Flat 2D Tori with Sparse Spectra

Michael Taylor

Abstract. We identify a class of 2D flat tori $\mathbb{T}_\omega$, quotients of the plane by certain lattices, on which the Laplace operator has spectrum contained in the set of integers $\mathbb{Z}$, as a sparse subset, i.e., a subset of density 0.

1. Introduction

The ring of Gaussian integers forms a nice lattice in the complex plane:

$$\mathbb{Z}[\sqrt{-1}] = \{j\sqrt{-1} + k : j, k \in \mathbb{Z}\}. \tag{1.1}$$

The problem of counting how many elements of $\mathbb{Z}[\sqrt{-1}]$ lie in a disk $D_R = \{z \in \mathbb{C} : |z| \le R\}$ is an old problem, whose mysteries have by no means been exhausted. The following two phenomena indicate some of the subtleties involved. Set

$$\mathcal{N}(k) = \#\{\zeta \in \mathbb{Z}[\sqrt{-1}] : |\zeta|^2 = k\}. \tag{1.2}$$

The phenomena are
(A) High multiplicity:

$$\sup_k \mathcal{N}(k) = \infty, \tag{1.3}$$

and
(B) Sparseness:

$$\mathcal{N}(k) = 0 \ \text{ except for a set of integers } k \text{ of density zero.} \tag{1.4}$$

It is easy to see that (1.4) ⇒ (1.3), since

$$\sum_{k\le K} \mathcal{N}(k) \sim \pi K, \quad \text{as} \ \ K \to \infty.$$

Actually (1.3) has a very short and simple proof, which extends to a broad class of lattices in $\mathbb{C}$. It goes like this. Take $m \in \mathbb{Z}^+$ large and consider

$$\zeta = m + \sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]. \tag{1.5}$$

Then $\zeta = \sqrt{m^2+1}e^{i\theta}$ with $\theta \in (0, \pi/\kappa)$, where the integer $\kappa = \kappa(m) \to \infty$ as $m \to +\infty$. Hence

$$\zeta^j \overline{\zeta}^{\kappa - j}, \quad 0 \le j \le \kappa, \tag{1.6}$$

are distinct elements of $\mathbb{Z}[\sqrt{-1}]$ with the same square norm, so $\mathcal{N}((m^2+1)^\kappa) \ge \kappa$. This gives (1.3).

The proof of (1.4) makes use of more structure, including the fact that

$$\mathbb{Z}[\sqrt{-1}] \text{ is a Unique Factorization Domain (UFD).} \tag{1.7}$$

For this proof, take $k \in \mathbb{N}$ and factor it into prime integers,

$$k = p_1^{j_1} \cdots p_M^{j_M}, \tag{1.8}$$

with $p_1, \dots, p_M$ distinct primes in $\mathbb{Z}$. If $\zeta \in \mathbb{Z}[\sqrt{-1}]$ and $k = |\zeta|^2$, factor ζ into primes in $\mathbb{Z}[\sqrt{-1}]$,

$$\zeta = \gamma_1^{i_1} \cdots \gamma_L^{i_L}, \quad \text{so} \quad k = |\gamma_1|^{2i_1} \cdots |\gamma_L|^{2i_L}. \tag{1.9}$$

It is readily established that

$$\gamma \in \mathbb{Z}[\sqrt{-1}] \Longrightarrow |\gamma|^2 \text{ not congruent to 3, mod 4.} \tag{1.10}$$

Now when the integer primes in (1.8) are factored into primes in $\mathbb{Z}[\sqrt{-1}]$, the associated factorization of k into primes in $\mathbb{Z}[\sqrt{-1}]$ must agree with (1.9), up to units, and we deduce that

$$\mathcal{N}(k) = 0 \text{ unless } j_\nu \text{ is even in (1.8) whenever } p_\nu \equiv 3 \text{ mod } 4. \tag{1.11}$$

Dirichlet's theorem on primes in an arithmetic progression implies that the set of primes $\equiv 3$ mod 4 has density 1/2 in the set of all primes, so (1.11) implies (1.4).

Our goal here is to establish analogues of (1.3) and especially (1.4), for a larger class of lattices, generated by 1 and $\omega \in \mathbb{C} \setminus \mathbb{R}$:

$$\mathcal{L}_\omega = \{j\omega + k : j, k \in \mathbb{Z}\}, \tag{1.12}$$

using

$$\mathcal{N}_\omega(k) = \#\{\zeta \in \mathcal{L}_\omega : |\zeta|^2 = k\}. \tag{1.13}$$

The lattices we study will have the property that $|\zeta|^2 \in \mathbb{Z}^+$ for all $\zeta \in \mathcal{L}_\omega$. Whenever $\mathcal{L}_\omega$ is a ring,

$$\mathcal{L}_\omega = \mathbb{Z}[\omega], \tag{1.14}$$

we have

$$\sup_k \mathcal{N}_\omega(k) = \infty. \tag{1.15}$$

This again has a short, simple proof, which we give in §2. In such a case, we can take either

$$\omega = \sqrt{-m}, \quad m \in \mathbb{N}, \tag{1.16}$$

or

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D \equiv 3 \mod 4. \tag{1.17}$$

(We review this well known result in §2.) The major goal of this paper is to identify lattices $\mathcal{L}_\omega$ for which

$$\mathcal{N}_\omega(k) = 0 \text{ except for a set } k \text{ of integers of density zero.} \tag{1.18}$$

When (1.18) holds, we say $\mathcal{L}_\omega$ is *sparse.* We will show that (1.18) holds whenever $\mathcal{L}_\omega$ is a ring $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\omega]$ is a UFD. These lattices are classified as follows.

