Similar Sublattices of Planar Lattices

Michael Baake, Rudolf Scharlau, and Peter Zeiner

Abstract. The similar sublattices of a planar lattice can be classified via its multiplier ring. The latter is the ring of rational integers in the generic case, and an order in an imaginary quadratic field otherwise. Several classes of examples are discussed, with special emphasis on concrete results. In particular, we derive Dirichlet series generating functions for the number of distinct similar sublattices of a given index, and relate them to zeta functions of orders in imaginary quadratic fields.

1 Introduction

Lattices in d-space (by which we mean co-compact discrete subgroups of $\mathbb{R}^d$) are important objects with increasingly many applications throughout mathematics and various applied sciences; see [11] for a comprehensive study. Among the sublattices of a lattice $\Gamma \subset \mathbb{R}^d$ are interesting special classes, such as similar sublattices (SSL) or coincidence site lattices (CSL); see [2,6,7] and references therein. Their classification has important applications in crystallography, materials science, and coding theory, but is also interesting in its own right. Here, we look at the special case of planar lattices and derive a rather complete picture of their SSLs by using a suitable blend of well-known results from quadratic forms, imaginary quadratic number fields, complex multiplication, and zeta functions. For known results on the related case of planar $\mathbb{Z}$-modules (in general non-discrete), we refer the reader to [3,13,19].

The classification of similar sublattices is closely related to that of coincidence sublattices, and analogously for modules, via the underlying (generalised) symmetry groups [13,14,16,27]. We will thus use a formulation via the (orientation preserving) similarity mappings of a lattice into itself, which form a ring in our case. Beyond the planar situation, various results are known in 3- and 4-space (via quaternions; see [4,5,7,10,27]). General results are still sparse and restricted to rather special cases; see [10,16] and references therein.

In this article, we use complex numbers throughout, with [12] being one of our main references. For completeness and readability, we give a brief account of the setting in Section 2, followed by a section on Dirichlet series generating functions in this context. Section 4 establishes the link between SSLs and principal ideals, which is then explored in the remaining sections with examples of increasing complexity.

2 General Setting and Basic Tools

Since we only consider planar lattices in this paper, we employ complex numbers. Two planar lattices $\Gamma \subset \mathbb{C}$ and $\Gamma' \subset \mathbb{C}$ are called (properly) *similar* (or *complex ho-*

1220

mothetic), written as $\Gamma \sim \Gamma'$, when $\Gamma' = a\Gamma$ for some nonzero $a \in \mathbb{C}$. Similarity is an equivalence relation, and we denote the equivalence class of a lattice Γ by $\mathrm{sim}(\Gamma)$. More generally, one can (and should) also consider orientation reversing similarities, then defining similar lattices in the wider sense. In this paper, apart from some brief comments, we restrict ourselves to orientation preserving mappings.

Each planar lattice can be written as the integer span of two nonzero complex numbers u, v, denoted as $\Gamma = \langle u, v \rangle_{\mathbb{Z}}$, where the ratio v/u is a number in the open upper half-plane (and thus not real). This has an interesting and well-known consequence, which follows from a multiplication by $1/u$.

Fact 2.1 *Each planar lattice is similar to a lattice of the form $\Gamma_\tau := \langle 1, \tau \rangle_{\mathbb{Z}}$, where τ is a complex number in the open upper half-plane $H := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.* ∎

One can further restrict τ to the region given by the conditions $|\tau| \geq 1$, $|\tau \pm 1| \geq |\tau|$ (compare [1, Fig. 2.1 and Thm. 2.2]), which define a fundamental domain for the action of the modular group $\mathrm{PSL}(2, \mathbb{Z})$. In this sense, knowing the similar sublattices for all lattices Γ_τ with τ in this region is sufficient to solve the classification problem.

Given a planar lattice $\Gamma \subset \mathbb{C}$, let us consider the set

$$(2.1) \qquad \mathrm{MR}(\Gamma) := \{a \in \mathbb{C} \mid a\Gamma \subset \Gamma\},$$

which will be the central object for the study of planar SSLs below. Clearly, $\mathrm{MR}(\Gamma)$ is closed under addition and multiplication and contains 1, so it is a ring (a subring of $\mathbb{C}$). This ring is called the *multiplier ring* of Γ. In particular, it always contains $\mathbb{Z}$ as a subring. For our further analysis of $\mathrm{MR}(\Gamma)$, we recall the following concepts from elementary algebraic number theory (see [8, 18] for details).

Fact 2.2 *For a complex number c, the following properties are equivalent:*

(i) *There exists a finitely generated additive subgroup M of $\mathbb{C}$ with $cM \subset M$.*

(ii) *The number c is a root of a monic polynomial with integer coefficients.*

Such a number is called an algebraic integer. ∎

For instance, the golden ratio $(\sqrt{5} + 1)/2$ is an algebraic integer, since it is a root of $x^2 - x - 1$. Clearly, an algebraic integer is algebraic over $\mathbb{Q}$ (in the sense of field extensions). Notice that it is not required, but is a consequence of (ii), that the minimal polynomial of an algebraic integer has integral coefficients. Notice also that the group M in (i) need not be a lattice, though it is isomorphic to $\mathbb{Z}^n$ as a group, for some $n \in \mathbb{N}$. Assuming (i), the polynomial equation of (ii) can be obtained from a matrix representation of the linear map induced by c on the rational vector space generated by M. For the converse implication, one observes that the subgroup M generated by $1, c, c^2, \ldots, c^{n-1}$, where n is the degree of the assumed polynomial, is mapped into itself by c, since $c \cdot c^{n-1} = -m_{n-1}c^{n-1} - \cdots - m_0$ for appropriate integers $m_0, \ldots, m_{n-1}$.

A subring $\mathcal{O}$ of $\mathbb{C}$ is called an *order* if it is finitely generated as a group. All elements of an order are algebraic integers (take $M = \mathcal{O}$ in Fact 2.2). The quotient field K of $\mathcal{O}$ is then a number field, meaning a finite extension of $\mathbb{Q}$ (the degree of K over $\mathbb{Q}$ coincides with the rank of $\mathcal{O}$). One often starts with K and speaks of an *order in K*,

now refering to a full module in K that is also a ring containing 1 (which is consistent with the above definition). The set of all algebraic integers in a given number field K is also an order, the *maximal order* of K, denoted by $\mathcal{O}_K$, where "maximal" means that it is not contained in any larger order of K.

Let us return to the discussion of the multiplier ring $\mathrm{MR}(\Gamma)$, as defined in (2.1). It is clear that all elements in this ring are algebraic integers (take $M = \Gamma$ in Fact 2.2). Similar lattices have the same multiplier ring because the multiplication in $\mathbb{C}$ is commutative. By Fact 2.1, it is thus sufficient to restrict to lattices of the shape Γ_τ, with $\tau \in H$. A planar lattice Γ is called *generic* when $\mathrm{MR}(\Gamma) = \mathbb{Z}$ and *non-generic* otherwise. The following determination of $\mathrm{MR}(\Gamma)$ in the non-generic case (which is the one we are mainly interested in) is well-known from the theory of elliptic functions. For the convenience of the reader, we recall the result in some detail, since it is fundamental for everything that follows in this paper.

Proposition 2.3 *If Γ is a non-generic planar lattice, its multiplier ring $\mathrm{MR}(\Gamma)$ is an order in an imaginary quadratic field. Explicitly, if $\Gamma \in \mathrm{sim}\big(\langle 1, \tau \rangle_{\mathbb{Z}}\big)$ with $\tau \in \mathbb{C} \setminus \mathbb{R}$ is non-generic, the number τ is algebraic of degree 2 over $\mathbb{Q}$, and one has*

$$\mathrm{MR}(\Gamma) = \langle 1, s\tau \rangle_{\mathbb{Z}}$$

for an appropriate non-zero integer s.

