

Therefore $\|c\| = \max\limits_{x \in \operatorname{span}(B)} \|x - \mathcal{L}(B)\|$. But since c is the center of $\Phi(B)$ and B is orthogonal, Lemma 1 implies

$$\|c - \mathcal{L}(B)\|^2 = \sum_{i=1}^m (\tfrac{1}{2} - a_i)^2 \|b_i\|^2 ,$$

where either $a_i = 0$ or $a_i = 1$. So $(\frac{1}{2} - a_i) = \pm\frac{1}{2}$. Thus

$$\sum_{i=1}^{m} (\tfrac{1}{2} - a_i)^2 \left\| b_i \right\|^2 = \sum_{i=1}^{m} \tfrac{1}{4} \left\| b_i \right\|^2 .$$

Thus $\|c\| = \|c - \mathcal{L}(B)\|$. Hence c is a deep hole. □

Corollary 2.1. *If a lattice $\mathcal{L}$ is orthogonal, then $\rho(\mathcal{L}) = \frac{1}{2}\sqrt{\sum_{i=1}^{m} \lambda_i(\mathcal{L})^2}$.*

Proof. Assume $\mathcal{L}$ is orthogonal. Let $B = \{b_1, \ldots, b_m\}$ be an orthogonal basis for $\mathcal{L}$ with $\|b_i\| \leq \|b_{i+1}\|$. Then $\Phi(B)$ is a hyperrectangle, so by Proposition 4 the center $c = \frac{1}{2}\sum_{i=1}^{m} b_i$ of $\Phi(B)$ is a deep hole. Hence $\rho(\mathcal{L}) = \|c\|$. Observe that

$$\|c\|^2 = \langle c, c\rangle = \left\langle \tfrac{1}{2}\sum_{i=1}^{m} b_i, \tfrac{1}{2}\sum_{i=1}^{m} b_i \right\rangle = (\tfrac{1}{4}) \left\langle \sum_{i=1}^{m} b_i, \sum_{i=1}^{m} b_i \right\rangle .$$

Since B is orthogonal, we know $\langle b_i, b_j\rangle = 0$ for all $i \neq j$. So

$$(\tfrac{1}{4}) \left\langle \sum_{i=1}^{m} b_i, \sum_{i=1}^{m} b_i \right\rangle = (\tfrac{1}{4}) \sum_{i=1}^{m} \langle b_i, b_i\rangle = (\tfrac{1}{4}) \sum_{i=1}^{m} \left\| b_i \right\|^2 .$$

Then, by Proposition 3,

$$(\tfrac{1}{4}) \sum_{i=1}^{m} \left\| b_i \right\|^2 = (\tfrac{1}{4}) \sum_{i=1}^{m} \lambda_i(\mathcal{L})^2.$$

□

2.2 Number Fields

Definition 9. A *number field* K is a field extension of $\mathbb{Q}$ of finite degree. That is, $\mathbb{Q}$ is a subfield of K where K has finite dimension when considered as a vector space over $\mathbb{Q}$.

Theorem 2.2 (Theorem 4.1.8 in [2])**.** *Let K be a number field of degree n. Then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.*

Definition 10. An element $\alpha \in K$ is *integral* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Example 1. For $K = \mathbb{Q}(\sqrt{2})$, we consider $f(x) = x^2 - 2$, and observe that $f(\sqrt{2}) = 0$. Thus, $\sqrt{2}$ is integral.

Theorem 2.3 (Theorem 2.1 in [3])**.** *The set of integral elements of K forms a ring.*

Definition 11. The integral elements of K is known as the *ring of integers*, denoted $\mathcal{O}_K$. We write $\mathcal{O}_K^\times$ for the set of invertible elements in $\mathcal{O}_K$.

Example 2. A well-known example is the Gaussian integers, the ring of integers in $\mathbb{Q}(i)$, i.e,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Proposition 5. *The set $\mathcal{O}_K^\times$ forms a multiplicative group.*

Proposition 6 (Proposition 9 in [4])**.** *Let K be a number field, and let $\alpha \in K$. Then there exists a unique irreducible monic polynomial $f \in \mathbb{Q}(x)$ of smallest degree such that $f(\alpha) = 0$.*

The polynomial f in the above is known as the *minimal polynomial* of α over $\mathbb{Q}$.

Theorem 2.4 (Theorem 4.1.3 in [2])**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. Then there are exactly n distinct homomorphisms $\sigma : K \hookrightarrow \mathbb{C}$ and each $\sigma(\alpha)$ is a root of the minimal polynomial of α over $\mathbb{Q}$.*

Definition 12. Assume K is a number field of degree n, and let $\sigma : K \hookrightarrow \mathbb{C}$ be a homomorphism. If $\sigma(K) \subseteq \mathbb{R}$, then we say that σ is a *real embedding*; otherwise, we say that σ is a *complex embedding.*

Remark. Note that the complex conjugate of a homomorphism is also a homomorphism, so complex embeddings come in pairs $\{\sigma, \overline{\sigma}\}$.

Definition 13. Suppose K is a number field of degree n with r real embeddings and s pairs of complex embeddings. Then $n = r + 2s$ and we define the *signature* of K to be (r, s).

Definition 14. Suppose K is a number field with signature (r, s). Let $\mu(K)$ be the roots of unity which lie in K. Assume $\mathcal{O}_K^\times/\mu(K) = \langle \varepsilon_1, \ldots, \varepsilon_{r+s-1} \rangle$. Define $b_{ij} = \ln |\varepsilon_i|_j$ and let the matrix $A \in \mathbb{R}^{r\times(r-1)}$ be given by

$$A = \begin{bmatrix} b_{11} & b_{21} & \dots & b_{(r-1)1} \\ b_{12} & b_{22} & \dots & b_{(r-1)2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1r} & b_{2r} & \dots & b_{(r-1)r} \end{bmatrix}.$$

Let $A_i \in \mathbb{R}^{(r-1)\times(r-1)}$ be the matrix obtained by deleting the i^{th}-row from A, $1 \leq i \leq r$. Then the *regulator* R of K is defined to be

$$R = |\det(A_i)|.$$

Example 3. For $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, the minimal polynomial $f(x) = x^3 - 2$ has both real and complex roots, namely,

$$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2},$$

where $\omega = e^{\frac{2\pi i}{3}}$. So, by Theorem 2.4, there are three embeddings $K \hookrightarrow \mathbb{C}$ given by

$$\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \sigma_2(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \quad \sigma_3(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}.$$

Note that σ_1 is real, whereas σ_2 and $\overline{\sigma_2} = \sigma_3$ are complex conjugates; hence, the signature of $\mathbb{Q}(\sqrt[3]{2})$ is $(1, 1)$.