Theorem A. *The lattice $\mathcal{L}_\omega$ is a UFD provided either*

$$\omega = \sqrt{-1}, \quad \sqrt{-2}, \tag{1.19}$$

or

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D = 3,\ 7,\ 11, \tag{1.20}$$

or

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D = 19,\ 43,\ 67,\ 163. \tag{1.21}$$

We divide the cases above because in cases (1.19)–(1.20) the rings $\mathbb{Z}[\omega]$ are actually Principal Ideal Domains (PIDs), and the demonstration of this is fairly elementary. The demonstration that $\mathbb{Z}[\omega]$ is a UFD for ω in (1.21) is harder. Final results are due to H. Stark; see [HW] and Chapter 6 of [MM] for further references. Our main result is the following.

Theorem B. *In all cases of ω covered by Theorem A, the sparseness result (1.18) holds.*

The results (1.15) and (1.18), when they hold, can be cast as results about the spectrum of the Laplace operator on flat 2D tori. In fact, given a lattice $\mathcal{L}_\omega$ as in (1.12), we can form the dual lattice

$$\mathcal{L}'_\omega = \{z \in \mathbb{C} : \operatorname{Re} z\overline{\zeta} \in \mathbb{Z}, \forall\, \zeta \in \mathcal{L}_\omega\}, \tag{1.22}$$

and the associated torus

$$\mathbb{T}_\omega = \mathbb{C}/2\pi\mathcal{L}'_\omega. \tag{1.23}$$

If Δ_ω denotes the Laplace operator on $\mathbb{T}_\omega$, it has eigenfunctions

$$e_\zeta(z) = e^{\sqrt{-1}\,\mathrm{Re}\, z\bar{\zeta}}, \quad \zeta \in \mathcal{L}_\omega, \tag{1.24}$$

satisfying

$$\Delta_\omega e_\zeta = -|\zeta|^2 e_\zeta. \tag{1.25}$$

The functions (1.14) form an orthogonal basis of $L^2(\mathbb{T}_\omega)$. Hence

$$\mathrm{Spec}(-\Delta_\omega) = \{|\zeta|^2 : \zeta \in \mathcal{L}_\omega\}, \tag{1.26}$$

i.e.,

$$k \in \mathrm{Spec}(-\Delta_\omega) \Longleftrightarrow \mathcal{N}_\omega(k) > 0. \tag{1.27}$$

Furthermore,

$$\text{multiplicity of } k \text{ in } \mathrm{Spec}(-\Delta_\omega) = \mathcal{N}_\omega(k). \tag{1.28}$$

Thus, for example, Theorem B implies that for each ω in (1.19)–(1.21), $-\Delta_\omega$ has sparse spectrum in $\mathbb{Z}^+$.

Such sparse spectral results appear in [P] for the Laplace operator on an equilateral triangle, with Dirichlet or Neumann boundary conditions, where arithmetic in $\mathbb{Z}[e^{\pi i/3}]$ is used to specify these spectra. The paper [P] stimulated our work here.

This paper proceeds as follows. Section 2 gives background on lattices in $\mathbb{C}$ that are rings and records a simple proof of (1.15), parallel to the proof of (1.3) given above. In §3 we specialize to the UFDs listed in Theorem A, and in §4 prove Theorem B. This proof is somewhat parallel to the proof of (1.4) sketched above, but a number of details require elaboration. In particular, we need the following variant of (1.9). For each ω in (1.19)–(1.21), there are numbers $L \in \mathbb{N}$ and $\ell \in \{1, \dots, L-1\}$, relatively prime to L, such that

$$\zeta \in \mathbb{Z}[\omega] \Longrightarrow |\zeta|^2 \ \text{ not congruent to } \ell \bmod L. \tag{1.29}$$

As mentioned above, for $\omega = \sqrt{-1}$, this holds with $L = 4,\ \ell = 3$. A straightforward approach to this is to let j and k run independently over $\{0, 1, 2, \dots, L-1\}$, set $\zeta = j\omega + k$, calculate $|\zeta|^2$ and reduce mod L, and see if the set of residue classes is exhausted. Such an approach can be readily carried out by hand for $\omega = \sqrt{-2}$ and for $\omega = (1+\sqrt{-3})/2$. For other values of ω in (1.20)–(1.21), such a hand calculation becomes very laborious. We have written a C program to do the calculation. The program verifies (1.29) for all ω in (1.20)–(1.21), with

$$L = D. \tag{1.30}$$

In Appendix A we present the C program and discuss how it works.

In turn, the output from this program allowed me to see phenomena that led to a non-computer proof of (1.29). This proof is also presented in §4.

In §5 we mention some unanswered questions.

