Essays on the arithmetic of quadratic fields

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Quadratic forms and quadratic extensions

In this essay I'll say something about the relationship between non-degenerate integral quadratic forms and lattices in quadratic field extensions. The main result will be a bijection between strict equivalence classes of lattices and proper equivalence of integral binary quadratic forms.

I'll illustrate this by looking at quadratic imaginary extensions. Real quadratic fields are more complicated (as well as more interesting), and I'll deal with them elsewhere.

Main results are perhaps essentially due to Gauss or even a predecessor, but I follow primarily [Davenport:1992].

Contents

1. Lattices ...

In this section I'll discuss briefly integral quadratic forms in arbitrary dimensions.

Suppose V to be a vector space of dimension n over $\mathbb{Q}$. I'll write vectors as column matrices. A basis of V is thus a horizontal array of vectors. If a coordinate system is in place, it may also be considered a matrix of size $n \times n$, whose columns are the vectors in the basis. The coordinate matrix x of a vector v with respect to the basis λ is defined by the condition that $v = \lambda x$. For example, if (λ, μ) is a basis of $\mathbb{R}^2$ then

$$x\lambda + y\mu = [\,\lambda \;\; \mu\,] \begin{bmatrix} x \\ y \end{bmatrix} .$$

A **lattice** in V is an embedded copy of $\mathbb{Z}^n$.

1.1. Lemma. *An additive subgroup of V is a lattice if and only if (i) it is a finitely generated and (ii) for every v in V some nv with $n > 0$ lies in L.*

A **quadratic function** on V is a function Q with values in $\mathbb{Q}$ such that

$$\nabla_Q(x, y) = Q(x + y) - Q(x) - Q(y)$$

is bilinear. Since $Q(2x) = 2\nabla(x, x)$ it is homogeneous of degree two. It is called **non-degenerate** if the bilinear form ∇ is non-degenerate. If (λ_i) is a basis of V then Q determines the **quadratic form**

$$Q(u) = \sum_{i,j} m_{i,j} x_i x_j \quad (m_{i,j} = \nabla(\lambda_i, \lambda_j)/2)$$

for $u = \sum x_i \lambda_i$. This can be written as

(1.2)
$$Q(u) = \sum_i m_{i,i} x_i^2 + \sum_{i<j} 2m_{i,j} x_i x_j \,.$$

It can also be expressed in matrix form:
$$Q(u) = {}^t x \, M_\lambda x \,.$$

Suppose we change the basis to $\mu = \lambda X$, with X an invertible matrix in $\mathrm{GL}_n(\mathbb{Q})$. It u is a vector in V then its coordinate arrays x, y are determined by the equation $u = \lambda x = \mu y$, which gives the coordinate transformation $x = Xy$. This leads directly to a formula for a transformed quadratic function. It is most simply given as a matrix equation:

$${}^t x \, M_\lambda x = {}^t y \, {}^t X M_\lambda X y = {}^t y \, M_\mu y \,.$$

The matrix of Q with respect to the basis μ is hence

(1.3)
$$M_\mu = {}^t X M_\lambda X \,.$$

The bilinear form ∇_Q may also be expressed as a matrix product:

$$\nabla(u, v) = 2 \, {}^t x M_\lambda y \quad (u = \lambda x, v = \lambda y) \,.$$

The matrix M_λ is non-singular if and only if the quadratic form is non-degenerate.

If L is a lattice in V, a choice of basis will determine a quadratic form. A change of basis will change the form by a matrix X in $\mathrm{GL}_n(\mathbb{Z})$, according to (1.3) . The two forms will be called **properly equivalent** if $\det(X) = 1$.

Given Q, the lattice L is called **integral** if Q takes integral values on it. Equivalent is the condition that the coefficients in (1.2) , determined by a basis of L, be integral. The $m_{i,j}$ for $i \neq j$ are allowed to be half-integral. I should point out that this convention as to what constitutes an integral lattice is not universal. Some authors, including Gauss, require that the matrix M_λ have integral entries.

Suppose S to be any set of rational numbers with the property that $n|S|$ is contained in the positive integers for some $n > 0$. Since every set of positive integers has a minimum element, the set $n|S|$ possesses a greatest common divisor, say g. Then g/n is the greatest common divisor of S. In particular, if L is a lattice in V the image $Q(L)$ has a greatest common divisor, which I'll call $\Gamma(L)$. It is often called the **norm** of L.

An integral form is called **primitive** if $\Gamma(L) = 1$. Thus a lattice L is always primitive with respect to $Q/\Gamma(L)$.

1.4. Lemma. *Suppose L to be a lattice in V. If*

$$Q(u) = \sum_{i \le j} q_{i,j} x_i x_j$$

is the quadratic form corresponding to some basis of L, then $\Gamma(L)$ is the greatest common divisor of the $q_{i,j}$.

The group GO_Q is made up of all the linear transformations T if V such that $Q(T(u)) = c\,Q(u)$ for every u in V and some scalar c, which I define to be $\mathrm{NM}(T)$. The map taking T to $\mathrm{NM}(T)$ is a homomorphism. The following is elementary:

1.5. Lemma. *For T in GO_Q we have $\Gamma(TL) = |\mathrm{NM}(T)| \cdot \Gamma(L)$.*

The **discriminant** D_L of the lattice is

$$\big|\det(2M_\lambda)\big| = 2^n \big|\det(M_\lambda)\big| \,.$$

Because of (1.3) , this is independent of the choice of basis.