Definition 15. Let K be a number field of degree n. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K into $\mathbb{C}$, and let $\sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+1}, \ldots, \overline{\sigma}_{r+s}$ be the conjugate pairs of complex embeddings. Then the *logarithmic embedding* is the map $\mathrm{Log} : K^\times \to \mathbb{R}^{r+s}$ defined by

$$\mathrm{Log}(x) = (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_r(x)|, 2\ln|\sigma_{r+1}(x)|, \ldots, 2\ln|\sigma_{r+s}(x)|).$$

Proposition 7. *Let K be a number field with signature (r, s). Then the logarithmic embedding* Log *is a homomorphism from the multiplicative group $K^\times$ to the additive group $\mathbb{R}^{r+s}$.*

Proof. Let $\alpha, \beta \in K^\times$. Then

$$\begin{aligned}\operatorname{Log}(\alpha)+\operatorname{Log}(\beta) &= (\ln|\sigma_1(\alpha)|,\ldots,2\ln|\sigma_{r+s}(\alpha)|)+(\ln|\sigma_1(\beta)|,\ldots,2\ln|\sigma_{r+s}(\beta)|)\\ &= (\ln|\sigma_1(\alpha)|+\ln|\sigma_1(\beta)|,\ldots,2\ln|\sigma_{r+s}(\alpha)|+2\ln|\sigma_{r+s}(\beta)|)\\ &= (\ln|\sigma_1(\alpha)\sigma_1(\beta)|,\ldots,2\ln|\sigma_{r+s}(\alpha)\sigma_{r+s}(\beta)|)\\ &= (\ln|\sigma_1(\alpha\beta)|,\ldots,2\ln|\sigma_{r+s}(\alpha\beta)|)\\ &= \operatorname{Log}(\alpha\beta).\end{aligned}$$

□

Theorem 2.5 (*Dirichlet's Unit Theorem* [5]). *Let K be a number field with signature (r, s) and let $\mu(K)$ be the cyclic group consisting of the roots of unity which lie in K. Then the unit group $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \operatorname{Log}(\mathcal{O}_K^\times)$, where $\Lambda = \operatorname{Log}(\mathcal{O}_K^\times) \cong \mathbb{Z}^{r+s-1}$.*

In the proof of Dirichlet's Unit Theorem it is shown that Log embeds $\mathcal{O}_K^\times$ as a lattice in $\mathbb{R}^{r+s}$ with rank $r+s-1$. In fact, $\operatorname{Log}(\mathcal{O}_K^\times)$ is a full-rank lattice in the hyperplane $\sum v_i = 0$ of $\mathbb{R}^{r+s}$. The lattice Λ is called the *log-unit lattice* associated to K. We consider log-unit lattices associated to real biquadratic number fields.

Definition 16. Let K be a number field. Then K is a *real biquadratic number field* if

$$K = \mathbb{Q}\left(\sqrt{d_1},\sqrt{d_2}\right) = \left\{a + b\sqrt{d_1} + c\sqrt{d_2} + e\sqrt{d_1}\sqrt{d_2} \mid a, b, c, e \in \mathbb{Q}\right\}$$

where d_1 and d_2 are distinct square-free integers > 1.

Theorem 2.6. *Let $x \in K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. We have*

$$x = a + b\sqrt{d_1} + c\sqrt{d_2} + e\sqrt{d_1}\sqrt{d_2}$$

for some $a, b, c, e \in \mathbb{Q}$. Then there are four embeddings of K into $\mathbb{C}$ given by

$$\begin{aligned}\sigma_0(x) &= a + b\sqrt{d_1} + c\sqrt{d_2} + e\sqrt{d_1d_2},\\ \sigma_1(x) &= a + b\sqrt{d_1} - c\sqrt{d_2} - e\sqrt{d_1d_2},\\ \sigma_2(x) &= a - b\sqrt{d_1} + c\sqrt{d_2} - e\sqrt{d_1d_2},\\ \sigma_3(x) &= a - b\sqrt{d_1} - c\sqrt{d_2} + e\sqrt{d_1d_2}.\end{aligned}$$

Proof. Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and let x be as above. Then

$$\begin{aligned}\sigma(x) &= \sigma\left(a + b\sqrt{d_1} + c\sqrt{d_2} + e\sqrt{d_1d_2}\right)\\ &= \sigma(a) + \sigma\left(b\sqrt{d_1}\right) + \sigma\left(c\sqrt{d_2}\right) + \sigma\left(e\sqrt{d_1d_2}\right)\\ &= \sigma(a) + \sigma(b)\,\sigma\left(\sqrt{d_1}\right) + \sigma(c)\,\sigma\left(\sqrt{d_2}\right) + \sigma(e)\,\sigma\left(\sqrt{d_1}\right)\sigma\left(\sqrt{d_2}\right)\\ &= a + b\sigma\left(\sqrt{d_1}\right) + c\sigma\left(\sqrt{d_2}\right) + e\sigma\left(\sqrt{d_1}\right)\sigma\left(\sqrt{d_2}\right).\end{aligned}$$

By definition, an embedding is a homomorphism, so $\sigma\left(\sqrt{d_1}\right) = \pm\sqrt{d_1}$ and $\sigma\left(\sqrt{d_2}\right) = \pm\sqrt{d_2}$. Result follows by applying all possible combinations of $\pm\sqrt{d_1}$ and $\pm\sqrt{d_2}$. □

By Theorem 2.6, we get that a real biquadratic number field has signature $(4, 0)$. Thus, the rank of the associated log-unit lattice is $r + s - 1 = 3$.

Definition 17. Suppose $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d. Then the *discriminant* Δ of K is given by

$$\Delta(K) = \begin{cases} d & \text{if } d \equiv 1 \mod 4, \\ 4d & \text{otherwise} \end{cases}$$

Theorem 2.7. *Suppose $K = \mathbb{Q}\left(\sqrt{d_1}, \sqrt{d_2}\right)$ be a real biquadratic number field. Then there are exactly three real quadratic subfields K_i of K, namely,*

$$K_1 = \mathbb{Q}\left(\sqrt{d_1}\right), \; K_2 = \mathbb{Q}\left(\sqrt{d_2}\right), \; K_3 = \mathbb{Q}\left(\sqrt{d_1 d_2}\right).$$

3 Experimental Data

To collect experimental data on log-unit lattices, we implemented a program in SAGE, a computer algebra package, which computes bases for specific classes of biquadratic number fields. Our program then checks to determine whether these bases are orthogonal. We include the following segment of code:

```
def init_orthog_check(a, lower_bound, upper_bound, test=lambda x: True, verb=
    lambda x: True):
    """"Generate real biquadratic number fields."""
    if (not is_squarefree(a)):
        return
    if (a < 2):
        return
    if (lower_bound <= 2):
        return
    if (lower_bound > upper_bound):
        return
    count = 0
    for b in range(lower_bound, upper_bound):
        if(is_squarefree(b) and a!=b and test(b)):
            print 'Number␣field:␣Q[{}^(1/2),{}^(1/2)]'.format(a,b)
            verb(b)
            count = orthog_check(a,b,count)
    print '\n','Counter␣=',count

def orthog_check(a, b, c):
    """Compute BB^T."""
    K.<a,b> = NumberField([minpoly(a^(1/2)), minpoly(b^(1/2))])
    B = log_unit_basis(K, print_basis="yes")
    B = matrix(B).n()
    M = ((B*B.T).n(digits=3))
    print B,'\n'
    print '\n',M,'\n'
    c = c + 1
    return c

def desired_condition(x):
    """Check if x is prime and congruent to 3 mod 4."""
    r = x%4
    if (r==3 and is_prime(x)):
        print 'Congruence␣class␣(d_2):␣{}␣mod␣{}'.format(r,4)
        return True
    return False

def log_unit_basis(K, **opt):
    """Compute basis for log-unit lattice associated to K."""
    B, U = [], []
    for u in Set(UnitGroup(K).fundamental_units()):
        v = [log(abs(i(u))) for i in K.embeddings(QQbar)]
        B = B + [v]
        U = U + [u]
    if ('print_basis' in opt):
        print "Fundamental␣Units␣=", (Set(U))
    return B
```

To run this code, we used the following command:

```
init_orthog_check(2, 3, 5100, desired_condition).
```

This command generates real biquadratic number fields of the form $K = \mathbb{Q}(\sqrt{2},\sqrt{d})$, where d is prime in $[3, 5100]$ and congruent to $3 \mod 4$. Then SAGE finds a set of units u_1, u_2, u_3

which generate $\mathcal{O}_K^\times/\{\pm 1\}$ and computes the basis $\{\lambda(u_1), \lambda(u_2), \lambda(u_3)\}$ of the associated log-unit lattice. The program then forms the matrix B whose rows correspond to each basis vector and computes BB^T, a 3×3 a symmetric matrix whose entries are given by the euclidean inner-product $\langle b_i, b_j \rangle\,;\ i, j \in \{1, 2, 3\}$. In particular, the off-diagonal entries correspond to the inner-product of two distinct basis vectors. If all the off-diagonal entries are zero, then we conclude that the basis B is orthogonal.