Acknowledgments. Thanks to Rafe Mazzeo for interesting conversations on the topic of this paper, for for relaying conversations with Brian Conrad on these matters. This work was begun while I was visiting MSRI and was supported by NSF grant DMS-0758320.

2. Lattices in $\mathbb{C}$ that are rings

Let $\omega \in \mathbb{C} \setminus \mathbb{R}$ and let $\mathcal{L}_\omega$ be the lattice generated by 1 and ω:

$$\mathcal{L}_\omega = \{j\omega + k : j, k \in \mathbb{Z}\}. \tag{2.1}$$

The set $\mathcal{L}_\omega$ is a ring provided $\omega^2 \in \mathcal{L}_\omega$, i.e., provided

$$\omega^2 = b\omega + c, \quad \text{for some} \ \ b, c \in \mathbb{Z}. \tag{2.2}$$

Standard notation for $\mathcal{L}_\omega$ in this case is $\mathbb{Z}[\omega]$. Given $b, c \in \mathbb{Z}$, the solutions to (2.2) are

$$\omega = \frac{b}{2} \pm \frac{1}{2}\sqrt{b^2 + 4c}. \tag{2.3}$$

To say $\omega \notin \mathbb{R}$ is to say $b^2 + 4c < 0$. In such a case

$$|\omega|^2 = \frac{b^2}{4} + \frac{|b^2 + 4c|}{4} = \frac{b^2}{4} - \frac{b^2 + 4c}{4} = -c, \tag{2.4}$$

which is an integer. More generally,

$$\begin{aligned} |j\omega + k|^2 &= |\omega|^2 j^2 + k^2 + jk(\omega + \overline{\omega}) \\ &= |\omega|^2 j^2 + k^2 + bjk, \end{aligned} \tag{2.5}$$

which is an integer.

From here on we assume $\omega \in \mathbb{C} \setminus \mathbb{R}$ satisfies (2.2). Note that for each $j \in \mathbb{Z}$, $\{1, \omega - j\}$ generates the same lattice as $\{1, \omega\}$, and $\mathbb{Z}[\omega - j] = \mathbb{Z}[\omega]$. (Also note:(2.2) $\Rightarrow (\omega-j)^2 = (a-2j)\omega+(b+j^2) = (a-2j)(\omega-j)+(b-j^2+aj)$.) Also there exists j such that $\omega_0 = \omega - j$ has the property

$$\operatorname{Re}\omega_0 = 0 \quad \text{or} \quad \frac{1}{2}. \tag{2.6}$$

Such ω_0 has the property

$$|\omega_0| = \min\{|\zeta| : \zeta \in \mathbb{Z}[\omega] \setminus \mathbb{R}\}. \tag{2.7}$$

Without loss of generality, we can relabel ω_0 as ω and hence arrange that ω has this length-minimizing property. In case $\operatorname{Re}\omega = 0$, ω (or $\overline{\omega}$) is as in (1.16), and in case $\operatorname{Re}\omega = 1/2$, ω (or $\overline{\omega}$) is as in (1.17), with

$$D = -4c - b^2 = 4|\omega|^2 - 1, \tag{2.8}$$

in light of (2.3)–(2.4), since now $b = 1$. Hence

$$\frac{D+1}{4} = |\omega|^2 = a \tag{2.9}$$

is an integer, and (2.5) becomes

$$|j\omega + k|^2 = aj^2 + k^2 + jk. \tag{2.10}$$

Here is one easy consequence of these calculations.

Proposition 2.1. *If there exists $\zeta \in \mathbb{Z}[\omega] \setminus \mathbb{R}$ such that $|\zeta| = 1$, then $\mathbb{Z}[\omega] = \mathbb{Z}[\zeta]$, and*

$$\zeta = \pm i, \quad \pm e^{\pm\pi i/3}, \quad \textit{or} \quad \pm\, e^{\pm 2\pi i/3}. \tag{2.11}$$

Here is another.

Proposition 2.2. *If $\zeta \in \mathbb{Z}[\omega]$, then $\overline{\zeta} \in \mathbb{Z}[\omega]$.*

Proof. It suffices to show that $\overline{\omega}_0 \in \mathbb{Z}[\omega]$, with $\omega_0 = \omega - j$ as in (2.10). Indeed, $\operatorname{Re}\omega_0 = 0 \Rightarrow \overline{\omega}_0 = -\omega_0$ and $\operatorname{Re}\omega_0 = 1/2 \Rightarrow \overline{\omega}_0 = -\omega_0 + 1$.

We can now prove (1.15).

Proposition 2.3. *Whenever $\mathcal{L}_\omega$ is a ring,*

$$\sup_k \mathcal{N}_\omega(k) = \infty. \tag{2.12}$$

Proof. Take $m \in \mathbb{Z}^+$ large and consider

$$\zeta = m + \omega \in \mathbb{Z}[\omega]. \tag{2.13}$$

Then $\zeta = re^{i\theta}$ with $r > 0$ and either $\theta \in (0, \pi/\kappa)$ or $\theta \in (-\pi/\kappa, 0)$, where the integer $\kappa = \kappa(m) \to \infty$ as $m \to +\infty$. Hence (via Proposition 2.2)

$$\zeta^j \overline{\zeta}^{\kappa-j}, \quad 0 \le j \le \kappa, \tag{2.14}$$

are distinct elements of $\mathbb{Z}[\omega]$ with the same square norm, so we have (2.12).