Proof As $\mathrm{MR}(\Gamma)$ is the same for all elements of $\mathrm{sim}(\Gamma)$, let $\Gamma = \langle 1, \tau \rangle_{\mathbb{Z}}$ be non-generic and consider an element $a \in \mathrm{MR}(\Gamma) \setminus \mathbb{Z}$, which exists by assumption. By Fact 2.2, a is an algebraic integer. To expand on this, observe that $a = a \cdot 1 \in \Gamma$, so $a = u + v\tau$ for some $u, v \in \mathbb{Z}$ with $v \neq 0$. Moreover, $a \cdot \tau = u\tau + v\tau^2 \in \Gamma$ implies $u\tau + v\tau^2 = k + \ell\tau$ for some $k, \ell \in \mathbb{Z}$. This gives a quadratic equation $v\tau^2 + (u - \ell)\tau - k = 0$ over $\mathbb{Z}$ (and $\mathbb{Q}$) for τ, which is thus algebraic.

Slightly changing the notation, there is then an equation

$$(2.2) \qquad s\tau^2 + p\tau + q = 0, \quad \text{with } s, p, q \in \mathbb{Z}, \ s > 0, \text{ and } \gcd(s, p, q) = 1,$$

where s, p, q are uniquely determined by τ. Lemma 1 in [8, Kap. 2, §7.4] (derived from similar, easy computations) now shows that $\mathrm{MR}(\Gamma)$ is as claimed in the proposition, with s from (2.2). In particular, it is itself a planar lattice, and thus an order in the quadratic field $\mathbb{Q}(\tau)$. ∎

If, in the above proof, one writes $\tau = \alpha + \mathrm{i}\beta$ with $\alpha, \beta \in \mathbb{R}$ and $\beta > 0$ (so that $\tau \in H$), the non-genericity of Γ_τ leads to an explicit necessary and sufficient criterion for α and β, which follows from a straightforward calculation.

Corollary 2.4 *Consider Γ_τ with $\tau = \alpha + \mathrm{i}\beta$, where $\alpha, \beta \in \mathbb{R}$ and $\beta > 0$. This lattice is non-generic if and only if both α and β^2 are rational numbers.* ∎

Let us briefly mention that $\tau = \frac{1}{3} + \mathrm{i}\beta$ defines a lattice Γ with $3\overline{\Gamma} \subset \Gamma$, which shows the possibility of sublattices that are (only) similar to Γ in the wider sense. More generally, for $\tau = \alpha + \mathrm{i}\beta$, this happens if and only if $2m\alpha + n(\alpha^2 + \beta^2)$ is integer for some $m, n \in \mathbb{Z}$, not both 0. This integrality condition is always satisfied in the

non-generic case. The existence of an orientation reversing similarity for Γ does not lead to new sublattices precisely when the symmetry group of Γ contains a reflection. We skip further details in this direction and concentrate on proper similarities.

When a basis $B = \{b_1, b_2\}$ for a planar lattice $\Gamma \subset \mathbb{R}^2$ is chosen, we denote by $G_B = (g_{ij})$ the corresponding *Gram matrix*, where g_{ij} is the Euclidean inner product of b_i and b_j. A Gram matrix is called *rational* when some $0 \neq \alpha \in \mathbb{R}$ exists such that αG_B has rational entries only. Otherwise, it is called *irrational*. The rationality or irrationality of the Gram matrix (in this sense) is not affected by the choice of the basis, and is shared by all lattices similar to Γ.

Corollary 2.5 *Let Γ be a planar lattice, with basis B and associated Gram matrix G_B. The condition of Corollary 2.4 is then equivalent to G_B being rational. This condition is independent of the actual choice of basis.* ■

Closely related to the (properly) similar sublattices of a lattice Γ is the corresponding set of orientation preserving (linear) similarity isometries, defined as

$$\mathrm{SOS}(\Gamma) = \{z \in \mathbb{S}^1 \mid \alpha z \Gamma \subset \Gamma \text{ for some } \alpha > 0\}.$$

It is immediate that $\mathrm{SOS}(\Gamma)$ is a subgroup of $\mathbb{S}^1$; compare [14, 16] and references therein. Its elements are referred to as the *special orthogonal similarities* (SOS) of Γ, although, strictly speaking, we consider only the rotational parts of the actual similarities here. Note that the latter only form a monoid, which was investigated in some detail in [6]; see also [13, 14] and references therein.

Theorem 2.6 *Let Γ be a planar lattice. If it is generic, it has multiplier ring $\mathrm{MR}(\Gamma) = \mathbb{Z}$ and SOS-group $\mathrm{SOS}(\Gamma) = \{\pm 1\} \simeq C_2$. Otherwise, one has*

$$\mathrm{SOS}(\Gamma) = \left\{ \tfrac{w}{|w|} \mid 0 \neq w \in \mathcal{O} \right\},$$

where $\mathrm{MR}(\Gamma) = \mathcal{O} = \mathrm{MR}(\mathcal{O})$ is an order in an imaginary quadratic number field K. Its explicit form follows from Proposition 2.3. Moreover, one has

$$\mathrm{SOS}(\Gamma) = \mathrm{SOS}(\mathcal{O}) = \mathrm{SOS}(\mathcal{O}_K) = \left\{ \tfrac{w}{|w|} \mid 0 \neq w \in \mathcal{O}_K \right\},$$

where $\mathcal{O}_K$ is the maximal order of K and thus contains $\mathcal{O}$. Finally, the group $\mathrm{SOS}(\Gamma)$ is the same for all lattices in $\mathrm{sim}(\Gamma)$.

Proof In view of Proposition 2.3, the claims follow from the observation that the SOS-group precisely consists of the directions $w/|w|$ with $w \neq 0$ in the multiplier ring of Γ, expressed as numbers on the unit circle. Clearly, $\mathcal{O}$ is also its own multiplier ring, and every direction in $\mathcal{O}$ is a direction in $\mathcal{O}_K$. On the other hand, $\mathcal{O}$ has finite index in $\mathcal{O}_K$, say n, so that $nz \in \mathcal{O}$ for all $z \in \mathcal{O}_K$, and the claim on the orders follows. The final property is a simple consequence of the commutativity of $\mathbb{C}$. ■

Let us mention in passing that $\mathrm{SOS}(\Gamma)$ remains unchanged for each lattice that is commensurate with Γ (meaning that there is a common sublattice), but also for all elements of $\mathrm{sim}(\Gamma)$ (and thus for all lattices commensurate with any of the latter). This is a special feature of the planar situation (and trivially true for $d = 1$), but does not hold in higher dimensions, as one loses commutativity of the special orthogonal group.

Example ***2.7*** ($\mathrm{SOS}(\mathbb{Z}[\mathrm{i}])$ and $\mathrm{SOS}(\mathbb{Z}[\frac{1+\mathrm{i}\sqrt{3}}{2}])$)   As $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain (and even Euclidean), its arithmetic can be used to derive $G = \mathrm{SOS}(\mathbb{Z}[\mathrm{i}])$ explicitly. If $z = \frac{w}{|w|} \in G$, then so is $z^2 = w^2/|w|^2$. Using the unique prime decomposition [15] up to units in $\mathbb{Z}[\mathrm{i}]$ together with the fact that $|w|^2 \in \mathbb{N}$, one finds

$$z^2 = \varepsilon \prod_{p \equiv 1\,(4)} \left(\frac{\omega_p}{\overline{\omega}_p} \right)^{n_p} = \varepsilon \prod_{p \equiv 1\,(4)} \left(\frac{\omega_p^2}{p} \right)^{n_p},$$

where $\varepsilon = \mathrm{i}^k$ with $k \in \{0, 1, 2, 3\}$ is a unit in $\mathbb{Z}[\mathrm{i}]$ and the product runs over the splitting primes of the field extension $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$. Here, all $n_p \in \mathbb{Z}$, at most finitely many of them non-zero, and $p = \omega_p \overline{\omega}_p$ is the splitting of $p \equiv 1 \bmod 4$ into two non-associate Gaussian primes; for details of this derivation, we refer to [2, 19] and references therein. Clearly, one then has

$$z = \left(\frac{1+\mathrm{i}}{\sqrt{2}} \right)^{\ell} \prod_{p \equiv 1\,(4)} \left(\frac{\omega_p}{\sqrt{p}} \right)^{n_p}$$

for some $\ell \in \{0, 1, \dots, 7\}$ and the $n_p \in \mathbb{Z}$ with the restrictions as above. Noting that $(1 + \mathrm{i})/\sqrt{2}$ is a primitive eighth root of unity, one concludes $\mathrm{SOS}(\mathbb{Z}[\mathrm{i}]) \simeq C_8 \times \mathbb{Z}^{(\aleph_0)}$. Explicit choices of the corresponding generators can be read from the previous formula.