Define

$$L^\perp = \{v \in \mathbb{R}^n \,|\nabla(v, L) \subseteq \mathbb{Z}\} .$$

It is a lattice if and only if Q is non-degenerate, and then has as basis the dual $(\lambda_i^\vee)$ of the basis (λ_i) with respect to ∇, which is

$$\lambda^\vee = \lambda(2M_\lambda)^{-1} .$$

Hence:

1.6. Proposition. *If the restriction of Q to the lattice L is integral, then L is contained in $L^\perp$, and its index in $L^\perp$ is equal to the discriminant.*

Remark. There are really two different discriminants associated to a rational quadratic form. The one just defined might be called the **integral** or **lattice** discriminant. One point of this discriminant, which I shall not pursue here, is that it tells you about the quadratic forms induced on the finite groups L/NL. The **radical** of Q on L/NL is the subspace of all u in V such that $\nabla_Q(u, L) \equiv_N 0$. This is the same as $NL^\perp \cap L$. It is trivial if and only if N is relatively prime to the discriminant. The best measure of how bad things are is the set of principal divisors of $L^\perp/L$.

For example, the quadratic form is badly behaved in characteristic 2. If $L = \mathbb{Z}^2$, then $L^\perp = (1/2)L$, and the discriminant is 4.

There is another way to see it. The function ∇_Q is in some sense the gradient of Q, since formally

$$Q(x + h) = Q(x) + \nabla(x, h) + O(h^2) .$$

Whether the linear form $h \mapsto \nabla(x, h)$ is non-trivial or not measures the singularity of the algebraic variety $Q(x) = c$ at x.

The other I'll call the **rational discriminant**. It is usually defined as the image of $\det(M)$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, but in order to be consistent with my earlier definition, I'll define it to be the image of $\det(2M_\lambda)$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. In any case, a rational change of basis leaves this discriminant invariant.

2. ... in dimension two

Suppose $F = \mathbb{Q}(\sqrt{N})$ to be a quadratic field extension of $\mathbb{Q}$, with N square-free. I fix once and for all one of the square roots of N, which I'll express as $\sqrt{N}$. Let

$$\mathrm{IM}(x + y\sqrt{N}) = y .$$

The map

$$\sigma\colon\ \lambda = x + y\sqrt{N} \longmapsto \overline{\lambda} = x - y\sqrt{N}$$

is the unique non-trivial automorphism of F. Define also

$$\mathrm{TR}(\lambda) = \lambda + \overline{\lambda}, \quad \mathrm{NM}(\lambda) = \lambda\overline{\lambda} ,$$

which take values in $\mathbb{Q}$. The multiplicative homomorphisms NM is an **anisotropic** quadratic form, which means that $\mathrm{NM}(\lambda) = 0$ if and only if $\lambda = 0$. Multiplication by an element of $F^\times$ is in $\mathrm{GO}_{\mathrm{NM}}$.

2.1. Lemma. *The group $\mathrm{GO}_{\mathrm{NM}}$ is the semi-direct product of $F^\times$ and $\{1, \sigma\}$.*

Proof. This reduces to the claim that if $g \neq 1$ lies in $\mathrm{GO}_{\mathrm{NM}}$ and $g(1) = 1$ then $g = \sigma$. ▮

In the rest of this section I'll construct bijections between three sets.

THE SETS. **(1)** If L and M are two lattices in F, they are **strictly similar** if and only if $L = \alpha M$ with $\mathrm{NM}(\alpha) > 0$. I define $\mathfrak{A}$ to be the set of strict similarity classes of F-lattices.

(2) A quadratic form

$$ax^2 + bxy + cy^2$$

will be called F-admissible if (1) its rational discriminant (the image of $b^2 - 4ac$ modulo $\mathbb{Q}^2$) agrees wutrh N and (2) a is the product of an element of $\mathbb{Q}^\times_{>0}$ and something in $\mathrm{NM}(F^\times)$. Again, if F is real this is no restriction, but if it is quadratic imaginary, a must be positive.

Suppose Q and R to be F-admissible forms. I'll call them properly equivalent if their matrices satisfy an equation

$$M_R = \rho \cdot {}^t X M_Q X$$

with $\rho > 0$ in $\mathbb{Q}^\times$ and X in $\mathrm{SL}_2(\mathbb{Z})$. I define $\mathfrak{B}$ to be the set of such proper equivalence classes.

(3) Suppose ω to lie in $F^\times$. I'll call it F-admissible if $\mathrm{IM}(\omega)$ lies in $\mathrm{NM}(F^\times) Cdot \mathbb{Q}^\times$. Again, if F is real this is no restriction, but if it is quadratic imaginary, it eliminates half of $F^\times$.

2.2. Lemma. *For any ω in $F^\times$ and*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\mathrm{IM}\left(\frac{a\omega + b}{c\omega + d}\right) = \frac{\det(A) \cdot \mathrm{IM}(\omega)}{(c\omega + d)(c\overline{\omega} + d)} .$$

Hence the set of F-admissible ω is stable under the action of $\mathrm{SL}_2(\mathbb{Z})$.

I'll say that ω_1 and ω_2 in $F^\times$ are properly equivalent if

$$\omega_1 = \frac{a\omega_2 + b}{c\omega_2 + d}$$

with

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

in $\mathrm{SL}_2(\mathbb{Z})$. Let $\mathfrak{C}$ be the set of such proper equivalence classes. (According to Theorem of [Hardy-Wright:1960], this happens if and only if the continued fractions of ω_1 and ω_2 have common tails.)

THE MAPS. I am next going to define maps among these three sets that will turn out to be bijections.