Remark. Brian Conrad has shown me an elegant proof of the following very strong converse to Proposition 2.3.

Theorem C. *(Conrad) Let $\mathcal{L}_\omega$ be a lattice in $\mathbb{C}$ of the form (1.12), and assume*

$$\sup_k \mathcal{N}_\omega(k) \geq 5. \tag{2.15}$$

Then $\mathcal{L}_\omega$ contains a lattice of this form that is a ring.

Note that $\sup_k \mathcal{N}_\omega(k) \geq 4$ whenever ω is purely imaginary.

We recall that a lattice $\mathcal{L} \subset \mathbb{C}$ is said to admit *complex multiplication* provided there exists $\gamma \in \mathbb{C} \setminus \mathbb{R}$ such that

$$\zeta \in \mathcal{L} \Longrightarrow \gamma\zeta \in \mathcal{L}. \tag{2.16}$$

If $1 \in \mathcal{L}$, this implies $\gamma \in \mathcal{L}$, and furthermore,

$$\mathbb{Z}[\gamma] \subset \mathcal{L}. \tag{2.17}$$

Hence $\mathcal{L}$ contains a lattice that is a ring.

We next discuss factorization of elements of $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ into primes. First, some definitions. We say $\zeta \in \mathbb{Z}[\omega]$ is a *unit* if also $\zeta^{-1} \in \mathbb{Z}[\omega]$. Note that in such a case $|\zeta| \geq 1$ and $|\zeta^{-1}| \geq 1$, so in fact if ζ is a unit we must have $|\zeta| = 1$. The numbers ± 1 are always units in $\mathbb{Z}[\omega]$. Clearly $\pm i$ are units in $\mathbb{Z}[i]$; also $\pm\omega$ are units in $\mathbb{Z}[\omega]$ in the other cases of (2.11), as one sees from

$$\begin{aligned} \omega^2 = \pm\omega - 1 &\Longrightarrow \omega = \pm 1 - \omega^{-1} \\ &\Longrightarrow \omega^{-1} = \pm 1 - \omega. \end{aligned} \tag{2.18}$$

These are all the cases where one has units other than ± 1. To see this, we note the following.

Proposition 2.4. *An element $\zeta \in \mathbb{Z}[\omega]$ is a unit if and only if $|\zeta| = 1$.*

Proof. The only point to examine is the consequence of having $\zeta \in \mathbb{Z}[\omega] \setminus \mathbb{R}$ with $|\zeta| = 1$. For this we can just apply Proposition 2.1.

Next, given $\zeta \in \mathbb{Z}[\omega]$, we say ζ is *prime* provided ζ is not a unit and one has the implication

$$\zeta = \zeta_1\zeta_2,\ \zeta_j \in \mathbb{Z}[\omega] \Longrightarrow \zeta_1 \ \text{ or } \ \zeta_2 \ \text{ is a unit.} \tag{2.19}$$

The following is an extension from $\mathbb{Z}$ to $\mathbb{Z}[\omega]$ of half of the Fundamental Theorem of Arithmetic.

Proposition 2.5. *Given $\zeta \in \mathbb{Z}[\omega]$, not a unit, we can write*

$$\zeta = \gamma_1 \cdots \gamma_n, \quad \gamma_j \ \textit{primes in} \ \mathbb{Z}[\omega]. \tag{2.20}$$

Proof. If ζ is prime, we are done. If not, write

$$\zeta = \zeta_1 \zeta_2, \quad \zeta_j \in \mathbb{Z}[\omega], \ \text{not units.} \tag{2.21}$$

By Proposition 2.4, $|\zeta_j| > 1$, so each $|\zeta_j| < |\zeta|$. The proof now follows by induction on $|\zeta|^2 \in \mathbb{N}$.

Remark. A byproduct of this argument is the implication

$$\zeta \in \mathbb{Z}[\omega], \ |\zeta|^2 \ \text{prime in} \ \mathbb{Z} \Longrightarrow \zeta \ \text{prime in} \ \mathbb{Z}[\omega]. \tag{2.22}$$

The other half of the Fundamental Theorem of Arithmetic (in $\mathbb{Z}$) is that the factorization of an element $m \in \mathbb{Z}$ into primes (in $\mathbb{Z}$) is unique, up to units. This property might or might not hold in $\mathbb{Z}[\omega]$. If $\mathbb{Z}[\omega]$ has this property, we say it is a unique factorization domain (UFD). We will wait until §3 to discuss special properties of lattices in $\mathbb{C}$ that are UFDs. We continue to deal with general lattices in $\mathbb{C}$ that are rings.

The following describes how a prime in $\mathbb{Z}$ might factor in $\mathbb{Z}[\omega]$.