For all values of d in the specified interval, we observed that each product matrix BB^T, has either all zero or approximately zero off-diagonal entries (for a sample of these values, see Appendix). However, the occurrence of nonzero off-diagonal entries was suspected to be due to the limited degree of precision with which SAGE computes the log-unit embeddings. Our program's output shows that for such values of d the given basis B is orthogonal.

4 Main Results

Theorem 4.1. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ be a biquadratic number field, where d is prime. If $d \equiv 3 \mod 4$, then $\Lambda = \operatorname{Log}(\mathcal{O}_K^\times)$ is orthogonal.*

Proof. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ where d is prime, and let $\mu(K)$ be the cyclic group consisting of the roots of unity which lie in K. Assume $d \equiv 3 \mod 4$. Then, by Theorem 2 in [6], we can find $\varepsilon_1, \varepsilon_2, \varepsilon_3$ such that $\mathcal{O}_K^\times/\mu(K) = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$, where

$$\sigma_i\,(\varepsilon_i) = \varepsilon_i \text{ and } \sigma_j\,(\varepsilon_i) = \varepsilon_i^{-1} \text{ for all } i \neq j;\ i, j \in \{1, 2, 3\}.$$

By Dirichlet's Unit Theorem, $\Lambda = \operatorname{Log}\left(\mathcal{O}_K^\times\right)$ is a lattice in $\mathbb{R}^4$ with rank 3 and basis $B = \{\operatorname{Log}(\varepsilon_1), \operatorname{Log}(\varepsilon_2), \operatorname{Log}(\varepsilon_3)\}$. We claim B is orthogonal. By applying the definition of Log embedding and using the fact that ln is a homomorphism, we get

$$\begin{aligned} \operatorname{Log}(\varepsilon_1) &= (\ln|\varepsilon_1|, \ln|\varepsilon_1|, \ln\left|\varepsilon_1^{-1}\right|, \ln\left|\varepsilon_1^{-1}\right|) \\ &= (\ln|\varepsilon_1|, \ln|\varepsilon_1|, -\ln|\varepsilon_1|, -\ln|\varepsilon_1|). \end{aligned}$$

Similarly,

$$\begin{aligned} \operatorname{Log}(\varepsilon_2) &= (\ln|\varepsilon_2|, -\ln|\varepsilon_2|, \ln|\varepsilon_2|, -\ln|\varepsilon_2|), \text{ and} \\ \operatorname{Log}(\varepsilon_3) &= (\ln|\varepsilon_3|, -\ln|\varepsilon_3|, -\ln|\varepsilon_3|, \ln|\varepsilon_3|). \end{aligned}$$

Now write $b_i = \ln|\varepsilon_i|$. Then

$$\begin{aligned} \langle \operatorname{Log}(\varepsilon_1), \operatorname{Log}(\varepsilon_2) \rangle &= b_1b_2 - b_1b_2 - b_1b_2 + b_1b_2 = 0, \text{ and} \\ \langle \operatorname{Log}(u_1), \operatorname{Log}(u_3) \rangle &= b_1b_3 - b_1b_3 + b_1b_3 - b_1b_3 = 0, \text{ and} \\ \langle \operatorname{Log}(\varepsilon_2), \operatorname{Log}(\varepsilon_3) \rangle &= b_2b_3 + b_2b_3 - b_2b_3 - b_2b_3 = 0. \end{aligned}$$

Thus B is orthogonal, as claimed. The result follows. □

Theorem 4.2. *Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a real biquadratic number field, where d_1, d_2 are prime. Assume either $d_1 = 2$ and $d_2 \equiv 3 \mod 4$ or $d_1 \equiv 1 \mod 4$ and $d_2 \not\equiv 3 \mod 4$ with $\sigma_K = (-1, -1, +1)$. Let R_i be the regulator of each subfield K_i of K. Then $R_i = \frac{1}{2}\lambda_i(\Lambda)$.*

Proof. By Theorem 2 in [6] there exists $u_i \in K_i^\times$ for all $i \in \{1, 2, 3, \}$ such that $\mathcal{O}_K^\times/\mu(K) = \langle u_1, u_2, u_3 \rangle$, where

$$\sigma_i\,(u_i) = u_i \text{ and } \sigma_j\,(u_i) = u_i^{-1} \text{ for } i \neq j;\ i, j \in \{1, 2, 3\}.$$

Then

$$\begin{aligned} b_1 &= (\ln|u_1|, \ln|u_1|, -\ln|u_1|, -\ln|u_1|), \\ b_2 &= (\ln|u_2|, -\ln|u_2|, \ln|u_2|, -\ln|u_2|), \\ b_3 &= (\ln|u_3|, -\ln|u_3|, -\ln|u_3|, \ln|u_3|) \end{aligned}$$

is a basis for Λ, a rank 3 lattice in R^4. By Theorem 4.1, Λ is orthogonal. Assume $\|b_1\| < \|b_2\| < \|b_3\|$, so by Proposition 3 $\lambda_i(\Lambda) = \|b_i\|$. But $\|b_i\| = 2\ln|u_i|$. Also, for any real quadratic number field we know $R_i = \ln|u_i|$. Then $\|b_i\| = 2R_i$ for all $i \in \{1, 2, 3\}$, so $\frac{\lambda_i}{2} = R_i$. □

Remark. In particular, since $\psi(\Lambda) = \frac{\lambda_1}{2}$ for any lattice, it follows from the above result that $\psi(\Lambda) = R_1$.

Corollary 4.3. *Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a real biquadratic number field, where d_1, d_2 are prime. Assume either $d_1 = 2$ and $d_2 \equiv 3 \mod 4$ or $d_1 \equiv 1 \mod 4$ and $d_2 \not\equiv 3 \mod 4$ with $\sigma_K = (-1, -1, +1)$. Let R_i be the regulator of each subfield K_i of K. Then*

$$\left(\sum_{i=1}^{3} \left(\log\left(\tfrac{1}{2} \left(\sqrt{\Delta_i - 4} + \sqrt{\Delta_i} \right) \right) \right)^2 \right)^{\frac{1}{2}} < \rho(\Lambda) < \left(\sum_{i=1}^{3} \tfrac{1}{2}\Delta_i \left(\tfrac{1}{2} \log \Delta_i + 1 \right)^2 \right)^{\frac{1}{2}}.$$

Proof. By Proposition 2.1 and Theorem 4.2 we have the following

$$\rho(\Lambda)^2 = \tfrac{1}{2} \sum_{i=1}^{3} \lambda_i^2 = \tfrac{1}{2} \sum_{i=1}^{3} (2R_i)^2 = 2 \sum_{i=1}^{3} R_i^2.$$

Then by Hua

$$\sum_{i=1}^{3} R_i^2 < \sum_{i=1}^{3} \left(\sqrt{\tfrac{1}{2}\Delta_i} \left(\tfrac{1}{2} \log \Delta_i + 1 \right) \right)^2.$$

So

$$\rho(\Lambda)^2 < \sum_{i=1}^{3} \tfrac{1}{2}\Delta_i \left(\tfrac{1}{2} \log \Delta_i + 1 \right)^2.$$

Lower bound follows from Nagell. □

Lemma 2. Let $\mathcal{L}$ be a rank two lattice. Suppose $w_1 \not\perp w_2 \in \mathcal{L}$ are linearly independent with $\lambda_1 = \|w_1\|$ and $\lambda_2 = \|w_2\|$. Then $\mathcal{L}(w_1, w_2)$ is not orthogonal.