(1) $\mathfrak{ab}$ I'll say that a pair $\Lambda = (\lambda, \mu)$ in F is **positively oriented**, or sometimes just **positive**, and write $\Lambda \succ 0$, if

$$\mathrm{IM}\det\left(\begin{bmatrix} \lambda & \mu \\ \overline{\lambda} & \overline{\mu} \end{bmatrix}\right) = \frac{\lambda\overline{\mu} - \overline{\lambda}\mu}{2\sqrt{N}} > 0$$

Thus in $\mathbb{Z}[\sqrt{N}]$ the basis $(\sqrt{N}, 1)$ is positively oriented. If (λ, μ) is not positively oriented, then (μ, λ) is, so that every lattice possesses a positively oriented basis, which will be unique to up transformations $M = \Lambda X$ with X in $\mathrm{SL}_2(\mathbb{Z})$.

Suppose L to be a lattice in F with basis $\Lambda = (\lambda, \mu) \succ 0$. To these data is associated the quadratic form

$$Q_\Lambda(x, y) = (x\lambda + y\mu)(x\overline{\lambda} + y\overline{\mu}) = Ax^2 + Bxy + Cy^2$$

with

$$\begin{aligned} A &= \mathrm{NM}(\lambda) \\ B &= \mathrm{TR}(\lambda\overline{\mu}) \\ C &= \mathrm{NM}(\mu) . \end{aligned}$$

Note that if

$$\Delta = \det\left(\begin{bmatrix} \lambda & \mu \\ \overline{\lambda} & \overline{\mu} \end{bmatrix}\right)$$

then $\Delta^2 = B^2 - 4AC$.

Dividing by the (positive) greatest common divisor of A, B, C, we get in turn the primitive form

$$q_\Lambda(x,y) = \frac{Q_\Lambda(x,y)}{\Gamma(L)} = ax^2 + bxy + cy^2 \, .$$

If a different oriented basis Λ is chosen, then q_Λ is transformed by a matrix in $\mathrm{SL}_2(\mathbb{Z})$, hence to a properly equivalent form. I'll call q_L the proper equivalence class of q_Λ.

If γ is an element of $F^\times$ with $\mathrm{NM}(\gamma) > 0$ then multiplication by γ takes Λ to $(\gamma\lambda, \gamma\mu)$, which is also positive. The associated primitive form is again q_L. The map $L \mapsto q_L$ therefore induces a well defined map $\mathfrak{ab}$ from $\mathfrak{A}$ to $\mathfrak{B}$.

(1) $\mathfrak{ac}$ Given $\Lambda = (\lambda, \mu) \succ 0$, map it to $\omega = \lambda/\mu$. If $c = \mathrm{NM}(\mu)$, then $\mathrm{IM}(c\omega) > 0$.

(2) $\mathfrak{bc}$ Suppose given an F-admissible binomial form

$$ax^2 + bxy + cy^2 \, .$$

Multiplying by a positive rational, one may assume that a, b, and c are relatively prime integers. This form can be factored as

$$c(y - \gamma x)(y - \overline{\gamma} x)$$

with

$$\gamma = \frac{-b - \sqrt{D}}{2c} \, ,$$

which I'll call its **characteristic root**. It is characterized by the condition that $\mathrm{IM}(c\gamma) < 0$. I'll then define its **characteristic element** to be $\omega = -\gamma$. If the form is transformed by

$$P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

in $\mathrm{GL}_2(\mathbb{Z})$ then ω changes to

$$P(\omega) = \frac{p\omega + q}{r\omega + s} \, .$$

We have thus defined a map $\mathfrak{bc}$ from $\mathfrak{B}$ to $\mathfrak{C}$.

(3) $\mathfrak{ca}$ Given ω, choose $\alpha \neq 0$ in $F^\times$ such that

$$\alpha\overline{\alpha} \cdot \mathrm{IM}(\omega) > 0 \, .$$

Associate to ω the lattice basis $(\alpha\omega, \alpha)$. Since

$$\det \begin{bmatrix} \alpha\omega & \alpha \\ \overline{\alpha\omega} & \overline{\alpha} \end{bmatrix} = \alpha\overline{\alpha}(\omega - \overline{\omega}) \, ,$$

it is a positive basis of some lattice L_ω in F, well defined up to strict similarity. This defines a map $\mathfrak{ba}$ from $\mathfrak{B}$ to $\mathfrak{A}$.

(2) $\mathfrak{ba}$ Map the form first to its characteristic element, then to a lattice as in the previous definition.

(3) $\mathfrak{cb}$ Associate to ω the form

$$c(x\omega + y)(x\overline{\omega} + y)$$

in which c is chosen so that (1) the form is primitive and (2) $\mathrm{sgn}(c) = \mathrm{sgn}(\mathrm{IM}(\omega))$.

Examples. Suppose that the form associated to ω is

$$ax^2 + bxy + cy^2 .$$

This means, in addition to the sign compatibility, that

$$\omega + \overline{\omega} = b/c, \quad \omega\overline{\omega} = a/c .$$

Since

$$\frac{1}{\omega} + \frac{1}{\overline{\omega}} = b/a, \quad \frac{1}{\omega\overline{\omega}} = c/a, \quad \frac{1}{\omega} - \frac{1}{\overline{\omega}} = -(\omega - \overline{\omega})(c/a) ,$$

we have the following related assignments

$$\begin{aligned} \overline{\omega}\colon &\ -ax^2 - bxy - cy^2 \\ -\omega\colon &\ -ax^2 + bxy - cy^2 \\ 1/\omega\colon &\ -cx^2 - bxy - ay^2 \\ 1/\overline{\omega}\colon &\ cx^2 + bxy + ay^2 \\ -1/\overline{\omega}\colon &\ -cx^2 + bxy - ay^2 . \end{aligned}$$

∘ ———— ∘

2.3. Theorem. *All these maps are bijections.*

Proof. It is an immediate consequence of definitions that the maps $\mathfrak{ab}\cdot\mathfrak{ba}$, $\mathfrak{ac}\cdot\mathfrak{ca}$, $\mathfrak{ba}\cdot\mathfrak{ab}$, $\mathfrak{bc}\cdot\mathfrak{cb}$, $\mathfrak{ca}\cdot\mathfrak{ac}$, and $\mathfrak{cb}\cdot\mathfrak{bc}$ are all identity maps on the sets of equivalences. ∎

3. Orders

The partition into proper equivalences in the previous section can be refined somewhat. If L is a lattice in F, its **endomorphism ring** $\mathrm{End}(L)$ is the ring of all γ in F such that $\gamma L \subseteq L$. These can be characterized very nicely.