Proposition 2.6. *Let p be a prime in $\mathbb{Z}$. Then either p is prime in $\mathbb{Z}[\omega]$ or*

$$p = |\zeta|^2, \quad \zeta \in \mathbb{Z}[\omega] \ \textit{prime.} \tag{2.23}$$

Proof. Assume p is not prime in $\mathbb{Z}[\omega]$. Then write

$$p = \zeta\eta, \quad \zeta, \eta \in \mathbb{Z}[\omega], \ \text{not units.} \tag{2.24}$$

We have

$$p^2 = |\zeta|^2 |\eta|^2, \tag{2.25}$$

and hence

$$|\zeta|^2 = |\eta|^2 = p. \tag{2.26}$$

By (2.22) this implies both ζ and η are primes in $\mathbb{Z}[\omega]$. Also (2.24) implies η is a positive real multiple of $\overline{\zeta}$, say $\eta = r\overline{\zeta}$, and (2.26) implies $|r| = 1$; hence $r = 1$. This gives (2.23).

3. Lattices in $\mathbb{C}$ that are UFDs

Throughout this section (except in the statements of Propositions 3.1 and 3.2) we assume $\mathcal{L}_\omega$ is a lattice of the form (2.1) such that $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ is a UFD. As stated in Theorem A, ω could have the form

$$\sqrt{-1}, \quad \sqrt{-2}, \tag{3.1}$$

or

$$\frac{1}{2}+\frac{1}{2}\sqrt{-D}, \quad D=3,\ 7,\ 11, \tag{3.2}$$

or

$$\frac{1}{2}+\frac{1}{2}\sqrt{-D}, \quad D=19,\ 43,\ 67,\ 163. \tag{3.3}$$

As we mentioned in §1, in cases (3.1)–(3.2), $\mathbb{Z}[\omega]$ is actually a PID, i.e., each ideal $\mathcal{I} \subset \mathbb{Z}[\omega]$ is of the form

$$(\alpha) = \{(j\omega+k)\alpha : j,k \in \mathbb{Z}\}, \tag{3.4}$$

for some $\alpha \in \mathcal{I}$. This can be seen by applying the following criterion.

Proposition 3.1. *Let $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ be a lattice in $\mathbb{C}$ of the form (2.1) that is a ring. If*

$$\operatorname{dist}(\zeta, \mathbb{Z}[\omega]) < 1, \quad \forall\, \zeta \in \mathbb{C}, \tag{3.5}$$

then $\mathbb{Z}[\omega]$ is a PID.

Proof. Given an ideal $\mathcal{I} \subset \mathbb{Z}[\omega] = \mathcal{L}_\omega$, pick $\alpha \in \mathcal{I} \setminus 0$ to minimize $|\alpha|$. If $(\alpha) \neq \mathcal{I}$, there must exist $\beta \in \mathcal{I},\ \beta \notin (\alpha)$. Given such β, pick $\alpha_1 \in (\alpha)$ to minimize $|\beta - \alpha_1|$. Thus $\beta_1 = \beta - \alpha_1 \in \mathcal{I} \setminus (\alpha)$. We necessarily have $|\beta_1| \geq |\alpha|$. We have a contradiction if the following property holds:

$$\forall\, \zeta \in \mathbb{C}, \quad \operatorname{dist}(\zeta, (\alpha)) < |\alpha|, \tag{3.6}$$

which in turn follows from (3.5).

The reader can verify that (3.5) holds for all ω in (3.1)–(3.2). For the reader's convenience, we record the standard proof of the following.

Proposition 3.2. *If $\mathbb{Z}[\omega]$ is a PID, then it is a UFD.*

Proof. Uniqueness follows readily once one has the following property.

$$p, a, b, \in \mathbb{Z}[\omega],\ p \ \text{ prime},\ p|ab \Longrightarrow p|a \ \text{ or } \ p|b. \tag{3.7}$$

Here $p|ab$ (*p divides ab*) means

$$ab = pc \quad \text{for some} \quad c \in \mathbb{Z}[\omega]. \tag{3.8}$$

To prove (3.7), assume p does not divide a, and let $\mathcal{I} = (p, a)$ to be the ideal in $\mathbb{Z}[\omega]$ generated by p and a. If $\mathbb{Z}[\omega]$ is a PID, $\mathcal{I} = (q)$ for some $q \in \mathbb{Z}[\omega]$, hence $p = qd$ for some $d \in \mathbb{Z}[\omega]$, so either q or d is a unit.

If d were a unit, we could take $q = p$, $d = 1$. We also have $a = qe$ for some $e \in \mathbb{Z}[\omega]$. If $q = p$, then $p|a$, which we are assuming is not the case. Hence q must be a unit. This implies $\mathcal{I} = \mathbb{Z}[\omega]$, hence

$$\zeta p + \eta a = 1 \quad \text{for some} \quad \zeta, \eta \in \mathbb{Z}[\omega]. \tag{3.9}$$

Hence

$$\zeta pb + \eta ab = b. \tag{3.10}$$

Since p divides the left side of (3.10), it must divide the right side. This gives (3.7).

Remark. We mention that

$$\mathbb{Z}[\sqrt{-5}] \quad \text{is not a UFD.} \tag{3.11}$$

In fact, 2 and 3 are prime in $\mathbb{Z}[\sqrt{-5}]$ (exercise), but

$$\begin{aligned} 2 \cdot 3 = 6 &= (1 + \sqrt{-5})(1 - \sqrt{-5}), \\ 3 \cdot 3 = 9 &= (2 + \sqrt{-5})(2 - \sqrt{-5}). \end{aligned} \tag{3.12}$$

Thus (3.7) fails for $\mathbb{Z}[\sqrt{-5}]$.