An analogous result holds for the triangular lattice, where the SOS-group is $C_{12} \times \mathbb{Z}^{(\aleph_0)}$, with a primitive twelfth root of unity as generator for the cyclic group C_{12} and $\omega_p/\sqrt{p}$ with $p \equiv 1 \bmod 3$ as generators for the infinite cyclic groups, where ω_p is a (complex) Eisenstein prime in the Euclidean ring $\mathbb{Z}[(1 + \mathrm{i}\sqrt{3})/2]$; see [15] for background.

3   Generating Functions

If Γ is a planar lattice, we denote the number of distinct SSLs of Γ of index m by $f(m)$. The integer-valued arithmetic function f is super-multiplicative, which means that one has $f(mn) \geq f(m)f(n)$ for coprime $m, n \in \mathbb{N}$; see [5] and references therein for details. An example for genuine super-multiplicativity is given by the rectangular lattice $\langle 1, \tau \rangle_{\mathbb{Z}}$ with $\tau = 3\mathrm{i}/2$; further examples will follow below.

In many interesting cases, however, f is a multiplicative function (for instance, when the multiplier ring is a principal ideal domain). This motivates the use of Dirichlet series as their generating functions. We thus define

$$(3.1) \qquad\qquad D_{\Gamma}(s) := \sum_{m=1}^{\infty} \frac{f(m)}{m^s}.$$

As $[\Gamma : m\Gamma] = m^2$, a lower bound for $f(m)$ is given by the function that takes the value 1 on all squares of $\mathbb{N}$ and the value 0 otherwise. This lower bound gives the Dirichlet series of the function $\zeta(2s)$, which converges absolutely for all s with

Re$(s) > 1/2$. An upper bound is the number of *all* sublattices of Γ of index m, which is given by the divisor function $\sigma_1(m) = \sum_{d|m} d$; see [2, Appendix] or [21, p. 99, Lemma 2]. It defines the Dirichlet series of $\zeta(s)\zeta(s-1)$, with absolute convergence for all s with Re$(s) > 2$. This implies that all Dirichlet series $D_\Gamma(s)$ of planar lattices converge absolutely at least in the open right half-plane $\{s \in \mathbb{C} \mid \text{Re}(s) > 2\}$.

Recall from [5] that a sublattice Λ of Γ is called *primitive* in Γ when $x\Lambda \subset \Gamma$ with $x \in \mathbb{Q}$ implies $x \in \mathbb{Z}$. It is advantageous to distinguish SSLs that are primitive from those that are not. In fact, each sublattice of Γ can be uniquely written as $k\Lambda$ with $k \in \mathbb{N}$ and Λ a primitive sublattice. If we count the number of primitive SSLs of Γ by the function $f^{\text{pr}}(m)$ and define $D_\Gamma^{\text{pr}}(s) := \sum_{m=1}^\infty (f^{\text{pr}}(m))/m^s$ in analogy to (3.1), it is clear that one always has the relation

$$(3.2) \qquad\qquad D_\Gamma(s) = \zeta(2s)\, D_\Gamma^{\text{pr}}(s).$$

The determination of the generating function is thus reduced to finding its primitive part, the Dirichlet series $D_\Gamma^{\text{pr}}(s)$.

Fact 3.1 *If Γ is a planar lattice with generic multiplier ring, which is $\mathbb{Z}$, one has $D_\Gamma^{\text{pr}}(s) = 1$ and thus $D_\Gamma(s) = \zeta(2s)$.* ∎

In previous articles, the generating functions have been calculated for a variety of examples in the plane (see [3, 6] and references therein) and in higher dimensions (compare [5–7, 10]). Standard results such as Delange's Theorem [24, Thm. II.15] then yield the asymptotic growth of $\sum_{m=1}^n f(m)$ for large n, which is one further benefit of using generating functions. It is now our aim to develop a general approach for the calculation of the generating functions in the planar case.

4 Similar Sublattices and Principal Ideals

Let Γ be a planar lattice with non-trivial multiplier ring MR(Γ), which is thus an order $\mathcal{O}$ in an imaginary quadratic field K. Note that $\mathcal{O}$ itself is a planar lattice and its own multiplier ring, though it need not be similar to Γ (we will see examples for this below). Nevertheless, the rotation symmetry group of Γ is canonically isomorphic with the unit group $\mathcal{O}^\times$, which is C_2, C_4 (when Γ is similar to the standard square lattice, $\Gamma \in \text{sim}(\mathbb{Z}^2)$) or C_6 (when Γ is similar to the regular triangular lattice, $\Gamma \in \text{sim}(A_2)$). Observe that the linear mapping $z \mapsto az$ in $\mathbb{C}$ has determinant $a\bar{a}$. Consequently, one has $[\Gamma : a\Gamma] = a\bar{a}$ for any non-zero $a \in \mathcal{O}$ by a standard argument involving areas of fundamental domains. In other words, $a\Gamma$ is an SSL of Γ of index $a\bar{a} = \text{N}(a)$, where N denotes the field norm of K and the non-trivial Galois automorphism needed here is complex conjugation $z \mapsto \bar{z}$.

Proposition 4.1 *If Γ is a planar lattice with multiplier ring MR$(\Gamma) = \mathcal{O} \neq \mathbb{Z}$, one has an index-preserving bijection between the SSLs of Γ and the principal ideals of $\mathcal{O}$. The Dirichlet series generating function for the number of SSLs of Γ of a given index is thus given by the Dirichlet series for the non-zero principal ideals of $\mathcal{O}$.*

Proof The lattice Γ is similar to a lattice Γ_τ for some τ in the fundamental domain of the modular group, as discussed above. By assumption and an application of Proposition 2.3, $K = \mathbb{Q}(\tau)$ is then an imaginary quadratic field, and the multiplier ring of

both Γ_τ and Γ is an order $\mathcal{O}$ in K. Observe that $a\mathcal{O}$ is a principal ideal of $\mathcal{O}$ of index $N(a)$. Since $a\Gamma = b\Gamma$ for non-zero $a, b \in \mathcal{O}$ implies $b^{-1}a\Gamma = \Gamma$, one has $ba^{-1} \in \mathcal{O}$ with $N(ba^{-1}) = 1$, whence $b^{-1}a$ must be a unit in $\mathcal{O}$. Furthermore, any unit $\varepsilon \in \mathcal{O}$ satisfies $\varepsilon\Gamma = \Gamma$ due to $[\Gamma : \varepsilon\Gamma] = N(\varepsilon) = 1$. This establishes the bijectivity as claimed.

The generating function then satisfies

$$D_\Gamma(s) = \sum_{m=1}^{\infty} \frac{f(m)}{m^s} = \sum_{\substack{0 \neq \mathfrak{a} \subset \mathcal{O} \\ \mathfrak{a} \text{ is principal}}} \frac{1}{N(\mathfrak{a})^s},$$

where $\mathfrak{a} = a\mathcal{O}$ for some $a \in \mathcal{O}$ when $\mathfrak{a}$ is principal. Since $N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = N(a)$ in this case, the second claim follows.   ∎

For the remainder of the article, we will now use our approach to treat concrete classes of examples, in increasing order of complexity.

5   Orders of Class Number 1

A particularly nice and simple situation emerges when the multiplier ring $\mathcal{O}$ of Γ is a principal ideal domain (PID), or when at least all proper ideals are principal (see below for more). In this case, the Dirichlet series $D_\Gamma(s)$ is just the zeta function of $\mathcal{O}$ itself, which is the Dirichlet series generating function for *all* non-zero ideals of $\mathcal{O}$. To continue, it is easier to make the distinction whether the order $\mathcal{O}$ is maximal or not.

5.1   Maximal Orders

Let K be an imaginary quadratic field of class number 1, with discriminant d_K (we follow the notation of [12]), and let $\mathcal{O} = \mathcal{O}_K$ be the maximal order of K, which is the ring of integers in K and a PID due to the assumption on the class number. The following result is classic, compare [12, Thm. 7.30].