Proof. Suppose to the contrary that $\mathcal{L}$ is orthogonal. Then there is a basis $B = \{b_1, b_2\}$ of $\mathcal{L}$ with $b_1 \perp b_2$. Assume $\|b_1\| \leq \|b_2\|$. Then by Proposition 3, $\|b_1\| = \|w_1\|$ and $\|b_2\| = \|w_2\|$. Since $w_1, w_2 \in \mathcal{L}(B)$, we know

$$w_1 = a_1 b_1 + a_2 b_2 \quad \text{and} \quad w_2 = c_1 b_1 + c_2 b_2$$

for some $a_i, c_i \in \mathbb{Z}$. So

$$\|w_1\|^2 = a_1^2 \|b_1\| + a_2^2 \|b_2\| \quad \text{and} \quad \|w_2\|^2 = c_1^2 \|b_1\|^2 + c_2^2 \|b_2\|^2$$

since B is orthogonal. Suppose $\lambda_1 < \lambda_2$. Then $\|b_1\|^2 = \|w_1\|^2$ implies $a_1 = \pm 1$ and $a_2 = 0$. Similarly, $\|b_2\|^2 = \|w_2\|^2$ implies $c_2 = \pm 1$ and $c_1 = 0$. So $w_1 = \pm b_1$ and $w_2 = \pm b_2$. But this implies $w_1 \perp w_2$, a contradiction. Now suppose $\lambda_1 = \lambda_2$. Then $\|b_2\|^2 = \|b_1\|^2 = \|w_1\|^2$ implies $a_1 = \pm 1$ and $a_2 = 0$ or $c_2 = \pm 1$ and $c_1 = 0$. So $w_1 = \pm b_1$ or $w_1 = \pm b_2$. Similarly, $\|b_1\|^2 = \|b_2\|^2 = \|w_2\|^2$ implies $c_2 = \pm 1$ and $c_1 = 0$ or $a_1 = \pm 1$ and $a_2 = 0$. So $w_2 = \pm b_2$ or $w_2 = \pm b_1$. Hence either $w_1 \perp w_2$ or $w_1 = \pm w_2$. But either case yields a contradiction. □

For the remainder of this section, let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a real biquadratic number field, and let K_i be the quadratic subfields of K. Let $\varepsilon_i > 1$ be such that $\langle \varepsilon_i \rangle = \mathcal{O}_{K_i}^\times / \mu(K_i)$.

Lemma 3. If d_1, d_2 are distinct primes congruent to $3 \mod 4$, then there exists a non-orthogonal basis $B = \{v_1, v_2, v_3\}$ for $\Lambda = \mathrm{Log}(\mathcal{O}_K^\times)$ with $v_3 \perp v_1, v_3 \perp v_2$, and $v_1 \not\perp v_2$.

Proof. Assume $d_1, d_2 \equiv 3 \mod 4$. Then, by Theorem 2 in [6],

$$\mathcal{O}_K^\times / \mu(K) = \left\langle \sqrt{\varepsilon_2 \varepsilon_1}, \sqrt{\varepsilon_2 \varepsilon_1^{-1}}, \sqrt{\varepsilon_3} \right\rangle.$$

By Dirichlet's Unit Theorem, $\Lambda = \mathrm{Log}\left(\mathcal{O}_K^\times\right)$ is a rank three lattice in $\mathbb{R}^4$ with basis

$$B = \left\{ v_1 = \mathrm{Log}\left(\sqrt{\varepsilon_2 \varepsilon_1}\right), v_2 = \mathrm{Log}\left(\sqrt{\varepsilon_2 \varepsilon_1^{-1}}\right), v_3 = \mathrm{Log}\left(\sqrt{\varepsilon_3}\right) \right\}.$$

Write $b_0 = \ln\left|\sigma_0\left(\sqrt{\varepsilon_2 \varepsilon_1}\right)\right|, c_0 = \ln\left|\sigma_0\left(\sqrt{\varepsilon_2 \varepsilon_1^{-1}}\right)\right|$ and $a_0 = \ln\left|\sigma_0\left(\sqrt{\varepsilon_3}\right)\right|$. Then

$$\begin{aligned} b_0 &= \ln\left|\sigma_0\left(\sqrt{\varepsilon_2}\right)\sigma_0(\sqrt{\varepsilon_1})\right| = \ln\left|\pm\sqrt{\sigma_0(\varepsilon_2)\sigma_0(\varepsilon_1)}\right| = \tfrac{1}{2}\big(\ln(\varepsilon_2) + \ln(\varepsilon_1)\big), \\ c_0 &= \ln\left|\sigma_0\left(\sqrt{\varepsilon_2}\right)\sigma_0\left(\sqrt{\varepsilon_1^{-1}}\right)\right| = \ln\left|\pm\sqrt{\sigma_0(\varepsilon_2)(\sigma_0(\varepsilon_1))^{-1}}\right| = \tfrac{1}{2}\big(\ln(\varepsilon_2) - \ln(\varepsilon_1)\big), \\ a_0 &= \ln\left|\sqrt{\sigma_0(\varepsilon_3)}\right| = \ln\left|\pm\sqrt{\sigma_0(\varepsilon_3)}\right| = \tfrac{1}{2}\ln(\varepsilon_3). \end{aligned}$$

So

$$v_1 = (b_0, -c_0, c_0, -b_0), \quad v_2 = (c_0, -b_0, b_0, -c_0), \quad v_3 = (a_0, -a_0, -a_0, a_0).$$

Note that $v_1 \perp v_3$, $v_2 \perp v_3$, but $v_1 \not\perp v_2$. □

Lemma 4. The sublattice $\mathcal{L}(v_1, v_2) \subseteq \Lambda$ is not orthogonal.

Proof. Consider the sublattice $\mathcal{L}(v_1, v_2) \subseteq \Lambda$. Set $w_1, w_2 \in \mathcal{L}(v_1, v_2)$ to be

$$\begin{aligned} w_1 &= v_1 - v_2 = (\ln\varepsilon_1, \ln\varepsilon_1, -\ln\varepsilon_1, -\ln\varepsilon_1) \\ w_2 &= v_1 + v_2 = (\ln\varepsilon_2, -\ln\varepsilon_2, \ln\varepsilon_2, -\ln\varepsilon_2). \end{aligned}$$

Since $v_1 \not\perp v_2$, we know $\|w_2\| \neq \|w_1\|$. So either $\|w_2\| > \|w_1\|$ or $\|w_2\| < \|w_1\|$. Without loss of generality, assume $\|w_2\| > \|w_1\|$, i.e., suppose $\varepsilon_2 > \varepsilon_1$. We claim $\|v_1\| < \|w_2\|$. Since $w_1 \perp w_2$ and $v_1 = \frac{1}{2}(w_1 + w_2)$, we get that

$$\|v_1\|^2 = \langle v_1, v_1 \rangle = \tfrac{1}{4}\|w_1\|^2 + \tfrac{1}{4}\|w_2\|^2.$$

But $\|w_i\|^2 = 4(\ln\varepsilon_i)^2$. So

$$\|v_1\|^2 = (\ln\varepsilon_1)^2 + (\ln\varepsilon_2)^2 < 2\left(\ln\varepsilon_2\right)^2 < 4\left(\ln\varepsilon_2\right)^2 = \|w_2\|^2.$$

Thus $\|v_1\| < \|w_2\|$, as claimed. Now let $x \in \mathcal{L}(v_1, v_2) \setminus \{0\}$. So $x = a_1 v_1 + a_2 v_2$ for some $a_i \in \mathbb{Z}$ with at least one nonzero a_i. Observe that

$$x = a_1 \left(\tfrac{1}{2}(w_1 + w_2)\right) + a_2 \left(\tfrac{1}{2}(-w_1 + w_2)\right) = \tfrac{1}{2}(a_1 - a_2)w_1 + \tfrac{1}{2}(a_1 + a_2)w_2.$$