We now establish some further results about prime factorization for lattices in $\mathbb{C}$ that are UFDs. The following result complements Proposition 2.6.

Proposition 3.3. *Assume $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ is a UFD. Let γ be a prime in $\mathbb{Z}[\omega]$. Then either γ (times a unit) belongs to $\mathbb{Z}$ and is a prime in $\mathbb{Z}$, or $|\gamma|^2$ is a prime in $\mathbb{Z}$.*

Proof. Set $p = |\gamma|^2$. If p is not a prime in $\mathbb{Z}$, we have

$$\gamma\overline{\gamma} = p = q_1 \cdots q_K, \quad q_j \in \mathbb{Z} \ \text{ primes}, \ K \geq 2. \tag{3.13}$$

In turn, each q_j has a factorization into primes in $\mathbb{Z}[\omega]$. If γ is a prime in $\mathbb{Z}[\omega]$, so is $\overline{\gamma}$. Given that $\mathbb{Z}[\omega]$ is a UFD, this forces $K = 2$ and q_j primes in $\mathbb{Z}[\omega]$. This in turm forces $\gamma = q_1$, up to a unit.

We are now in a position to establish the following, which will play a key role in §4.

Proposition 3.4. *Assume $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ is a UFD. Let $k \ge 2$ be an integer, and set*

$$k = p_1^{j_1} \cdots p_M^{j_M}, \tag{3.14}$$

Where $p_1, \dots, p_M$ are distinct primes in $\mathbb{Z}$. Then there exists $\zeta \in \mathbb{Z}[\omega]$ such that

$$k = |\zeta|^2 \tag{3.15}$$

if and only if each p_ν for which j_ν in (3.14) is odd is composite in $\mathbb{Z}[\omega]$.

Proof. If the stated conditions hold in (3.14), the fact that k has the form (3.15) (whether or not $\mathbb{Z}[\omega]$ is a UFD) follows readily from Proposition 2.6. It remains to establish the converse. Thus, suppose k has the form (3.15). Factor ζ into primes in $\mathbb{Z}[\omega]$:

$$\zeta = \gamma_1^{i_1} \cdots \gamma_L^{i_L}. \tag{3.16}$$

Then

$$k = |\gamma_1|^{2i_1} \cdots |\gamma_L|^{2i_L}. \tag{3.17}$$

By Proposition 3.3, for each ν, either $|\gamma_\nu|^2$ is a prime p_ν in $\mathbb{Z}$ (which is then composite in $\mathbb{Z}[\omega]$), or γ_ν times a unit is a prime in $\mathbb{Z}$, so $|\gamma_\nu|^2$ is the square of a prime in $\mathbb{Z}$. This yields the stated conditions on the factorization of k in (3.14).

Remark. The conclusion of Proposition 3.4 fails for $\mathbb{Z}[\sqrt{-5}]$, as illustrated by

$$\begin{aligned} 6 = 2 \cdot 3; \quad 6 &= |1 + \sqrt{-5}|^2, \\ 21 = 3 \cdot 7; \quad 21 &= |1 + 2\sqrt{-5}|^2. \end{aligned} \tag{3.18}$$

4. Sparseness

Our goal here is to prove Theorem B, i.e., whenever ω is of the form (3.1)–(3.3), the lattice $\mathcal{L}_\omega$ has the property that

$$\Lambda_\omega = \{|\zeta|^2 : \zeta \in \mathcal{L}_\omega\} \tag{4.1}$$

has density 0 in $\mathbb{Z}^+$. In light of Proposition 3.4, what we need to know is that lots of primes in $\mathbb{Z}$ are also primes in $\mathbb{Z}[\omega]$. The following result moves toward that goal.

Proposition 4.1. *Assume $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ is a UFD. If there exist $L \in \mathbb{Z}^+$, $\ell \in \{1, \dots, L-1\}$, relatively prime to L, such that*

$$\zeta \in \mathbb{Z}[\omega] \Longrightarrow |\zeta|^2 \neq \ell \ \ mod \ \ L, \tag{4.2}$$

then Λ_ω has density 0 in $\mathbb{Z}^+$.

Proof. By Proposition 3.4, if $k \in \mathbb{Z}^+$ has the form

$$k = p_1^{j_1} \cdots p_M^{j_M}, \tag{4.3}$$

with $p_1, \dots, p_M$ distinct primes in $\mathbb{Z}$, and if $k \in \Lambda_\omega$, then each p_ν satisfying

$$p_\nu \equiv \ell \mod L \tag{4.4}$$

must have an even exponent in (4.3). By Dirichlet's theorem on primes in an arithmetic progression, the set of primes satisfying (4.4) has positive density ($> 1/L$) in the set of all primes. This implies Λ_ω has density 0 in $\mathbb{Z}^+$, if (4.2) holds.