Fact 5.1   *There are precisely* 9 *imaginary quadratic fields with class number* 1*, which means that their maximal orders are PIDs. These are the fields $K = \mathbb{Q}(\omega_0)$ for*

$$\omega_0 \in \left\{ \tfrac{1+i\sqrt{3}}{2}, i, \tfrac{1+i\sqrt{7}}{2}, i\sqrt{2}, \tfrac{1+i\sqrt{11}}{2}, \tfrac{1+i\sqrt{19}}{2}, \tfrac{1+i\sqrt{43}}{2}, \tfrac{1+i\sqrt{67}}{2}, \tfrac{1+i\sqrt{163}}{2} \right\},$$

which are fields of discriminant $d_K \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$. In this formulation, the maximal order is $\mathcal{O}_K = \mathbb{Z}[\omega_0]$, while $\mathbb{Q}(\omega_0) = \mathbb{Q}(\sqrt{d_K})$.   ∎

The zeta function of $\mathcal{O}_K$ is the Dedekind zeta function of the quadratic field K. It is known [26] to factorise as

$$(5.1) \qquad\qquad \zeta_K(s) = \zeta(s)\, L(s, \chi),$$

where $L(s, \chi)$ is the L-series of the non-trivial character $\chi = \chi_{d_K}$ of the field K. The latter is a totally multiplicative arithmetic function and thus given by $\chi_{d_K}(1) = 1$

together with its values on rational primes,

$$\chi_{d_K}(p) = \begin{cases} 0, & p \mid d_K, \\ \left(\frac{d_K}{p}\right), & 2 \neq p \nmid d_K, \\ \left(\frac{d_K}{2}\right), & p = 2 \nmid d_K. \end{cases}$$

Here, (d_K/p) and $(d_K/2)$ denote the Legendre and the Kronecker symbol, the latter defined as

$$\left(\frac{d_K}{2}\right) = \begin{cases} 1, & d_K \equiv 1 \ (8), \\ -1, & d_K \equiv 5 \ (8), \\ 0, & d_K \equiv 0 \ (4). \end{cases}$$

This permits a direct calculation of the zeta function via its Euler product, as the character $\chi(p)$ takes only the values 0, -1, or 1, depending on whether the rational prime p ramifies, is inert, or splits in the extension from $\mathbb{Q}$ to K. The general formula reads

$$(5.2) \qquad \zeta_K(s) = \prod_{p \in \mathcal{P}} \frac{1}{(1 - p^{-s})(1 - \chi(p)p^{-s})}$$

$$= \prod_{\substack{p \in \mathcal{P} \\ \chi(p)=0}} \frac{1}{1 - p^{-s}} \prod_{\substack{p \in \mathcal{P} \\ \chi(p)=-1}} \frac{1}{1 - p^{-2s}} \prod_{\substack{p \in \mathcal{P} \\ \chi(p)=1}} \frac{1}{(1 - p^{-s})^2},$$

where $\mathcal{P}$ denotes the set of rational primes.

Let us recall that equation (5.1) implies the relation $f_K(m) = \sum_{\ell \mid m} \chi_{d_K}(\ell)$ for the number of principal ideals of norm m in $\mathcal{O}_K$. This is also the number of representations, counted modulo the unit group of $\mathcal{O}_K$, of the norm form $N(x + y\omega_0)$, where ω_0 is as in Fact 5.1. This number can be derived by elementary means as well; compare [26, Thm. 8.3]. Either way, one can now calculate the contributions from primitive lattices by means of equation (3.2). An Euler factor that will show up repeatedly in these zeta functions is

$$(5.3) \qquad \frac{1 + p^{-s}}{1 - p^{-s}} = 1 + \frac{2}{p^s} + \frac{2}{p^{2s}} + \frac{2}{p^{3s}} + \cdots .$$

The result on the generating functions now reads as follows.

Proposition 5.2 *Let K be any of the 9 imaginary quadratic fields of Fact 5.1, and let p_{ram} be its ramified prime, which is the unique rational prime that divides d_K. The Dirichlet series generating function for the number of SSLs of $\mathcal{O}_K$ is given by $D_{\mathcal{O}_K}(s) = \zeta_K(s)$ with the Dedekind zeta function of K according to eqation (5.2).*

Moreover, the generating function for the primitive SSLs of $\mathcal{O}_K$ is

$$D_{\mathcal{O}_K}^{\mathrm{pr}}(s) = \frac{D_{\mathcal{O}_K}(s)}{\zeta(2s)} = (1 + p_{\mathrm{ram}}^{-s}) \prod_{p \ \text{splits}} \frac{1 + p^{-s}}{1 - p^{-s}},$$

where the product runs over all rational primes p that split in the extension to K. The same generating function also applies to any planar lattice $\Gamma \in \mathrm{sim}(\mathcal{O}_K)$. ∎

If we write $D^{\mathrm{pr}}_{\mathcal{O}_K}(s) = \sum_{m=1}^{\infty} f^{\mathrm{pr}}(m) \, m^{-s}$, the arithmetic function f^{pr} satisfies $f^{\mathrm{pr}}(m) = 0$ for any $m \in \mathbb{N}$ that is divisible by p^2_{ram} or by an inert prime. Otherwise, it takes the value 2^a, where a is the number of distinct splitting primes that divide m.

d_K	norm form	d_K	norm form	d_K	norm form
-3	$x^2 + xy + y^2$	-8	$x^2 + 2y^2$	-43	$x^2 + xy + 11y^2$
-4	$x^2 + y^2$	-11	$x^2 + xy + 3y^2$	-67	$x^2 + xy + 17y^2$
-7	$x^2 + xy + 2y^2$	-19	$x^2 + xy + 5y^2$	-163	$x^2 + xy + 41y^2$

Table 1: Norm forms for the 9 maximal orders $\mathcal{O} = \mathbb{Z}[\omega_0]$ of class number 1 in imaginary quadratic number fields, labelled with the field discriminant d_K.

It remains to formulate a characterisation of the index spectrum and the primitive index spectrum, meaning the integers m for which $f(m) \neq 0$ or $f^{\mathrm{pr}}(m) \neq 0$. The result can be phrased by means of the norm form of K (or $\mathcal{O}_K$), which is given in Table 1.

Corollary 5.3 *Let Γ be a planar lattice with $\mathrm{MR}(\Gamma) = \mathcal{O}_K$ for one of the 9 imaginary quadratic fields K of Fact 5.1. Then, the indices of the SSLs of Γ are precisely the positive integers that can be represented by the norm form of K, while those of the primitive SSLs form the subset of primitively representable integers.* ∎

Example 5.4 (Square and triangular lattices)   The square lattice $\mathbb{Z}[i]$ and the triangular lattice $\mathbb{Z}[(1 + i\sqrt{3})/2]$ are the most prominent examples, and also (up to similarity) the only ones with a larger point symmetry, as mentioned above. Since they have been analysed explicitly in various other sources (see [2, 3, 6] and references therein), we omit details of the derivation and simply state the result. For any lattice $\Gamma \in \mathrm{sim}\big(\mathbb{Z}[i]\big)$, Proposition 5.2 leads to the generating function

$$D^{\mathrm{pr}}_{\square}(s) = \sum_{m=1}^{\infty} \frac{f^{\mathrm{pr}}_{\square}(m)}{m^s} = (1 + 2^{-s}) \prod_{p \equiv 1 \, (4)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

Here, $f^{\mathrm{pr}}_{\square}(m) = 0$ whenever m is divisible by 4 or by any prime $p \equiv 3 \bmod 4$, while one has $f^{\mathrm{pr}}_{\square}(m) = 2^a$ otherwise, where a is the number of distinct primes $p \equiv 1 \bmod 4$ that divide m.

Similarly, for any $\Gamma \in \mathrm{sim}\big(\mathbb{Z}[(1 + i\sqrt{3})/2]\big)$, one obtains

$$D^{\mathrm{pr}}_{\triangle}(s) = \sum_{m=1}^{\infty} \frac{f^{\mathrm{pr}}_{\triangle}(m)}{m^s} = (1 + 3^{-s}) \prod_{p \equiv 1 \, (3)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

In variation of the previous case, one now has $f^{\mathrm{pr}}_{\triangle}(m) = 0$ for all m that are divisible by 9 or by any prime $p \equiv 2 \bmod 3$, and otherwise $f^{\mathrm{pr}}_{\triangle}(m) = 2^a$, this time with a being the number of distinct primes $p \equiv 1 \bmod 3$ that divide m.