Then

$$\|x\|^2 = \langle x, x\rangle = \tfrac{1}{4}(a_1 - a_2)^2 \|w_1\|^2 + \tfrac{1}{4}(a_1 + a_2)^2 \|w_2\|^2$$

since $w_1 \perp w_2$. So

$$\|x\|^2 = (a_1 - a_2)^2 (\ln \varepsilon_1)^2 + (a_1 + a_2)^2 (\ln \varepsilon_2)^2.$$

Let $u_1 = a_1 - a_2$ and $u_2 = a_1 + a_2$. To minimize $\|x\|$, we find smallest integers $|u_1|$ and $|u_2|$. In matrix form, we have

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

But since $\det\left(\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}\right) = 2$, we get

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \tfrac{1}{2} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(u_1 + u_2) \\ \frac{1}{2}(-u_1 + u_2) \end{bmatrix}.$$

Recall that $a_1, a_2 \in \mathbb{Z}$, so $u_1 \equiv u_2 \mod 2$. So either $u_1 = u_2 = \pm 1$ or $u_1 = \pm 1, u_2 = \mp 1$ or $u_1 = \pm 2, u_2 = 0$ or $u_1 = 0, u_2 = \pm 2$. Thus $x = \pm v_1, \pm v_2, \pm w_1, \pm w_2$. Recall that $\|v_1\| = \|v_2\|$ and $\|w_2\| > \|w_1\|, \|v_1\|$ so $\lambda_1 = \|v_1\| = \|v_2\|$ and $\lambda_2 = \|w_1\|$ or vice versa. But $\langle v_1, w_1\rangle = 2(\ln \varepsilon_1)^2 \neq 0$ since $\varepsilon_1 > 1$. So $v_1 \not\perp w_1$. Similarly $v_2 \not\perp w_1$. Therefore, by Lemma 2, $\mathcal{L}(v_1, v_2)$ is not orthogonal.

□

Proposition 8. *Suppose V is a finite-dimensional inner product space. Let $v_0 \in V$ be a nonzero vector, and let W be the orthogonal complement of* $\operatorname{span}(v_0)$. *Let $L_W \subset W$ be a lattice, and let L be the lattice generated by L_W and v_0. Suppose that $(b_1, \ldots, b_n)$ is an orthogonal basis for L. Then $v_0 = \pm b_i$ for some i.*

Proof. Without loss of generality, the b_i are ordered so that $\|b_i\| \le \|b_{i+1}\|$ for each i. Choose the largest k for which $\|b_k\| \le \|v_0\|$. Since $\|b_1\| = \lambda_1 \le \|v_0\|$, such a k exists. As the b_i form a basis for L, we have that there exist $\alpha_i \in \mathbb{Z}$ for which

$$v_0 = \sum \alpha_i b_i = \sum_{i=1}^{k} \alpha_i b_i + \sum_{j=k+1}^{n} \alpha_j b_j.$$

Taking the square of the magnitude on both sides, and using the fact that $(b_1, \ldots, b_n)$ is orthogonal, we have

$$\|v_0\|^2 = \sum_{i=1}^{k} \alpha_i^2 \|b_i\|^2 + \sum_{j=k+1}^{n} \alpha_j^2 \|b_j\|^2.$$

But for $j \ge k+1$, $\|b_j\|^2 > \|v_0\|^2$, and hence $\alpha_j = 0$.

Every vector $v \in L$ may be written uniquely in the form $w + \beta v_0$, where $w \in L_W$ and $\beta \in \mathbb{Z}$. Since $\langle v_0, w\rangle = 0$, we see that

$$\|v\|^2 = \|w\|^2 + \beta^2 \|v_0\|^2.$$

In particular, if $\|v\| \leq \|v_0\|$, then $|\beta| \leq 1$. In the case that $\beta = \pm 1$, we have $w = 0$ and so $v = \pm v_0$. If $\beta = 0$, then $v \in W$. Applying this reasoning to the b_i for $i \leq k$, we see that either all of the $b_i \in W$, or for some i, $b_i = \pm v_0$. Since $v_0 \notin W$, the first possibility cannot hold. □

Theorem 4.4. *If d_1, d_2 are distinct primes congruent to* $3 \mod 4$, *then* $\Lambda = \operatorname{Log}(\mathcal{O}_K^\times)$ *is not orthogonal.*

Proof. Suppose (b_1, b_2, b_3) is an orthogonal basis for Λ. Then by Proposition 8, one of the b_i—say, b_3—equals $\pm v_3$. But then (b_1, b_2) must form an orthogonal basis for $\mathcal{L}(v_1, v_2)$, which contradicts Lemma 4. □

Proposition 9. *Let $\mathcal{L}(B)$ be a non-orthogonal lattice with basis $B = \{v_1, v_2, v_3\}$ where $v_3 \perp v_1, v_3 \perp v_2$, and $\|v_1\| = \|v_2\|$. Then*

$$\operatorname{covol}(\mathcal{L}(B)) = \tfrac{1}{2} \|v_1 - v_2\| \, \|v_1 + v_2\| \, \|v_3\| \, .$$

Proof. Consider the sublattice $\mathcal{L}(v_1, v_2)$. Since $\|v_1\| = \|v_2\|$, we know $\Phi(v_1, v_2)$ is a rhombus with diagonals of length $\|v_1 - v_2\|$ and $\|v_1 + v_2\|$. So

$$\operatorname{covol}\left(\mathcal{L}(v_1, v_2)\right) = \tfrac{1}{2} \|v_1 - v_2\| \, \|v_1 + v_2\| \, .$$

Now recall that $v_3 \perp v_1$ and $v_3 \perp v_2$, so $\Phi(B)$ is a parallelepiped with height $\|v_3\|$. Thus

$$\operatorname{covol}(\mathcal{L}(B)) = \tfrac{1}{2} \|v_1 - v_2\| \, \|v_1 + v_2\| \, \|v_3\| \, .$$

□

Proposition 10. *Let $\mathcal{L}(B)$ be a non-orthogonal lattice with basis $B = \{v_1, v_2, v_3\}$ where $v_3 \perp v_1, v_2$ and $\|v_1\| = \|v_2\|$. Let $\ell = \max\{\|v_1 - v_2\|, \|v_1 + v_2\|\}$. Then*

$$\rho(\mathcal{L}) = \sqrt{(\tfrac{1}{2}\|v_3\|)^2 + (k\ell)^2},$$

where $k = \frac{\|v_1\| \sin(\theta)}{\sin(180 - 2\theta)}$ and $\theta = \frac{1}{2} \cos^{-1}\left(\frac{\langle v_1, v_2 \rangle}{\|v_1\| \|v_2\|}\right)$.

References

[1] Craig Gentry, *A Fully Homomorphic Encryption Scheme*, Stanford University, 2009.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, 3rd Ed., Springer, Berlin, 1996.

[3] James S. Milne, *Algebraic Number Theory (v3.07)*, 2008. Available at www.jmilne.org/math/.

[4] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd Ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[5] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[6] Marcin Mazur and Stephen V. Ullom, *Galois module structure of units in real biquadratic number fields*, Acta Arith. **111** (2004), no. 2, 105–124, DOI 10.4064/aa111-2-1.