As mentioned in the introduction, when $\omega = \sqrt{-1}$, (4.2) holds with $L = 4,\ \ell = 3$. When $\omega = \sqrt{-2}$, we have

$$\zeta = j\sqrt{-2} + k \Longrightarrow |\zeta|^2 = 2j^2 + k^2. \tag{4.5}$$

Letting j and k run over $\mathbb{Z}/(8)$, one can check that

$$\zeta \in \mathbb{Z}[\sqrt{-2}] \Longrightarrow |\zeta|^2 \neq 5 \text{ or } 7 \mod 8. \tag{4.6}$$

This covers ω in (3.1). The cases (3.2)–(3.3) are covered by the following.

Proposition 4.2. *If ω is given by (3.2)–(3.3), we can take*

$$L = D, \tag{4.7}$$

and there exists $\ell \in \{1, \dots, L-1\}$ (necessarily relatively prime to L) such that (4.2) holds.

As we have seen in §2, given $D = -1 \mod 4$,

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D} \Longrightarrow |j\omega + k|^2 = aj^2 + k^2 + jk, \tag{4.8}$$

where

$$a = \frac{D+1}{4} \in \mathbb{Z}^+. \tag{4.9}$$

When ω is given by (3.2)–(3.3), we have

$$\begin{aligned} D &= 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163, \quad \text{hence} \\ a &= 1,\ 2,\ 3,\ 5,\ 11,\ 17,\ 41, \quad \text{respectively.} \end{aligned} \tag{4.10}$$

A straightforward approach to Proposition 4.2 would be to let j and k run independently through $\{0,1,\dots,L-1\}$ (with $L=D$), compute aj^2+k^2+jk, and mark off its residue class mod L. After doing this for each such j and k, check whether any elements of $\mathbb{Z}/(L)$ are left. For $D=3$, this involves computing j^2+k^2+jk for 9 pairs (j,k). The reader is invited to do this by hand, and verify that, for $\zeta\in\mathbb{Z}[\omega],\ \omega=(1+\sqrt{-D})/2$,

$$D=3 \Rightarrow |\zeta|^2 \neq 2 \mod 3. \tag{4.11}$$

For larger $L=D$ listed in (4.10), the task of making such calculations by hand would range from tedious (for $D=7$) to way over the top (for $D=163$). Fortunately, it is easy enough to write a C program to do these calculations. We present such a program in Appendix A. Running the program shows that we have, for $\zeta\in\mathbb{Z}[\omega],\ \omega=(1+\sqrt{-D})/2$, the following complements to (4.11):

$$\begin{aligned} D=7 &\Rightarrow |\zeta|^2 \neq 3,5,6 \mod 7, \\ D=11 &\Rightarrow |\zeta|^2 \neq 2,6,7,8,10 \mod 11, \\ D=19 &\Rightarrow |\zeta|^2 \neq 2,3,8,10,12,13,14,15,18 \mod 19, \\ D=43 &\Rightarrow |\zeta|^2 \neq 2,3,5,7,\dots,34,37,39,42 \mod 43, \\ D=67 &\Rightarrow |\zeta|^2 \neq 2,3,5,7,\dots,58,61,63,66 \mod 67, \\ D=163 &\Rightarrow |\zeta|^2 \neq 2,3,5,7,\dots,154,157,159,162 \mod 163. \end{aligned} \tag{4.12}$$

Once we have the sparse lattices $\mathcal{L}_\omega$ for ω in (3.1)–(3.3), we can produce others. If $\mathcal{L}\subset\mathbb{C}$ is any lattice such that

$$\zeta\in\mathcal{L} \Longrightarrow |\zeta|^2\in\mathbb{Z}^+, \tag{4.13}$$

and $\widetilde{\mathcal{L}}\subset\mathcal{L}$ is a sublattice, then clearly

$$\mathcal{L} \text{ sparse} \Longrightarrow \widetilde{\mathcal{L}} \text{ sparse}. \tag{4.14}$$

The next result shows that these lattices all have large multiplicities.

Proposition 4.3. *If $\mathcal{L}\subset\mathbb{C}$ is a lattice satisfying (4.13), then*

$$\mathcal{L} \textit{ sparse} \Longrightarrow \sup_k \mathcal{N}_{\mathcal{L}}(k)=\infty, \tag{4.15}$$

where, for $k \in \mathbb{Z}^+$,

$$\mathcal{N}_{\mathcal{L}}(k) = \#\{\zeta \in \mathcal{L} : |\zeta|^2 = k\}. \tag{4.16}$$

Proof. This is straightforward from the asymptotic result

$$\sum_{k \le K} \mathcal{N}_{\mathcal{L}}(k) \sim \frac{\pi K}{\operatorname{Area}(\mathbb{C}/\mathcal{L})}, \quad \text{as} \quad K \to \infty. \tag{4.17}$$

While Proposition 4.2 is adequate to complete the proof of Theorem B, it is actually a special case of a more general result, which we prove next, without use of a computer program. We were led to this by staring at the results displayed in (4.12) and noticing that the numbers listed as not congruent to $|\zeta|^2$ mod D are precisely those that are not squares in $\mathbb{Z}/(D)$. This suggested the following generalization.