INTEGERS. An **integer** in F is an element γ whose characteristic polynomial is monic. Equivalently, $\mathrm{TR}(\gamma)$ and $\mathrm{NM}(\gamma)$ are both in $\mathbb{Z}$.

3.1. Lemma. *The element γ is an integer of F if and only if multiplication by γ takes some lattice in F into itself.*

Proof. One way because given a basis of the lattice, multiplication by γ is expressed as multiplication by a matrix in $M_2(\mathbb{Z})$.

The other because if the characteristic polynomial of γ is monic, the lattice spanned by 1 and γ is stable under multiplication by γ:

$$\begin{aligned} \gamma\cdot 1 &= \gamma \\ \gamma\cdot\gamma &= -b\gamma - c . \end{aligned}$$ ∎

An **order** in F is a subring (containing 1) that is also a lattice.

3.2. Proposition. *The ring of integers in F is an order.*

Proof. If α and β are integers then multiplication by either $\alpha + \beta$ or $\alpha\beta$ takes the $\mathbb{Z}$-module spanned by 1, α, β, and $\alpha\beta$ into itself. Hence the integers are a ring.

If γ lies in F then some positive multiple of γ will lie in $\mathfrak{o}$. Therefore we can find a basis (λ, μ) of F contained in $\mathfrak{o}$. Let L be the lattice they span. Then

$$L \subseteq \mathfrak{o} \subseteq \mathfrak{o}^\perp \subseteq L^\perp .$$

Hence $\mathfrak{o}$ is a finitely generated module over $\mathbb{Z}$ and therefore by Lemma 1.1 it is a lattice.

3.3. Proposition. *If $F = \mathbb{Q}(\sqrt{N})$ with N square-free, its ring of integers $\mathfrak{o}$ has as basis 1 and ω_N, where*

$$\omega_N = \begin{cases} \dfrac{1+\sqrt{N}}{2} & \text{if } N \equiv_4 1 \\ \sqrt{N} & \text{if } N \equiv_4 2 \text{ or } 3. \end{cases}$$

For example, the integers in $\mathbb{Q}(\sqrt{-1})$ are generated over $\mathbb{Z}$ by $\sqrt{-1}$, while those in $\mathbb{Q}(\sqrt{-3})$ are generated by $(1 + \sqrt{-3})/2$.

3.4. Corollary. *If $F = \mathbb{Q}(\sqrt{N})$, the norm form on $\mathfrak{o}_F$ is*

$$\begin{cases} m^2 + mn + \left(\dfrac{1-N}{4}\right) n^2 & \text{if } N \equiv_4 1 \\ m^2 + Nn^2 & \text{otherwise.} \end{cases}$$

Let $D_N = D_F$ be the corresponding discriminant. It is N in the first case, $4N$ in the second.

I'll call the discriminant of the integer lattice of a quadratic extension a **minimal** discriminant. These are precisely the integers D with either (i) $D \equiv_4 1$ and square-free or (ii) $D \equiv_4 0$, $D/4 \equiv_4 2$ or 3 and square-free.

3.5. Lemma. *If γ is an integer in F but not in $\mathbb{Q}$, then the lattice with basis $(\gamma, 1)$ is an order. Conversely every order in F has a basis $(\gamma, 1)$ with γ in $\mathfrak{o}$.*

Proof. One way is an immediate consequence of Lemma 3.1.

For the other, suppose $\mathfrak{r}$ to be an order in F, say with basis λ, μ. By Lemma 3.1, they are all integers.

Since 1 is in $\mathfrak{r}$, we may write

$$1 = a\lambda + b\mu .$$

The greatest common divisor of a and b is certainly 1, so we can find ℓ, m such that $am + \ell b = 1$. But then

$$[\lambda \quad \mu] \begin{bmatrix} a & -\ell \\ b & m \end{bmatrix} = [1 \quad -\ell\lambda + m\mu] = \text{(say) } [1 \quad \gamma]$$

is also a basis of $\mathfrak{r}$.

3.6. Proposition. *Every order in F is contained in the ring $\mathfrak{o}_F$.*

Proof. Choose a basis of the order $\mathfrak{r}$, and γ in $\mathfrak{r}$. Then multiplication by γ amounts to matrix multiplication by an integral matrix, so its characteristic polynomial is monic and integral.

3.7. Lemma. *The orders in F_N are the lattices with basis 1, $f\omega_N$ for some $f > 0$.*

Proof. Suppose $\mathfrak{r}$ to be an order in F_N. It certainly contains 1 as part of a basis. Suppose $a + b\omega_N$ lie in $\mathfrak{r}$ with $f > 0$ smallest. Then $f\omega_N$ is also in $\mathfrak{r}$, and any other element of $\mathfrak{r}$ will be of the form $a + bf\omega_N$.

3.8. Lemma. *The discriminant of the order $\mathbb{Z}[f\omega_N]$ is*

$$\begin{cases} f^2 N & \text{if } N \equiv_4 1 \\ 4f^2 N & \text{otherwise.} \end{cases}$$

In particular, *the orders are distinguished by their discriminants*. The possible discriminants are all those $D \equiv_4 0$ or 1. Every possible discriminant has a unique factorization as $f^2 D_F$ for some quadratic extension $F = F_N$.