Fernando Azpeitia Tellez
California State University, San Marcos
333 S Twin Oaks Valley Rd
San Marcos, CA 92096
E-mail: `azpei002@cougars.csusm.edu`

Christopher Powell
California State University, San Marcos
333 S Twin Oaks Valley Rd
San Marcos, CA 92096
E-mail: `powel054@cougars.csusm.edu`

Appendix

Table 1: Selected SAGE Output

d	B	BB^T
3	$\begin{bmatrix} 0.659 & 0.659 & -0.659 & -0.659 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ -1.15 & 1.15 & 1.15 & -1.15 \end{bmatrix}$	$\begin{bmatrix} 1.73 & 0.000 & 0.000 \\ 0.000 & 3.11 & 0.000 \\ 0.000 & 0.000 & 5.26 \end{bmatrix}$
7	$\begin{bmatrix} 1.70 & -1.70 & -1.70 & 1.70 \\ 1.38 & 1.38 & -1.38 & -1.38 \\ -0.881 & 0.881 & -0.881 & 0.881 \end{bmatrix}$	$\begin{bmatrix} 11.6 & 0.000 & 2.22 \times 10^{-16} \\ 0.000 & 7.67 & -2.22 \times 10^{-16} \\ 2.22 \times 10^{-16} & -2.22 \times 10^{-16} & 3.11 \end{bmatrix}$
11	$\begin{bmatrix} 1.50 & 1.50 & -1.50 & -1.50 \\ -2.99 & 2.99 & 2.99 & -2.99 \\ -0.881 & 0.881 & -0.881 & 0.881 \end{bmatrix}$	$\begin{bmatrix} 8.96 & 0.000 & 0.000 \\ 0.000 & 35.7 & -4.44 \times 10^{-16} \\ 0.000 & -4.44 \times 10^{-16} & 3.11 \end{bmatrix}$
19	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 2.91 & 2.91 & -2.91 & -2.91 \\ 2.15 & -2.15 & -2.15 & 2.15 \end{bmatrix}$	$\begin{bmatrix} 3.11 & -4.44 \times 10^{-16} & 2.22 \times 10^{-16} \\ -4.44 \times 10^{-16} & 34.0 & 0.000 \\ 2.22 \times 10^{-16} & 0.000 & 18.5 \end{bmatrix}$
23	$\begin{bmatrix} 1.94 & 1.94 & -1.94 & -1.94 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ -5.40 & 5.40 & 5.40 & -5.40 \end{bmatrix}$	$\begin{bmatrix} 15.0 & 0.000 & 0.000 \\ 0.000 & 3.11 & -8.88 \times 10^{-16} \\ 0.000 & -8.88 \times 10^{-16} & 116 \end{bmatrix}$
31	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ -2.42 & 2.42 & 2.42 & -2.42 \\ 4.01 & 4.01 & -4.01 & -4.01 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 4.44 \times 10^{-16} & 0.000 \\ 4.44 \times 10^{-16} & 23.4 & 0.000 \\ 0.000 & 0.000 & 64.3 \end{bmatrix}$
43	$\begin{bmatrix} 4.42 & 4.42 & -4.42 & -4.42 \\ 4.97 & -4.97 & -4.97 & 4.97 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 78.3 & 0.000 & 0.000 \\ 0.000 & 98.9 & -8.88 \times 10^{-16} \\ 0.000 & -8.88 \times 10^{-16} & 3.11 \end{bmatrix}$
47	$\begin{bmatrix} 2.28 & 2.28 & -2.28 & -2.28 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 7.64 & -7.64 & -7.64 & 7.64 \end{bmatrix}$	$\begin{bmatrix} 20.8 & 0.000 & 0.000 \\ 0.000 & 3.11 & -8.88 \times 10^{-16} \\ 0.000 & -8.88 \times 10^{-16} & 233 \end{bmatrix}$
59	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 3.48 & 3.48 & -3.48 & -3.48 \\ -6.66 & 6.66 & 6.66 & -6.66 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 8.88 \times 10^{-16} \\ 0.000 & 48.5 & 0.000 \\ 8.88 \times 10^{-16} & 0.000 & 178. \end{bmatrix}$
67	$\begin{bmatrix} 5.74 & 5.74 & -5.74 & -5.74 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ -6.29 & 6.29 & 6.29 & -6.29 \end{bmatrix}$	$\begin{bmatrix} 132. & 0.000 & 0.000 \\ 0.000 & 3.11 & -8.88 \times 10^{-16} \\ 0.000 & -8.88 \times 10^{-16} & 158 \end{bmatrix}$
71	$\begin{bmatrix} 4.42 & 4.42 & -4.42 & -4.42 \\ -2.83 & 2.83 & 2.83 & -2.83 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 78.3 & 0.000 & 0.000 \\ 0.000 & 32.0 & 0.000 \\ 0.000 & 0.000 & 3.11 \end{bmatrix}$
79	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ 2.54 & 2.54 & -2.54 & -2.54 \\ 4.82 & -4.82 & -4.82 & 4.82 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 0.000 \\ 0.000 & 25.8 & 0.000 \\ 0.000 & 0.000 & 93.1 \end{bmatrix}$
83	$\begin{bmatrix} 11.0 & -11.0 & -11.0 & 11.0 \\ 2.55 & 2.55 & -2.55 & -2.55 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 482. & 0.000 & 1.78 \times 10^{-15} \\ 0.000 & 26.0 & 0.000 \\ 1.78 \times 10^{-15} & 0.000 & 3.11 \end{bmatrix}$
103	$\begin{bmatrix} 6.51 & 6.51 & -6.51 & -6.51 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ -5.84 & 5.84 & 5.84 & -5.84 \end{bmatrix}$	$\begin{bmatrix} 170. & 0.000 & 0.000 \\ 0.000 & 3.11 & 8.88 \times 10^{-16} \\ 0.000 & 8.88 \times 10^{-16} & 137. \end{bmatrix}$