5.2 Non-Maximal Orders

An application of the general class number formula for orders (see [20, Part I, Thm. 7] or [12, Thm. 7.24]) shows that there are precisely 4 non-maximal orders of class number 1 in imaginary quadratic fields. Note, however, that a non-maximal order $\mathcal{O}$ fails to be Dedekind, hence is never a PID in the usual sense. Here, the ideal class group only refers to the *proper* (or invertible) ideals, see [12, §7] for a nice summary. In particular, all principal ideals are proper, wherefore we still have a useful connection with the zeta function of $\mathcal{O}$. The basic data for our purposes are summarised in Table 2.

D	K	$\mathcal{O}$	norm form	$p \mid D$	conductor
-12	$\mathbb{Q}(i\sqrt{3})$	$\mathbb{Z}[i\sqrt{3}]$	$x^2 + 3y^2$	$2, 3$	2
-16	$\mathbb{Q}(i)$	$\mathbb{Z}[2i]$	$x^2 + 4y^2$	2	2
-27	$\mathbb{Q}(i\sqrt{3})$	$\mathbb{Z}[\frac{1}{2}(1 + i3\sqrt{3})]$	$x^2 + xy + 7y^2$	3	3
-28	$\mathbb{Q}(i\sqrt{7})$	$\mathbb{Z}[i\sqrt{7}]$	$x^2 + 7y^2$	$2, 7$	2

Table 2: Basic data for the 4 non-maximal orders of class number 1 in imaginary quadratic number fields, labelled with their discriminant D.

In our present situation, it turns out that the generating function for $\mathcal{O}$ still possesses an Euler product over all primes. This is clear for all but finitely many primes, due to the bijection property between ideals of $\mathcal{O}$ and those of $\mathcal{O}_K$ with norms coprime to the conductor; see [12, Prop. 7.20], and [26, Ex. 8.8] for an explicit expression in terms of characters. For the finitely many remaining primes, namely the ones dividing the conductor, one has to do some extra calculations, which then give the remaining Euler factors constructively. This will be outlined in the explicit treatment of the examples below, where we actually show this for all primes that divide the discriminant. As before, we focus on the Dirichlet series for the primitive SSLs, because the others simply follow by multiplication with $\zeta(2s)$, as in equation (3.2).

Example 5.5 ($D = -12$) The primes that need special attention are $p = 2$ and $p = 3$. The quadratic form $x^2 + 3y^2$ cannot represent 2, while congruence arguments (mod 8 and 9) show that it cannot *primitively* represent any integer that is divisible by 8 or 9. On the other hand, $3 = 0 + 3(\pm 1)^2$ and $4 = (\pm 1)^2 + 3(\pm 1)^2$ are the only possibilities to represent 3 and 4, respectively. Counted modulo the unit group $\mathcal{O}^\times \simeq C_2$, this amounts to a single solution for $m = 3$ and to two solutions for $m = 4$. All other primes can be extracted from the general formula (5.1). The multiplicativity of the counting function (by the relation to $\mathcal{O}_K$) is inherited for the combination of all primes except $p = 2$. By another congruence argument (mod 4), which in essence explores the different unit groups of $\mathcal{O}$ and $\mathcal{O}_K$, one sees that any primitive representation $x^2 + 3y^2 = 4m$ with m odd can be split into one of 4 and one

of m, so that multiplicativity holds also for this prime factor. Together, this results in the Dirichlet series

$$D_{\mathcal{O}}^{\mathrm{pr}}(s) = \left(1 + \frac{2}{4^s}\right)\left(1 + \frac{1}{3^s}\right) \prod_{p \equiv 1\,(3)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

Example 5.6 ($D = -16$)   Here, the only special prime is $p = 2$. When $m = x^2 + 4y^2$ is divisible by 16, congruence arguments mod 4 and 16 show that x and y cannot be coprime, so that no primitive solutions are possible. As 2 is not representable at all, it remains to count the solutions for $m = 4$ and $m = 8$, where one observes $4 = 0^2 + 4(\pm 1)^2$ and $8 = (\pm 2)^2 + 4(\pm 1)^2$, which (again mod the unit group $\mathcal{O}^\times \simeq C_2$) amounts to 1, resp. 2 solutions. As in the previous example, the multiplicativity of the counting function needs to be extended here to cover powers of $p = 2$. It follows from a congruence argument mod 8, resp. mod 16. Together with the standard Euler factor (5.3) for all other primes, one thus has the Dirichlet series

$$D_{\mathcal{O}}^{\mathrm{pr}}(s) = \left(1 + \frac{1}{4^s} + \frac{2}{8^s}\right) \prod_{p \equiv 1\,(4)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

Example 5.7 ($D = -27$)   Here, the kind of reasoning of the previous example has to be repeated for the prime $p = 3$, though for a slightly more complicated quadratic form. One can check that 3 is not representable by $x^2 + xy + 7y^2$, while

$$9 = 1^2 + 1 \cdot 1 + 7 \cdot 1^2 = 2^2 - 2 \cdot 1 + 7(-1)^2 \text{ and}$$

$$27 = 4^2 + 4 \cdot 1 + 7 \cdot 1^2 = 1^2 - 1 \cdot 2 + 7(-2)^2 = 5^2 - 5 \cdot 1 + 7(-1)^2$$

provide a complete list of representatives (mod units) for the primitive representations of 9 and 27. To see that no primitive representation of integers of the form $81m$ with $m \in \mathbb{Z}$ exists, one first observes

$$x^2 + xy + 7y^2 = \left(x + \tfrac{1}{2}y\right)^2 + \tfrac{27}{4}y^2,$$

and concludes via congruence considerations mod 81.

Moreover, a refined congruence argument (mod 27) also shows that, as in the previous two examples, we get an extension of multiplicativity to cover contributions from powers of $p = 3$. Invoking the standard Euler factor once more for all other primes, one gets

$$D_{\mathcal{O}}^{\mathrm{pr}}(s) = \left(1 + \frac{2}{9^s} + \frac{3}{27^s}\right) \prod_{p \equiv 1\,(3)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

Example 5.8 ($D = -28$)   In the last example of this section, the primes $p = 2$ and $p = 7$ need special attention, this time for the quadratic form $x^2 + 7y^2$. Clearly, there is only one way (mod units) to represent 7 and no primitive way to represent any

integer that is divisible by 49, which follows once more by a congruence argument (here, mod 49).

For the positive powers of the prime 2, one quickly finds that 2 and 4 are not primitively representable (and 2 not at all). The primitive representations of the higher powers of 2 can be derived from the factorisation $2 = \pi\bar{\pi}$ with $\pi = (1 + i\sqrt{7})/2$, where π is a prime in the maximal order (which is $\mathcal{O}_K = \mathbb{Z}[\pi]$) but not an element of $\mathcal{O}$. Observe next that the only ideals of $\mathcal{O}_K$ of norm 2^r are the principal ideals generated by $\pi^\ell\bar{\pi}^{r-\ell}$ for $0 \le \ell \le r$. We need to select the generating elements that also lie in $\mathcal{O}$ and are primitive there. It is not difficult to check that this requires $r \ge 3$ together with either $\ell = 1$ or $r - \ell = 1$. These two cases are not related by units, so that always precisely two primitive representations (up to units) exist for $r \ge 3$.

Now, one needs the identity

$$1 + \sum_{m \ge 3} \frac{2}{2^{ms}} = 1 + \frac{2}{8^s}\frac{1}{1 - 2^{-s}} = (1 - 2^{1-s} + 2^{1-2s})\frac{1 + 2^{-s}}{1 - 2^{-s}},$$

while all remaining primes work as in the previous examples. Here, multiplicativity of the counting function is once again clear for all primes except $p = 2$. For the latter, we observe that an integer in $\mathcal{O}_K$ with odd norm is automatically an element of $\mathcal{O}$, so that we can factorise any represented integer into powers of 2 and its odd part. Together, this yields

$$D_{\mathcal{O}}^{\mathrm{pr}}(s) = \left(1 - \frac{2}{2^s} + \frac{2}{4^s}\right)\left(1 + \frac{1}{7^s}\right) \prod_{p \equiv 1,2,4\ (7)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

6 Euler's Convenient Numbers

Similar results can be obtained for a larger, though still finite, list of discriminants. These are the numbers D such that every *genus* of (positive definite, binary) quadratic forms of discriminant D consists of one class only. The crucial property of such single class genera is that, for the corresponding forms, it only depends on a congruence condition modulo D whether a natural number is represented by the form or not. By definition, two quadratic forms (in any number of variables) are in the same genus if they are equivalent modulo N for every modulus $N \in \mathbb{N}$. In this case, the forms have the same discriminant, and the number of classes in one genus is thus always finite.