Let $\mathfrak{r}_D$ be the unique order with discriminant D.

LATTICE ENDOMORPHISMS. If L is a lattice in F, its **endomorphism ring** $\mathrm{End}(L)$ is that of all α in F such that $\alpha L \subseteq L$. *If* L *has basis* (λ, μ)*, what is* $\mathrm{End}(L)$*?*

3.9. Proposition. *Let*

$$ax^2 + bxy + cy^2$$

be the characteristic form associated to the positively oriented basis (λ, μ) *of the lattice* L*. The associated characteristic root is* $\gamma = -\mu/\lambda$*, and satisfies the quadratic equation*

$$a\gamma^2 + b\gamma + c = 0\,.$$

Then $\mathrm{End}(L)$ *is the ring* $\mathbb{Z}[a\gamma]$.

Note that $a\gamma$ is an integer.

Proof. For the first assertion:

$$\begin{aligned} Ax^2 + Bx + C &= (x\lambda + \mu)(x\overline{\lambda} + \overline{\mu}) \\ &= |\lambda|^2 (x + \mu/\lambda)(x + \overline{\mu}/\overline{\lambda}) \\ &= |\lambda|^2 (x - \gamma)(x - \overline{\gamma})\,. \end{aligned}$$

For the second, let $\lambda = x + y\gamma$. The lattice $(\!(\lambda, \mu)\!)$ is similar to $(\!(1, \gamma)\!)$, and the endomorphism rings of similar lattices are the same. Since

$$\begin{aligned} \lambda \cdot 1 &= \quad x + y\gamma \\ \lambda \cdot \gamma &= -\left(\frac{cy}{a}\right) + \left(x - \frac{by}{a}\right)\gamma\,, \end{aligned}$$

λ lies in $\mathrm{End}(L)$ if and only if x, y, cy/a, by/a are all integers. But a, b, c have greatest common divisor equal to 1. Therefore it is required that x, y, and y/a all be integers.

3.10. Corollary. *Suppose* L *to be a lattice in* F *with characteristic form* $ax^2 + bxy + cy^2$*. The ring* $\mathrm{End}(L)$ *is the unique order of* F *whose discriminant is* $b^2 - 4ac$*.*

In other words, a primitive form associated to L has the same discriminant as $\mathrm{End}(L)$. In other words, the lattices stable with respect to $\mathfrak{o}_D$ are those whose discriminant divides D.

It remains to describe the classification of reduced non-degenerate forms. I'll do this for positive definite ones in the rest of this essay.

4. Positive definite quadratic forms

This section will explain how to classify the equivalence classes of lattices in quadratic imaginary extensions of $\mathbb{Q}$, along related material.

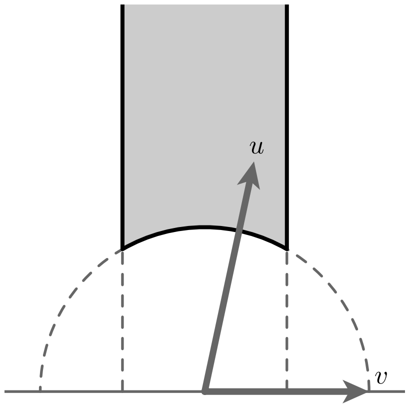
COMPLEX LATTICES. If $N < 0$ then $F = \mathbb{Q}(\sqrt{N})$ embeds into $\mathbb{C}$. Because I have fixed $\sqrt{N}$, the embedding is unique if we require that the image of $\sqrt{N}$ lies in the upper half-plane. A lattice in F determines therefore a lattice in $\mathbb{C}$, and it is useful to consider those.

Suppose L to be a lattice in $\mathbb{C}$. Since

$$\det \begin{bmatrix} u & v \\ \overline{u} & \overline{v} \end{bmatrix} = |u|^2\,\mathrm{IM}(u/v)\,,$$

a positively oriented basis of L in this case is a basis (u, v) with $\mathrm{IM}(u/v) > 0$.

Suppose L to be a lattice in $\mathbb{C}$ with basis $(u, v) \succ 0$. It is unique up to projective transformation by an element of $\mathrm{SL}_2(\mathbb{Z})$. The basis is called **reduced** if (i) $|v|$ is the minimum length of elements in L and (ii) the projection of u onto the line through v lies in the closed interval $[-v/2, v/2]$.



4.1. Proposition. *Every lattice in $\mathbb{C}$ possesses a reduced positively oriented basis.*

Proof. Choose v of minimum length in the given lattice L. It is a primitive vector, so there exists u in $\mathbb{C}$ such that (u, v) are a basis of L. Changing sign if necessary, we may assume $\mathrm{IM}(u/v) > 0$. This u is unique satisfying this condition up to translation by some nv. The projection condition will be satisfied for $u - nv$ if and only if

$$-1/2 \le \frac{(u - nv) \bullet v}{v \bullet v} \le 1/2\,,$$

which translates to

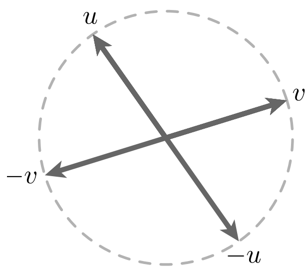
$$n \le \frac{u \bullet v}{v \bullet v} + \frac{1}{2} \le n + 1\,.$$

This is satisfied by

(4.2)
$$n = \left\lfloor \frac{u \bullet v}{v \bullet v} + \frac{1}{2} \right\rfloor\,.$$

This concludes the proof of the Proposition.

The reduced basis produced above is almost unique. Of course there is always a simple kind of n0on-uniqueness, since if (u, v) is reduced so is $(-u, -v)$. But there can be some additional ambiguity. First of all, $\pm v$ might not be unique—there might well be another vector u with $|u| = |v|$.