d	B	BB^T
107	$\begin{bmatrix} 3.78 & 3.78 & -3.78 & -3.78 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ -14.0 & 14.0 & 14.0 & -14.0 \end{bmatrix}$	$\begin{bmatrix} 57.2 & 0.000 & 0.000 \\ 0.000 & 3.11 & 1.78 \times 10^{-15} \\ 0.000 & 1.78 \times 10^{-15} & 782. \end{bmatrix}$
127	$\begin{bmatrix} 8.03 & 8.03 & -8.03 & -8.03 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ -3.12 & 3.12 & 3.12 & -3.12 \end{bmatrix}$	$\begin{bmatrix} 258. & 0.000 & 0.000 \\ 0.000 & 3.11 & -4.44 \times 10^{-16} \\ 0.000 & -4.44 \times 10^{-16} & 38.9 \end{bmatrix}$
131	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 4.98 & 4.98 & -4.98 & -4.98 \\ -9.58 & 9.58 & 9.58 & -9.58 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 0.000 \\ 0.000 & 99.3 & 0.000 \\ 0.000 & 0.000 & 367. \end{bmatrix}$
139	$\begin{bmatrix} 9.43 & 9.43 & -9.43 & -9.43 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ 4.26 & -4.26 & -4.26 & 4.26 \end{bmatrix}$	$\begin{bmatrix} 356. & 0.000 & 0.000 \\ 0.000 & 3.11 & -4.44 \times 10^{-16} \\ 0.000 & -4.44 \times 10^{-16} & 72.5 \end{bmatrix}$
151	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 11.0 & 11.0 & -11.0 & -11.0 \\ -7.98 & 7.98 & 7.98 & -7.98 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & -8.88 \times 10^{-16} \\ 0.000 & 482. & 0.000 \\ -8.88 \times 10^{-16} & 0.000 & 255. \end{bmatrix}$
163	$\begin{bmatrix} 9.33 & 9.33 & -9.33 & -9.33 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ -3.24 & 3.24 & 3.24 & -3.24 \end{bmatrix}$	$\begin{bmatrix} 349. & 0.000 & 0.000 \\ 0.000 & 3.11 & -4.44 \times 10^{-16} \\ 0.000 & -4.44 \times 10^{-16} & 41.9 \end{bmatrix}$
167	$\begin{bmatrix} 16.2 & -16.2 & -16.2 & 16.2 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 2.91 & 2.91 & -2.91 & -2.91 \end{bmatrix}$	$\begin{bmatrix} 1060. & 1.78 \times 10^{-15} & 0.000 \\ 1.78 \times 10^{-15} & 3.11 & 0.000 \\ 0.000 & 0.000 & 33.83.11 \end{bmatrix}$
179	$\begin{bmatrix} 7.97 & 7.97 & -7.97 & -7.97 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 13.3 & -13.3 & -13.3 & 13.3 \end{bmatrix}$	$\begin{bmatrix} 254. & 0.000 & 0.000 \\ 0.000 & 3.11 & 1.78 \times 10^{-15} \\ 0.000 & 1.78 \times 10^{-15} & 707. \end{bmatrix}$
191	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 8.35 & 8.35 & -8.35 & -8.35 \\ -13.3 & 13.3 & 13.3 & -13.3 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 1.78 \times 10^{-15} \\ 0.000 & 279. & 0.000 \\ 1.78 \times 10^{-15} & 0.000 & 703. \end{bmatrix}$
199	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ -3.34 & 3.34 & 3.34 & -3.34 \\ 12.1 & 12.1 & -12.1 & -12.1 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 4.44 \times 10^{-16} & 0.000 \\ 4.44 \times 10^{-16} & 44.7 & 0.000 \\ 0.000 & 0.000 & 586. \end{bmatrix}$
211	$\begin{bmatrix} -8.23 & 8.23 & 8.23 & -8.23 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 13.5 & 13.5 & -13.5 & -13.5 \end{bmatrix}$	$\begin{bmatrix} 271. & -8.88 \times 10^{-16} & 0.000 \\ -8.88 \times 10^{-16} & 3.11 & 0.000 \\ 0.000 & 0.000 & 731. \end{bmatrix}$
223	$\begin{bmatrix} 9.61 & -9.61 & -9.61 & 9.61 \\ 3.05 & 3.05 & -3.05 & -3.05 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 369. & 0.000 & -1.78 \times 10^{-15} \\ 0.000 & 37.3 & 0.000 \\ -1.78 \times 10^{-15} & 0.000 & 3.11 \end{bmatrix}$
227	$\begin{bmatrix} 19.0 & -19.0 & -19.0 & 19.0 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 3.06 & 3.06 & -3.06 & -3.06 \end{bmatrix}$	$\begin{bmatrix} 1450. & 0.000 & 0.000 \\ 0.000 & 3.11 & 0.000 \\ 0.000 & 0.000 & 37.4 \end{bmatrix}$
239	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 8.17 & 8.17 & -8.17 & -8.17 \\ 17.9 & -17.9 & -17.9 & 17.9 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & -1.78 \times 10^{-15} \\ 0.000 & 267. & 0.000 \\ -1.78 \times 10^{-15} & 0.000 & 1280. \end{bmatrix}$

d	B	BB^T
251	$\begin{bmatrix} -11.4 & 11.4 & 11.4 & -11.4 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ 7.91 & 7.91 & -7.91 & -7.91 \end{bmatrix}$	$\begin{bmatrix} 518. & 1.78 \times 10^{-15} & 0.000 \\ 1.78 \times 10^{-15} & 3.11 & 0.000 \\ 0.000 & 0.000 & 250. \end{bmatrix}$
263	$\begin{bmatrix} 23.3 & -23.3 & -23.3 & 23.3 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ 6.27 & 6.27 & -6.27 & -6.27 \end{bmatrix}$	$\begin{bmatrix} 2170. & 3.55 \times 10^{-15} & 0.000 \\ 3.55 \times 10^{-15} & 3.11 & 0.000 \\ 0.000 & 0.000 & 157. \end{bmatrix}$
271	$\begin{bmatrix} -7.98 & 7.98 & 7.98 & -7.98 \\ 13.1 & 13.1 & -13.1 & -13.1 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 255. & 0.000 & 8.88 \times 10^{-16} \\ 0.000 & 685. & 0.000 \\ 8.88 \times 10^{-16} & 0.000 & 3.11 \end{bmatrix}$
283	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ -9.53 & 9.53 & 9.53 & -9.53 \\ 9.72 & 9.72 & -9.72 & -9.72 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 1.78 \times 10^{-15} & 0.000 \\ 1.78 \times 10^{-15} & 364. & 0.000 \\ 0.000 & 0.000 & 378. \end{bmatrix}$
1019	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 39.7 & -39.7 & -39.7 & 39.7 \\ 15.1 & 15.1 & -15.1 & -15.1 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 0.000 \\ 0.000 & 6310. & 0.000 \\ 0.000 & 0.000 & 908. \end{bmatrix}$
1031	$\begin{bmatrix} 17.4 & 17.4 & -17.4 & -17.4 \\ -31.1 & 31.1 & 31.1 & -31.1 \\ -0.881 & 0.881 & -0.881 & 0.881 \end{bmatrix}$	$\begin{bmatrix} 1210. & 0.000 & 0.000 \\ 0.000 & 3880. & 3.55 \times 10^{-15} \\ 0.000 & 3.55 \times 10^{-15} & 3.11 \end{bmatrix}$
1039	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ 12.0 & -12.0 & -12.0 & 12.0 \\ 31.1 & 31.1 & -31.1 & -31.1 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 1.78 \times 10^{-15} & 0.000 \\ 1.78 \times 10^{-15} & 576. & 0.000 \\ 0.000 & 0.000 & 3860. \end{bmatrix}$
1051	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 31.4 & 31.4 & -31.4 & -31.4 \\ -19.5 & 19.5 & 19.5 & -19.5 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & -3.55 \times 10^{-15} \\ 0.000 & 3950. & 0.000 \\ -3.55 \times 10^{-15} & 0.000 & 1520. \end{bmatrix}$
1063	$\begin{bmatrix} 17.9 & 17.9 & -17.9 & -17.9 \\ 21.6 & -21.6 & -21.6 & 21.6 \\ -0.881 & 0.881 & -0.881 & 0.881 \end{bmatrix}$	$\begin{bmatrix} 1280. & 0.000 & 0.000 \\ 0.000 & 1860. & 3.55 \times 10^{-15} \\ 0.000 & 3.55 \times 10^{-15} & 3.11 \end{bmatrix}$
1087	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ 3.84 & 3.84 & -3.84 & -3.84 \\ 28.9 & -28.9 & -28.9 & 28.9 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & -3.55 \times 10^{-15} \\ 0.000 & 59.1 & 0.000 \\ -3.55 \times 10^{-15} & 0.000 & 3350. \end{bmatrix}$
1091	$\begin{bmatrix} 3.84 & 3.84 & -3.84 & -3.84 \\ 26.0 & -26.0 & -26.0 & 26.0 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 59.1 & 0.000 & 0.000 \\ 0.000 & 2710. & 0.000 \\ 0.000 & 0.000 & 3.11 \end{bmatrix}$
5003	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ -81.1 & 81.1 & 81.1 & -81.1 \\ 19.6 & 19.6 & -19.6 & -19.6 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 1.42 \times 10^{-14} & 0.000 \\ 1.42 \times 10^{-14} & 26300. & 0.000 \\ 0.000 & 0.000 & 1530. \end{bmatrix}$
5011	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ 31.3 & -31.3 & -31.3 & 31.3 \\ 17.8 & 17.8 & -17.8 & -17.8 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 3.55 \times 10^{-15} & 0.000 \\ 3.55 \times 10^{-15} & 3910. & 0.000 \\ 0.000 & 0.000 & 1270. \end{bmatrix}$
5023	$\begin{bmatrix} 54.9 & 54.9 & -54.9 & -54.9 \\ -0.881 & 0.881 & -0.881 & 0.881 \\ 67.1 & -67.1 & -67.1 & 67.1 \end{bmatrix}$	$\begin{bmatrix} 12100. & 0.000 & 0.000 \\ 0.000 & 3.11 & 0.000 \\ 0.000 & 0.000 & 18000. \end{bmatrix}$