Here, we deal with *binary* quadratic forms where the theory of genera has several special features (and is, in fact, a well established part of classical algebraic number theory, independent of the general theory of quadratic forms; compare [9, 12, 26]). As before, the distinction between fundamental and non-fundamental discriminants is relevant. For a given *fundamental* discriminant D, the equivalence classes of quadratic forms bijectively correspond to the ideal classes in the maximal order $\mathcal{O}_D$. For a quick description of the partition of classes into genera, one can take advantage of the group structure on the set $\mathcal{C}_D$ of ideal classes of $\mathcal{O}_D$: two ideal classes are in the same genus if they give the same element in the factor group $\mathcal{C}_D/\mathcal{C}_D^2$. All genera are of the single class type if and only if $\mathcal{C}_D^2$ is the trivial group, which is tantamount

to saying that the class group is a finite Abelian 2-group. For *non-fundamental* discriminants, there are certain complications to this approach (which works only for invertible ideals). We therefore briefly summarise the main facts in a different way, which is more suitable for our purposes.

The different genera of binary forms q of some fixed discriminant D are separated by the values $m = q(x, y)$ represented by the form. Together with an individual $m \in \mathbb{Z}$ coprime to D, also its whole square class in $(\mathbb{Z}/D\mathbb{Z})^\times$ is represented by the genus. Already one square class represented by q determines the genus of q. This square class, in turn, is determined by the values of all quadratic (or 'real') characters $\chi: (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$. Let us mention in passing that precisely half of the elements of $(\mathbb{Z}/D\mathbb{Z})^\times$ are represented by some form of discriminant D. These are the elements of the kernel of a certain 'principal' character χ_D; compare [9, 12, 26].

Following our earlier discussion, we are primarily interested in the principal genus, which contains the norm form of the order $\mathcal{O}_D$. The elements of $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by this genus form a subgroup of $(\mathbb{Z}/D\mathbb{Z})^\times$ that contains the group of all squares as another subgroup of index at most 2; compare [17, Lemma 3.17].

Let h be the class number of $\mathcal{O}_D$. Using the previously mentioned general formula

$$R_D(m) := \sum_{i=1}^{h} R_{q_i}(m) = \sum_{k|m} \chi_D(k)$$

for the total (weighted) representation number of a number m by all forms q_i of discriminant D, one can derive explicit results also in the present case, where $h > 1$, but all h forms q_i lie in different genera. Our previous discussion implies that the supports of the various R_{q_i} in $(\mathbb{Z}/D\mathbb{Z})^\times$ are disjoint and cover the kernel of χ_D. Notice that all representations are counted in this formula, not just the primitive ones.

The list of the known discriminants of positive definite binary single class genera is given (without further explanation) in [9, Sec. 5.2]. Among the discriminants $\equiv 0$ mod 4, there are presently 65 such numbers known, which were already studied by Gauss and Euler; see [23, Sequence A000926]. These numbers are also given in a Table on p. 60 of [12], sorted according to the class number, which also goes back to Gauß. Among the remaining discriminants, namely those $\equiv 1$ mod 4, further 36 cases are known [9, Sec. 5.2]. As before, they contain both fundamental and non-fundamental ones, and the figures contain the cases of our Tables 1 and 2.

The total list is believed to be complete, and it has been a long standing challenge of the 'analytic theory of algebraic numbers' to actually prove this. For a first general approach and a non-constructive finiteness result (naturally not for today's state of matters), see the classic lecture notes by Siegel [22, Thm. 25.5]. The known list of fundamental discriminants is complete if the generalised Riemann hypothesis is true [17]. By [25], there is at most one further fundamental discriminant with only one class in each genus. The case of arbitrary discriminants can be reduced relatively easily to the case of fundamental discriminants, for instance by the method explained in [9, Sec. 7.1], or by using the relative class number formula, as explained in [20], see also [12, Ex. 7.3].

When the class number fails to be 1, we will generally lose multiplicativity of the counting function f. This relates to the fact that the product of two non-principal

ideals in the corresponding order is principal. However, due to the structure of the ideal class group, we have a natural binary grading on the ideals, depending on whether they are principal or not. If the order under investigation is still principal, one can derive the generating function quickly from the zeta function.

Example 6.1 ($\mathbb{Z}[i\sqrt{6}\,]$) The discriminant is $D = -24$, which is fundamental, with class number 2, hence ideal class group C_2. The norm form is $x^2 + 6y^2$, which is the norm of principal ideals in the maximal order $\mathcal{O}$, while the non-principal ideals have a norm of the form $2x^2 + 3y^2$. The relevant totally multiplicative character χ_{-24} is defined by

$$\chi_{-24}(p) = \begin{cases} 0, & \text{if } p = 2 \text{ or } p = 3, \\ 1, & \text{if } p \equiv 1, 5, 7, 11 \text{ mod } 24, \\ -1, & \text{if } p \equiv 13, 17, 19, 23 \text{ mod } 24, \end{cases}$$

which leads to the zeta function $\zeta_K(s) = \zeta(s)\, L(s, \chi_{-24})$; compare [26]. Extracting the contribution from primitive ideals then gives the factorisation

$$\zeta_K(s) = \zeta(2s) \left((1 + 2^{-s})(1 + 3^{-s}) \prod_{p \equiv 5,11 \ (24)} \frac{1 + p^{-s}}{1 - p^{-s}} \right) \prod_{p \equiv 1,7 \ (24)} \frac{1 + p^{-s}}{1 - p^{-s}}.$$

The bracketed term contains the contributions from primitive ideals that are themselves not principal, while the last product covers the principal ones. Our Dirichlet series thus reads

$$D^{\mathrm{pr}}(s) = \prod_{p \equiv 1,7 \ (24)} \frac{1 + p^{-s}}{1 - p^{-s}} \sum_{m=1}^{\infty} \frac{b(m)}{m^s}$$

with $b(1) = 1$ and $b(m) = 0$ whenever $p \,|\, m$ for some $p \equiv 1, 7, 13, 17, 19, 23$ mod 24. What remains are the integers of the form $m = 2^\alpha 3^\beta \prod_{p \equiv 5,11 \ (24)} p^{\ell_p}$ with $\alpha, \beta \in \{0, 1\}$ and $\ell_p \in \mathbb{N}_0$, only finitely many of them $\neq 0$. For them, the grading implies

$$b(m) = \left(1 + (-1)^{\alpha + \beta + \sum \ell_p} \right)^{\mathrm{card}\{p > 3 \,|\, \ell_p \neq 0\}},$$

which, together with the contribution from primes $\equiv 7$ mod 24, results in

$$D^{\mathrm{pr}}(s) = 1 + \frac{1}{6^s} + \frac{2}{7^s} + \frac{2}{10^s} + \frac{2}{15^s} + \frac{2}{22^s} + \frac{2}{25^s} + \frac{2}{31^s} + \frac{2}{33^s} + \frac{2}{42^s} + \frac{4}{55^s} + \cdots$$

thus illustrating the calculation explained above.

The general situation for non-fundamental discriminants is more complicated. To work out further examples, it is advantageous to start from an order $\mathcal{O}$ and its SOS-group, which only depends on the quadratic field K by Theorem 2.6. Then, for each element of this group, one has to determine the index of the corresponding primitive SSL of $\mathcal{O}$, which can be linked to the results for the maximal order $\mathcal{O}_K$. Defining the denominator of $z \in \mathrm{SOS}(\Gamma)$ for a planar lattice Γ as

$$\mathrm{den}_\Gamma(z) = \min\{\alpha \geqslant 1 \mid \alpha z \Gamma \subset \Gamma\},$$

which exists by a standard discreteness argument on the basis of the lattice property of Γ, one sees that z gives rise to a primitive SSL of Γ of index $(\mathrm{den}_\Gamma(z))^2$. Since the latter is an integer, the denominator itself is either an integer or a quadratic irrationality.