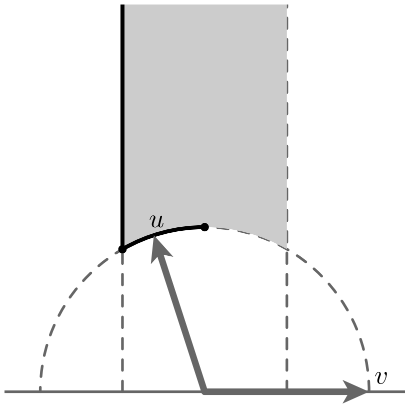


In this case the reduced bases are

$$\begin{array}{l} (\ \ u,\ \ \ v) \\ (-u, -v) \\ (\ \ v, -u) \\ (-v,\ \ \ u)\,. \end{array}$$

Otherwise, $\pm v$ is indeed unique. Given v, any possible u must be of the form $u - nv$ with n in $\mathbb{Z}$. As long as u does not project onto $\pm v$, it, too, is unique. But if it does so project, we may translate if necessary so that it projects onto $-v$.

A basis (u, v) is called **strictly** reduced if either (i) $|v| < |u|$ and the projection of u onto the line through v lies in $[-v/2, v/2)$ or (ii) $|u| = |v|$ and the projection of u onto the line through v lies in $[-v/2, 0]$.



We have thus proved:

4.3. Corollary. *Every form is equivalent to a unique strictly reduced form.*

The proof is not constructive, but there is a simple algorithm for finding the relevant strictly reduced basis.

Start with (u, v).
$\circ$ Replace u with $u - nv$, where

$$n = \left\lfloor \frac{u \bullet v}{v \bullet v} + \frac{1}{2} \right\rfloor .$$

If $|u| > |v|$, swap $(-v, u)$ for (u, v) and loop to $\circ$.
Otherwise, if $(u \bullet u)/(v \bullet v) > 0$ swap $(-v, u)$ for (u, v) and exit with the reduced basis (u, v).

In principle, this procedure works for any positive basis of $\mathbb{C}$, but in practice floating point errors restrict its practicality. The most important casde is when u and v belong to some quadratic field extesnion of $\mathbb{Q}$, and in that case it is simplest to transfer the problem to one involving integral quadratic forms.

Suppose F to be such a quadratic field, L a lattice in F, (u, v) a positive basis of L. This determines by restriction of the complex norm $|z|^2$ the positive definite quadratic form

$$(xu + yv)(x\overline{u} + y\overline{v}) = ax^2 + bxy + cy^2$$

with values in $\mathbb{Q}$. Scaling if necessary by a positive scalar, one may assume the form to be integral and primitive. The requirement that the basis be reduced means (i) $|a| \le |c|$ and (ii) $|b| \le |a|$.

The algorithm for finding a reduced form goes on (where (a, b, c) is a shortened way to denote the form):

$\circ$ Find n such that

$$-a \le b - 2na < a ,$$

Calculate a new value of c by making discriminants agree.
If $|a| > |c|$, change (a, b, c) to $(c, -b, (D - 4a))$. Loop to $\circ$.
Otherwise, exit with the reduced form (a, b, c).

COMPUTATION. *How to compute the reduced forms of a given discriminant D?* Because $D = b^2 - 4ac$ and $D < 0$ while $0 < a \le c$, one can deduce that

$$b^2 \le ac \le D/3 .$$

Also, b must be even if $D \equiv_4 0$ and odd if $D \equiv_4 1$. So we should scan through all b of suitable parity from 0 to $\lfloor\sqrt{D/3}\rfloor$, and for each factor, if possible, $ac = (D + b^2)/4$. Reject all for which $|b| \le |a| \le |c|$ does not hold.

EXAMPLES. **(1)** Take $D = -3$. Then $N = 3$, and the unique reduced form is $m^2 + mn + n^2$.

(2) Take $D = -4$. Then $N = 1$, and the only reduced form is $m^2 + n^2$.

(3) Take $D = -12$. Then $N = 3$, and the reduced forms are $m^2 + 3n^2$ and $2m^2 + 2mn + 2n^2$. The last is not primitive.

(4) Take $D = -20$. Then $N = 5$, and the two reduced forms are $m^2 + 5n^2$ and $2m^2 + 2mn + 3n^2$.

GENERATORS. There is another valuable application of the preceding algorithm. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane discretely, and the set of strictly reduced forms is a fundamental domain for the action. The preceding algorithm thus records an expression for any element γ of $\mathrm{SL}_2(\mathbb{Z})$ as a product of matrices S and $T(n)$

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$T(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

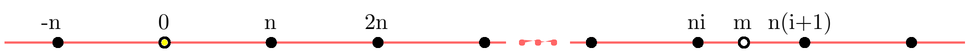
Howvere, there is some ambiguity in a factor of a matrix that takes Q to itself. This group is just $\pm I$ for strictly reduced Q for the forms $x^2 + y^2$, $x^2 \pm xy + y^2$. In these cases, the subgroups are isomorphic to μ_4 and μ_6.

5. Euclidean domains

There are several simple cases in which there is only one reduced form with discriminant D.