Proposition 4.4. *Let $D \in \mathbb{Z}^+$ be $= 3$ mod 4, and set $\omega = (1 + \sqrt{-D})/2$. Then for each $\zeta \in \mathbb{Z}[\omega]$, there exists $\ell \in \{0, 1, \dots, D-1\}$ such that*

$$|\zeta|^2 = \ell^2 \quad \mathit{mod} \quad D. \tag{4.18}$$

Proof. We have $\zeta = j\omega + k$, with $j, k \in \mathbb{Z}$, and hence $2\zeta = j\sqrt{-D} + (j + 2k)$, so

$$|2\zeta|^2 = (j + 2k)^2 \mod D. \tag{4.19}$$

Pick $\nu \in \{1, \dots, D-1\}$ such that

$$2\nu = 1 \mod D. \tag{4.20}$$

Then, since $|\zeta|^2 = aj^2 + jk + k^2$ and $a = (D+1)/4$ is an integer, we have

$$\begin{aligned} |\zeta|^2 &= |2\nu\zeta|^2 \mod D \\ &= \nu^2 (j + 2k)^2 \mod D, \end{aligned} \tag{4.21}$$

giving (4.18).

5. Further questions

The results presented above leave unanswered a number of questions. For example, consider $\mathcal{L}_\omega = \mathbb{Z}[\omega]$ with

$$\omega = \sqrt{-5}. \tag{5.1}$$

It follows from Proposition 2.3 that $\mathcal{L}_\omega$ has high multiplicities. On the other hand, as we have seen, Proposition 3.4 fails spectacularly in this case, and we have no proof that $\mathcal{L}_\omega$ is sparse. We also have no proof that $\mathcal{L}_\omega$ is not sparse. Is it? It would be interesting to know the answer to this and related questions, such as sparseness of $\mathcal{L}_\omega$ when $\omega = \sqrt{-D},\ D = 13,\ 17,\ 23$, etc. Note that sparseness for $D = 3,\ 7,\ 11,\ 19$ follows from (4.14).

Another mystery has to do with the existence of $\ell \in \{1, \dots, L-1\}$ such that

$$\forall\, j, k \in \mathbb{Z}/(L), \quad aj^2 + k^2 + jk \neq \ell, \quad \text{mod } \ L. \tag{5.2}$$

Guided by our computer program, we were led to show in Proposition 4.4 that this holds whenever

$$L = 4a - 1. \tag{5.3}$$

On the other hand, numerous runs indicate that (5.2) never holds when

$$L = 4a - 3, \quad \text{or} \quad L = 4a + 1, \quad \text{or} \quad L = 4a + 3. \tag{5.4}$$

Is this true? What is the general result here?

A. The C program

The C program presented below performs the following task. A positive integer a is given, and we set

$$L = 4a - 1. \tag{A.1}$$

In the example below, we take $a = 41$, so $L = 163$, but one can modify the line specifying a and take another value. The output from the program is a printed list of all the integers $\ell \in \{1, \dots, L-1\}$ such that

$$\forall\, j, k \in \mathbb{Z}/(L), \quad aj^2 + k^2 + jk \ \text{ is not congruent to } \ \ell \ (\text{mod } L). \tag{A.2}$$

(If no such ℓ exists, the list is empty.)

This task is accomplished as follows. We set up an integer array with 180 elements, using

$$\text{int} \ \ f[180]; \tag{A.3}$$

The elements are $f[0], f[1], \dots, f[179]$. We initially set

$$f[j] = 1, \quad 0 \le j \le L - 1. \tag{A.4}$$

For this to work, we need $L \leq 180$. For larger L, we would need to alter (A.3) accordingly.

Then we let j and k run independently through $\{0, 1, \dots, L-1\}$, and we compute

$$aj^2 + k^2 + jk \mod L, \tag{A.5}$$

by setting

$$\begin{aligned} m &= aj^2 + k^2 + jk, \\ n &= m - L(m/L). \end{aligned} \tag{A.6}$$

Integer arithmetic in C yields $n \in \{0, \dots, L-1\}$ congruent to (A.5). For each pair $(j, k) \in \{0, 1, \dots, L-1\} \times \{0, 1, \dots, L-1\}$, we obtain such a number n, and then we set

$$f[n] = 0. \tag{A.7}$$

Finally, we run through $j \in \{0, 1, \dots, L-1\}$, and execute the command

$$\text{print} \;\; j \Longleftrightarrow f[j] = 1. \tag{A.8}$$

This accomplishes the stated task. Here is the C program:

```
/* moduloL.c */

#include <stdio.h>

  long j,k,L,a,m,n;
  int f[180];

main()
{
  a=41;
  L=4*a-1;
  for (j=0;j<=L-1;j++) {
    f[j]=1;
  }
  for (j=0;j<=L-1;j++) {
    for (k=0;k<=L-1;k++) {
      m=a*j*j+k*k+j*k;
      n=m-L*(m/L);
      f[n]=0;
    }
  }
  for (j=0;j<=L-1;j++) {
    if (f[j]==1) printf("%ld ",j);
  }

  printf(" \n");
}
```

References

[HW] G. Hardy and E. Wright, An Introduction to the Theory of Numbers, 4th Ed., Oxford University Press, 1960.

[MM] H. McKean and V. Moll, Elliptic Curves, Cambridge Univ. Press, 1997.

[P] M. Pinsky, The eigenvalues of an equilateral triangle, SIAM J. Math. Anal. 11 (1980), 819–827.