Example 6.2 ($\mathbb{Z}[3\mathrm{i}]$ and $\mathbb{Z}[5\mathrm{i}]$) Let p be a prime and consider $\mathbb{Z}[p\mathrm{i}]$, which is an order in the field $\mathbb{Q}(\mathrm{i})$, with conductor p in the maximal order $\mathbb{Z}[\mathrm{i}]$. The case $p = 2$ was treated in Example 5.6 as a special case with class number 1. Two further primes lead to convenient numbers, namely $p = 3$ and $p = 5$. By Theorem 2.6, we have

$$\mathrm{SOS}(\mathbb{Z}[n\mathrm{i}]) = \mathrm{SOS}(\mathbb{Z}[\mathrm{i}]) \simeq C_8 \times \mathbb{Z}^{(\aleph_0)},$$

for arbitrary $n \in \mathbb{N}$, with the group and generators as described in Example 2.7.

To determine the SSLs of $\mathbb{Z}[p\mathrm{i}]$, it is again sufficient to concentrate on the primitive ones, meaning (by Proposition 4.1) the principal ideals of $\mathbb{Z}[p\mathrm{i}]$ that are primitive as sublattices. They can be obtained from the rotations of the SOS-group (which does not depend on p) by determining the corresponding denominators (which depend on p). If p is prime, the denominator of any $z \in \mathrm{SOS}(\mathbb{Z}[\mathrm{i}])$ for $\mathbb{Z}[p\mathrm{i}]$ is either the same as for $\mathbb{Z}[\mathrm{i}]$, or it gets multiplied by p. Each primitive SSL of $\mathbb{Z}[\mathrm{i}]$, labelled by some $z = w/|w|$ with $w = m + n\mathrm{i}$ and m, n coprime, gives rise to two distinct SSLs of $\mathbb{Z}[p\mathrm{i}]$ whose indices might differ by a factor of p^2. This follows from the different point symmetries, because z and $\mathrm{i}z$ define the same SSL of the square lattice, but distinct ones for $\mathbb{Z}[p\mathrm{i}]$. Let us thus consider Gaussian integers $w = m + \mathrm{i}n$ with m, n coprime, compare it with $\mathrm{i}w$, and distinguish the possible cases.

For $p = 3$, a Gaussian integer $w = m + 3n\mathrm{i}$ with $3 \nmid m$ results in $|w|^2 \equiv 1$ mod 3, while $w = m + \mathrm{i}n$ with $3 \nmid n$ gives either $|w|^2 \equiv 1$ mod 3 (when $3 \mid m$) or $|w|^2 \equiv 2$ mod 3 (when $3 \nmid m$). Of these possibilities, only $w = m + 3n\mathrm{i}$ leaves the index of the resulting SSL unchanged (in comparison to the square lattice), while all other indices have to be multiplied by 9. This gives the generating function

$$D^{\mathrm{pr}}_{\mathbb{Z}[3\mathrm{i}]}(s) = \sum_{\substack{m \geqslant 1 \\ m \equiv 1\ (3)}} (1 + 9^s)\, \frac{f^{\mathrm{pr}}_\square(m)}{(9m)^s} \; + \sum_{\substack{m \geqslant 1 \\ m \equiv 2\ (3)}} \frac{2 f^{\mathrm{pr}}_\square(m)}{(9m)^s}$$

with the arithmetic function $f^{\mathrm{pr}}_\square$ of Example 5.4. There is no meaningful Euler product expansion in line with the non-multiplicativity of the total number of SSLs of a given index in this case.

Similarly, for $p = 5$, one has $|w|^2 \equiv \pm 1$ mod 5 when $w = m + 5n\mathrm{i}$ with $5 \nmid m$ or when $w = m + \mathrm{i}n$ with $5 \mid m$ and $5 \nmid n$, while $|w|^2 \equiv 0$ or ± 2 mod 5 when $w = m + \mathrm{i}n$ with both m and n coprime to 5. This time, the generating function reads

$$D^{\mathrm{pr}}_{\mathbb{Z}[5\mathrm{i}]}(s) = \sum_{\substack{m \geqslant 1 \\ m \equiv \pm 1\ (5)}} (1 + 25^s)\, \frac{f^{\mathrm{pr}}_\square(m)}{(25m)^s} \; + \sum_{\substack{m \geqslant 1 \\ m \equiv 0, \pm 2\ (5)}} \frac{2 f^{\mathrm{pr}}_\square(m)}{(25m)^s}$$

with an interpretation analogous to the previous case.

7 General Case

Beyond the cases described so far, one loses the possibility to express the results via simple congruence conditions on the rational primes. Instead, one needs a criterion for the representability of a given prime by the norm form via a specific polynomial congruence, as explained in [12]. When we are dealing with lattices that are similar to the maximal order in an imaginary quadratic field, we may employ the main result of Cox [12], as extracted from his Theorems 9.2 and 13.23. It is formulated for discriminants of the form $-4n$, with class number $h(-4n)$. Its extension to the remaining discriminants is mentioned in [12, Ex. 9.3].

Fact 7.1 *For $n \in \mathbb{N}$, there exists an effectively computable polynomial $f_n(x)$ of degree $h(-4n)$ such that, for any odd prime p not dividing n, the equation $p = x^2 + ny^2$ has an integer solution if and only if $\left(\frac{-n}{p} \right) = 1$ and $f_n(x) \equiv 0 \mod p$ has an integer solution.*

The corresponding statement also holds for negative discriminants $D \equiv 1 \mod 4$, then for the representation of p by the form $x^2 + xy + \frac{1-D}{4} y^2$. Here, the conditions are $\left(\frac{m}{p} \right) = 1$ with $m = \frac{1-D}{4}$, and the polynomial has degree $h(D)$. ∎

One possible choice of the polynomial is the class equation, which can be expressed as a product over the classes and involves the j-invariants of its representatives; see [12, p. 298] for an example. For fundamental discriminants, there are simpler, more efficient alternatives for the class polynomials.[1]

Unfortunately, this approach does not easily seem to lead to closed expressions as soon as we are beyond the situation with one class per genus. As in the second part of the previous chapter, it is thus usually easier to employ the denominator of a rotation to come to concrete results. Let us illustrate this with one final example.

Example 7.2 ($\mathbb{Z}[pi]$ with p an odd prime)   As in Example 6.2, we have

$$\mathrm{SOS}\big(\mathbb{Z}[pi]\big) = \mathrm{SOS}\big(\mathbb{Z}[i]\big) \simeq C_8 \times \mathbb{Z}^{(\aleph_0)},$$

and, in principle, we can proceed as above. In particular, using the same conventions for $\omega = m + in$ as above, $z = \omega/|\omega|$ has denominator $|\omega|$ or $p|\omega|$, depending on whether p divides n or not. Indeed, z has denominator $p|\omega|$ if $|\omega|^2 = m^2 + n^2$ is not a quadratic residue modulo p, or if $|\omega|^2$ is divisible by p. If $|\omega|^2$ is a quadratic residue, both denominators may occur. Clearly, if z has denominator $|\omega|$, then iz has denominator $p|\omega|$, since m and n are relatively prime. Hence, for fixed $|\omega|^2$, the number of primitive SSLs with index $|\omega|^2$ is at most the number of primitive SSLs with index $p^2|\omega|^2$. Thus, in terms of the arithmetic function $f_\square^{\mathrm{pr}}$ of the square lattice, we may write

$$D_{\mathbb{Z}[pi]}^{\mathrm{pr}}(s) = \sum_{\left(\frac{m}{p} \right) = 1} \frac{f_\square^{\mathrm{pr}}(m)}{p^{2s}m^s}(b(m) + a(m)\, p^{2s}) + \sum_{\left(\frac{m}{p} \right) \neq 1} \frac{2 f_\square^{\mathrm{pr}}(m)}{p^{2s}m^s},$$

where $a(m)$ and $b(m)$ are still to be determined. They satisfy $a(m)+b(m) = 2$ together with $a(m) \leq b(m)$ and $f_\square^{\mathrm{pr}}(m)a(m) \in \mathbb{N}_0$ (we have seen above that $a(m) = b(m) = 1$ for $p = 3$ or $p = 5$).