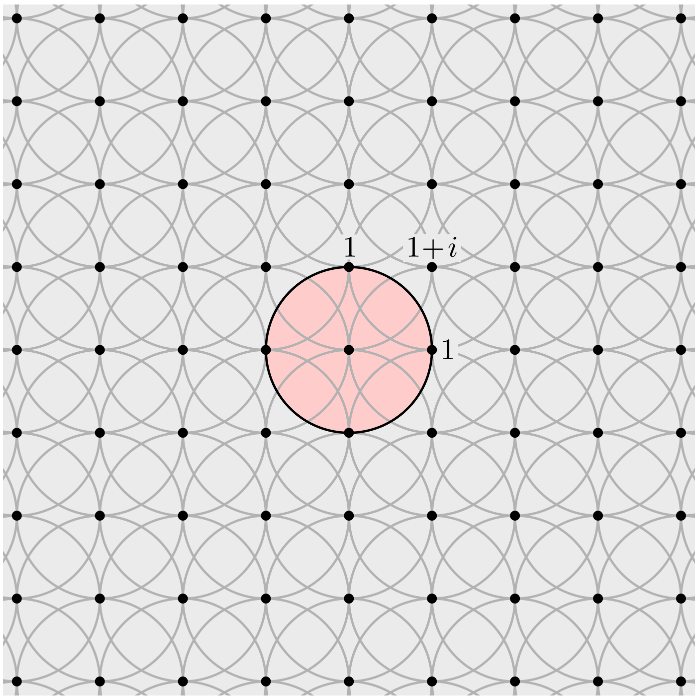
If all lattices stable under $\mathfrak{r}$ are generated by a single element, $\mathfrak{r}$ is said to be a **principal ideal domain**. There is one simple sufficient condition for this to happen, when $\mathfrak{r}$ has a division algorithm. In this section I'll use visual techniques in several cases to see that this is true.

I'll recall first how to prove that $\mathbb{Z}$ is a principal ideal domain. This means that any ideal is made up of multiples of a single element. Suppose I to be an ideal in $\mathbb{Z}$, and suppose n to be a positive element in I of least magnitude. Thsi implies that if m is any integer in I with $|m| < |n|$ then $m = 0$—or, equivalently, that if $|m - ni| < n$ then $m = ni$. But the division algorithm implies that the open intervals $(ni - n, ni + n)$ cover $\mathbb{Z}$, so that indeed every element of I is a multiple of n.

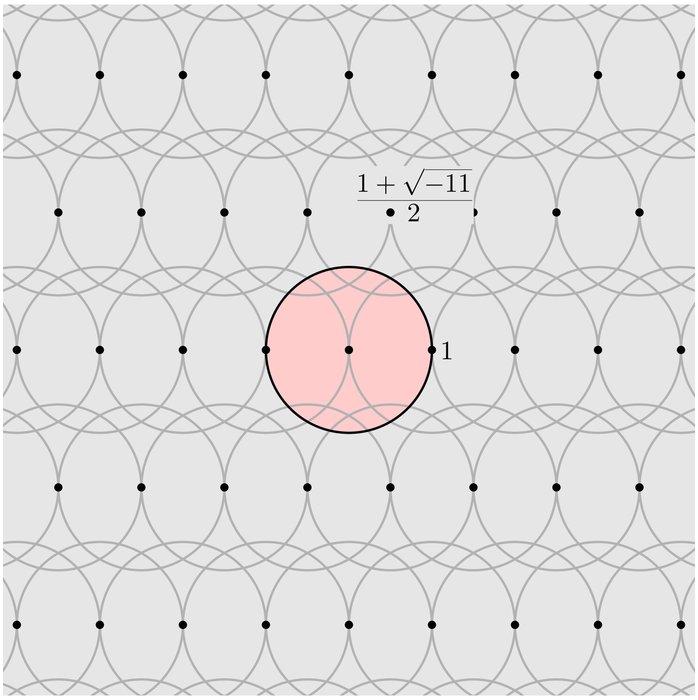


Of course, what the picture really illustrates is the division algorithm in $\mathbb{Z}$, which when applied in Euclid's algorithm leads to an explicit generator of any ideal in $\mathbb{Z}$.

Something similar happens for the Gaussian integers $\mathfrak{o} = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$. Here, the open unit discs around each of the z in $\mathfrak{o}$ cover all of $\mathbb{C}$:



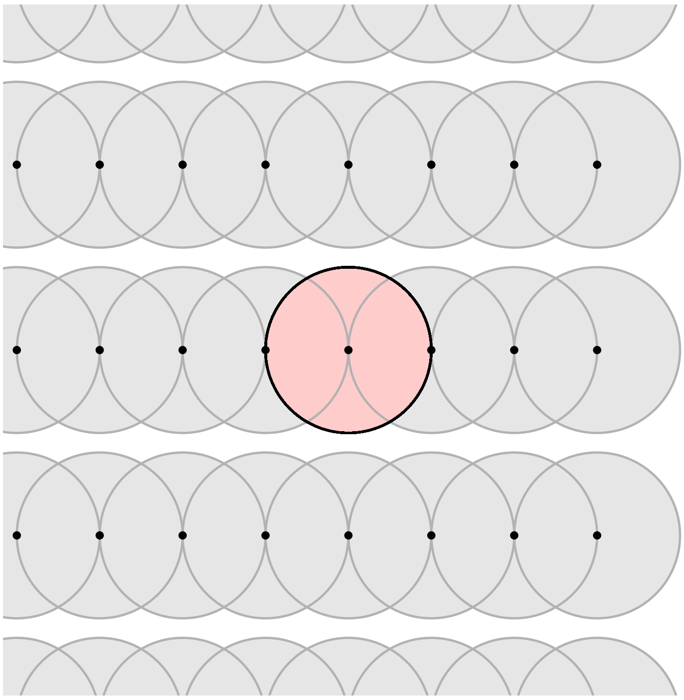
This is also true for the integral rings $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}(\omega_3]$, $\mathbb{Z}[\omega_7]$, and $\mathbb{Z}[\omega_{11}]$ (where $\omega_N = (1+\sqrt{-N})/2$), as the following picture suggests: :



5.1. Proposition. *Let $\mathfrak{o}$ be the ring of integers in a quadratic imaginary extension of $\mathbb{Q}$, embedded in $\mathbb{C}$. If the open unit disks around integers in $\mathfrak{o}$ cover $\mathbb{C}$, then every ideal I in $\mathfrak{o}$ is principal.*