d	B	BB^T
5039	$\begin{bmatrix} 4.61 & 4.61 & -4.61 & -4.61 \\ 0.881 & -0.881 & 0.881 & -0.881 \\ 46.9 & -46.9 & -46.9 & 46.9 \end{bmatrix}$	$\begin{bmatrix} 85.0 & 0.000 & 0.000 \\ 0.000 & 3.11 & 7.11 \times 10^{-15} \\ 0.000 & 7.11 \times 10^{-15} & 8790. \end{bmatrix}$
5051	$\begin{bmatrix} -0.881 & 0.881 & -0.881 & 0.881 \\ 36.4 & 36.4 & -36.4 & -36.4 \\ -82.0 & 82.0 & 82.0 & -82.0 \end{bmatrix}$	$\begin{bmatrix} 3.11 & 0.000 & 0.000 \\ 0.000 & 5290. & 0.000 \\ 0.000 & 0.000 & 26900. \end{bmatrix}$
5059	$\begin{bmatrix} 0.881 & -0.881 & 0.881 & -0.881 \\ -7.79 & 7.79 & 7.79 & -7.79 \\ 49.7 & 49.7 & -49.7 & -49.7 \end{bmatrix}$	$\begin{bmatrix} 3.11 & -8.88 \times 10^{-16} & 0.000 \\ -8.88 \times 10^{-16} & 243. & 0.000 \\ 0.000 & 0.000 & 9890. \end{bmatrix}$
5087	$\begin{bmatrix} 81.8 & -81.8 & -81.8 & 81.8 \\ 22.5 & 22.5 & -22.5 & -22.5 \\ 0.881 & -0.881 & 0.881 & -0.881 \end{bmatrix}$	$\begin{bmatrix} 26800. & 0.000 & 1.42 \times 10^{-14} \\ 0.000 & 2020. & 0.000 \\ 1.42 \times 10^{-14} & 0.000 & 3.11 \end{bmatrix}$
5099	$\begin{bmatrix} 11.9 & 11.9 & -11.9 & -11.9 \\ 49.9 & -49.9 & -49.9 & 49.9 \\ -0.881 & 0.881 & -0.881 & 0.881 \end{bmatrix}$	$\begin{bmatrix} 568. & 0.000 & 0.000 \\ 0.000 & 9950. & 7.11 \times 10^{-15} \\ 0.000 & 7.11 \times 10^{-15} & 3.11 \end{bmatrix}$

Table 2: Selected Units

d	$\mathcal{O}_K^\times/\{\pm 1\};\ a=\sqrt{2}, b=\sqrt{d}$
3	$\left\langle \frac{1}{2}ab+\frac{1}{2}a, a-1, a+b \right\rangle$
7	$\left\langle 2a-b, \frac{1}{2}ab+\frac{3}{2}a, a+1 \right\rangle$
11	$\left\langle \frac{1}{2}ab+\frac{3}{2}a, 7a+3b, a+1 \right\rangle$
19	$\left\langle a-1, \frac{3}{2}ab+\frac{13}{2}a, 3a-b \right\rangle$
23	$\left\langle \frac{1}{2}ab+\frac{5}{2}a, a+1, 78a+23b \right\rangle$
31	$\left\langle a+1, 4a+b, \frac{7}{2}ab+\frac{39}{2}a \right\rangle$
43	$\left\langle \frac{9}{2}ab+\frac{59}{2}a, 51a-11b, a-1 \right\rangle$
47	$\left\langle \frac{1}{2}ab+\frac{7}{2}a, a+1, 732a-151b \right\rangle$
59	$\left\langle a-1, \frac{3}{2}ab+\frac{23}{2}a, 277a+51b \right\rangle$
67	$\left\langle \frac{27}{2}ab+\frac{221}{2}a, a+1, 191a+33b \right\rangle$
71	$\left\langle \frac{7}{2}ab+\frac{59}{2}a, 6a+b, a-1 \right\rangle$
79	$\left\langle a+1, \frac{1}{2}ab+\frac{9}{2}a, 44a-7b \right\rangle$
83	$\left\langle 20621a-3201b, \frac{1}{2}ab+\frac{9}{2}a, a-1 \right\rangle$
103	$\left\langle \frac{47}{2}ab+\frac{477}{2}a, a+1, 122a+17b \right\rangle$
107	$\left\langle \frac{3}{2}ab+\frac{31}{2}a, a+1, 416941a+57003b \right\rangle$
127	$\left\langle \frac{193}{2}ab+\frac{2175}{2}a, a+1, 8a+b \right\rangle$
131	$\left\langle a-1, \frac{9}{2}ab+\frac{103}{2}a, 5123a+633b \right\rangle$
139	$\left\langle \frac{747}{2}ab+\frac{8807}{2}a, a-1, 25a-3b \right\rangle$
151	$\left\langle a-1, \frac{3383}{2}ab+\frac{41571}{2}a, 1034a+119b \right\rangle$
163	$\left\langle \frac{627}{2}ab+\frac{8005}{2}a, a-1, 9a+b \right\rangle$
167	$\left\langle 3993882a-437071b, a+1, \frac{1}{2}ab+\frac{13}{2}a \right\rangle$
179	$\left\langle \frac{153}{2}ab+\frac{2047}{2}a, a+1, 210107a-22209b \right\rangle$

d	$\mathcal{O}_K^\times/\{\pm1\};\ a=\sqrt{2}, b=\sqrt{d}$
191	$\left\langle a-1, \frac{217}{2}ab+\frac{2999}{2}a, 203100a+20783b\right\rangle$
199	$\left\langle a+1, 10a+b, \frac{9041}{2}ab+\frac{127539}{2}a\right\rangle$
211	$\left\langle 1325a+129b, a+1, \frac{36321}{2}ab+\frac{527593}{2}a\right\rangle$
223	$\left\langle 5248a-497b, \frac{1}{2}ab+\frac{15}{2}a, a-1\right\rangle$
227	$\left\langle 65030839a-6104097b, a+1, \frac{1}{2}ab+\frac{15}{2}a\right\rangle$
239	$\left\langle a-1, \frac{161}{2}ab+\frac{2489}{2}a, 20107956a-1839433b\right\rangle$
251	$\left\langle 30953a+2763b, a-1, \frac{121}{2}ab+\frac{1917}{2}a\right\rangle$
263	$\left\langle 4584105462a-399752993b, a-1, \frac{23}{2}ab+\frac{373}{2}a\right\rangle$
271	$\left\langle 1036a+89b, \frac{20687}{2}ab+\frac{340551}{2}a, a-1\right\rangle$
283	$\left\langle a+1, 4889a+411b, \frac{699}{2}ab+\frac{11759}{2}a\right\rangle$
1019	$\left\langle a-1, 63391078088730047a-2808381113280699b, \frac{77307}{2}ab+\frac{2467777}{2}a\right\rangle$
1031	$\left\langle \frac{795073}{2}ab+\frac{25529149}{2}a, 11906243381514a+524397268831b, a+1\right\rangle$
1039	$\left\langle a+1, 57460a-2521b, \frac{688971723361}{2}ab+\frac{22207985837961}{2}a\right\rangle$
1051	$\left\langle a-1, \frac{953426773899}{2}ab+\frac{30909266676193}{2}a, 102428683a+4468227b\right\rangle$
1063	$\left\langle \frac{1281361}{2}ab+\frac{41777085}{2}a, 843640322a-36593647b, a+1\right\rangle$
1087	$\left\langle a-1, \frac{1}{2}ab+\frac{33}{2}a, 1296174088928a-55598562271b\right\rangle$
1091	$\left\langle \frac{1}{2}ab+\frac{33}{2}a, 72655550323a-3110795193b, a-1\right\rangle$