---

[1]For instance, see http://www.uni-due.de/zahlentheorie/polynomials_de.shtml

The determination of $a(m)$ depends on the prime factorisation of m and is rather tedious in general. As an example, we discuss $p = 7$, where the quadratic residues are 1, 2, and 4. Here, we have three different types of prime numbers $q = (m+in)(m-in)$ (we only need to consider primes $q \equiv 1 \pmod 4$), namely

$q \equiv 1, 2, 4 \pmod 7$ and either $7 \mid m$ or $7 \mid n$
$q \equiv 1, 2, 4 \pmod 7$ and $7 \nmid m$, $7 \nmid n$, which implies $m^2 \equiv n^2 \pmod 7$,
$q \equiv 3, 5, 6 \pmod 7$, which implies $7 \nmid m$, $7 \nmid n$, and $m^2 \not\equiv n^2 \pmod 7$.

Note that $a(q) = 1$ in the first case, and $a(q) = 0$ in the other two. To handle composite numbers m, let $m = \prod_i q_i^{r_i}$ be the prime decomposition of m and define $s(m) := \sum_i t_i r_i$, where t_i is 4, 2, or 1, according to whether q_i is of type 1, 2, or 3, respectively. One can check that $s(m)$ is even if and only if $m \equiv 1, 2, 4 \pmod 7$. Such numbers m can be divided into three equivalence classes, namely

N_1: all prime factors $q_i \equiv 3, 5, 6 \pmod 7$ have even power and $s(m) \equiv 0 \pmod 4$,
N_2: all prime factors $q_i \equiv 3, 5, 6 \pmod 7$ have even power and $s(m) \equiv 2 \pmod 4$,
N_3: there are at least two prime factors $q_i \equiv 3, 5, 6 \pmod 7$ with odd power.

Both $a(m)$ and $b(m)$ are constant on these equivalence classes, with the following values.

m	N_1	N_2	N_3
$a(m)$	1	0	$\frac{1}{2}$
$b(m)$	1	2	$\frac{3}{2}$

This gives the generating function

$$D^{\mathrm{pr}}_{\mathbb{Z}[7i]}(s)$$

$$= \sum_{m \in N_1} \frac{f^{\mathrm{pr}}_\square(m)}{49^s m^s}(1 + 49^s) + \sum_{m \in N_2} \frac{2 f^{\mathrm{pr}}_\square(m)}{49^s m^s}$$

$$+ \sum_{m \in N_3} \frac{f^{\mathrm{pr}}_\square(m)}{49^s m^s}\left(\frac{3}{2} + \frac{49^s}{2}\right) + \sum_{m \equiv 3,5,6\,(7)} \frac{2 f^{\mathrm{pr}}_\square(m)}{49^s m^s}$$

$$= \frac{2}{49^s}D^{\mathrm{pr}}_{\mathbb{Z}[i]}(s) + \sum_{m \in N_1} \frac{f^{\mathrm{pr}}_\square(m)}{49^s m^s}(49^s - 1) + \sum_{m \in N_3} \frac{f^{\mathrm{pr}}_\square(m)}{49^s m^s}\left(\frac{49^s}{2} - \frac{1}{2}\right)$$

$$= 1 + \frac{1}{49^s} + \frac{2}{50^s} + \frac{2}{53^s} + \frac{2}{58^s} + \frac{2}{65^s} + \frac{2}{74^s} + \frac{2}{85^s} + \frac{2}{98^s} + \frac{2}{113^s} + \frac{2}{130^s} + \cdots,$$

which illustrates the higher complexity of this case.

References

[1]   T. M. Apostol, *Modular functions and Dirichlet series in number theory.* Second ed., Graduate Texts in Mathematics, 41, Springer-Verlag, New York, 1990.

[2]   M. Baake, *Solution of the coincidence problem in dimensions $d \leq 4$.* In: The mathematics of long-range aperiodic order (Waterloo, ON, 1995), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 489, Kluwer, Dordrecht, 1997, pp. 9–44.

[3]   M. Baake and U. Grimm, *Bravais colourings of planar modules with N-fold symmetry.* Z. Krist. **219**(2004), no. 2, 72–80.   doi:10.1524/zkri.219.2.72.26322

[4]   M. Baake, M. Heuer, U. Grimm, and P. Zeiner, *Coincidence rotations of the root lattice A_4.* European J. Combin. **29**(2008), no. 8, 1808–1819.   doi:10.1016/j.ejc.2008.01.012

[5]   M. Baake, M. Heuer, and R. V. Moody, *Similar sublattices of the root lattice A_4.* J. Algebra **320**(2008), no. 4, 1391–1408.   doi:10.1016/j.jalgebra.2008.04.021

[6]   M. Baake and R. V. Moody, *Similarity submodules and semigroups.* In: Quasicrystals and discrete geometry (Toronto, ON, 1995). Fields Inst. Monogr., 10, American Mathematical Society, Providence, RI, 1998, pp. 1–13.

[7]   _____, *Similarity submodules and root systems in four dimensions.* Can. J. Math. **51**(1999), no. 6, 1258–1276.   doi:10.4153/CJM-1999-057-0

[8]   S. I. Borewicz and I. R. Safarevic, *Zahlentheorie.* Aus dem Russischen übersetzt von Helmut Koch. Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften, Mathematische Reihe, 32, Birkhäuser Verlag, Basel-Stuttgart, 1966

[9]   D. A. Buell, *Binary quadratic forms. Classical theory and modern computations.* Springer-Verlag, New York, 1989.

[10] J. H. Conway, E. M. Rains, and N. J. A. Sloane, *On the existence of similar sublattices.* Can. J. Math. **51**(1999), no. 6, 1300–1306.   doi:10.4153/CJM-1999-059-5

[11] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups.* Third ed., Grundlehren der Mathematischen Wissenschaften, 290, Springer-Verlag, New York, 1999.

[12] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics, Wiley-Interscience, New York, 1997.

[13] S. Glied and M. Baake, *Similarity versus coincidence rotations of lattices.* Z. Krist. **223**(2008), 770–772.

[14] S. Glied, *Similarity and coincidence isometries for modules.* Canad. Math. Bull., to appear. arXiv:1005.5237.

[15] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers.* Sixth ed., revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, Oxford, 2008.

[16] C. Huck, *A note on coincidence isometries of modules in Euclidean space.* Z. Krist. **224**(2009), 341–344.

[17] S. Louboutin, *Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratique imaginaires. Application.* C. R. Acad. Sci. Paris Ser. I Math. **310**(1990), no. 12, 795–800.

[18] D. A. Marcus, *Number fields.* Universitext, Springer-Verlag, New York-Heildelberg, 1977.

[19] P. A. B. Pleasants, M. Baake, and J. Roth, *Planar coincidences with N-fold symmetry.* J. Math. Phys. **37**(1996), no. 2, 1029–1058.   doi:10.1063/1.531424

[20] R. Scharlau, *Seminar über komplexe Multiplikation.* Parts 1, 2, and 3, available online at http://www.mathematik.uni-dortmund.de/~scharlau/research/

[21] J.-P. Serre, *A course in arithmetic.* Graduate Texts in Mathematics, 7, Springer-Verlag, New York-Heidelberg, 1973.

[22] C. L. Siegel, *Analytische Zahlentheorie. II.* lecture notes, edited by K. F. Kürten and G. Köhler, Univ. Göttingen (1964).

[23] N. J. A. Sloane, *The online encyclopedia of integer sequences.* http://www.research.att.com/~njas/sequences/.

[24] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres.* Second edition. Cours Spécialisés, 1, Société Mathématique de France, Paris, 1995.

[25] P. J. Weinberger, *Exponents of class groups of quadratic fields.* Acta Arith. **22**(1973), 117–124.

[26] D. B. Zagier, *Zetafunktionen und quadratische Körper.* Hochschultext, Springer-Verlag, Berlin-New York, 1981.

[27] P. Zeiner, *Symmetries of coincidence site lattices of cubic lattices.* Z. Krist. **220**(2005), 915–925.

Fakultät für Mathematik, Universität Bielefeld, 33501 Bielefeld, Germany
e-mail: mbaake@math.uni-bielefeld.de   pzeiner@math.uni-bielefeld.de

Fakultät für Mathematik, Universität Dortmund, 44221 Dortmund, Germany
e-mail: Rudolf.Scharlau@math.uni-dortmund.de