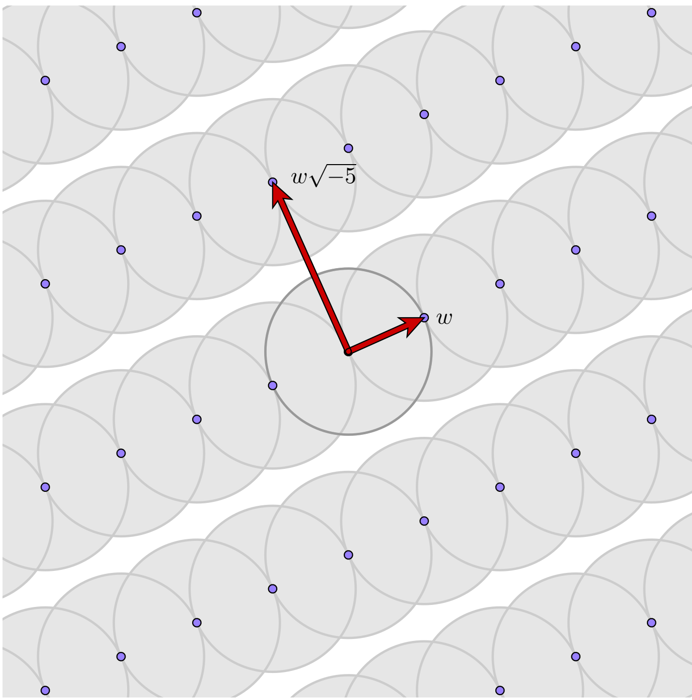
Proof. Let $\alpha \neq 0$ an element of I of smallest magnitude. Scaling the diagram by α, we deduce that open discs of radius $|\alpha|$ cover $\mathbb{C}$. If β is any of I, it will will therefore lie within distance $|\alpha|$ of some element γ of $\mathfrak{o} \cdot \alpha$. But because $|\alpha|$ is minimum, β must in fact be γ.

This argument fails, however, for $\mathbb{Z}[\sqrt{-5}]$:

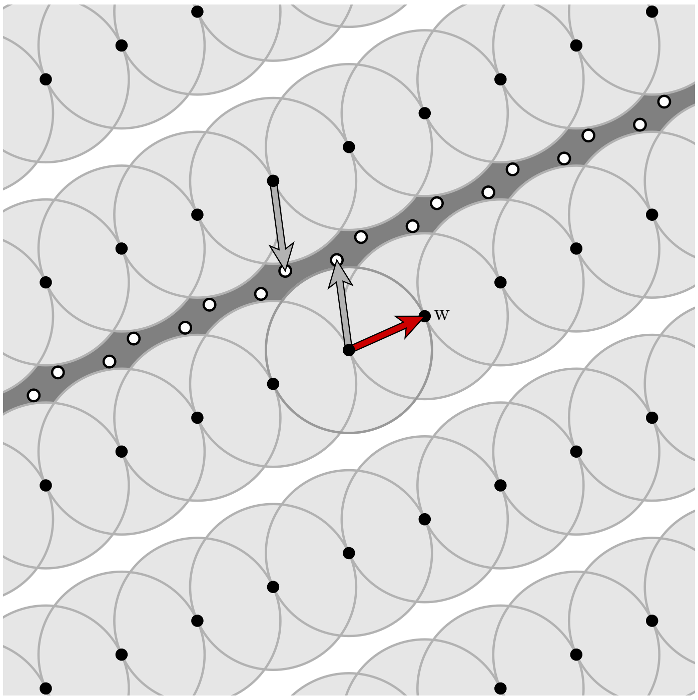


Interestingly, though, the same picture tells us more precisely how far this ring is from being a principal ideal domain.

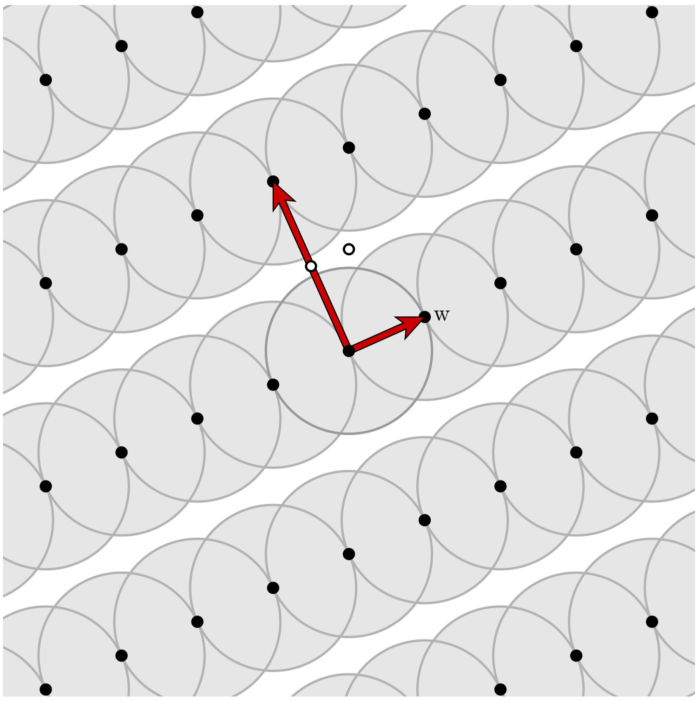
Suppose I to be an ideal in $\mathbb{Z}[\sqrt{-5}]$, and suppose w to be of least magnitude in I. Building the lattice $L = \mathbb{Z}[\sqrt{-5}] \cdot w$ we get this picture:



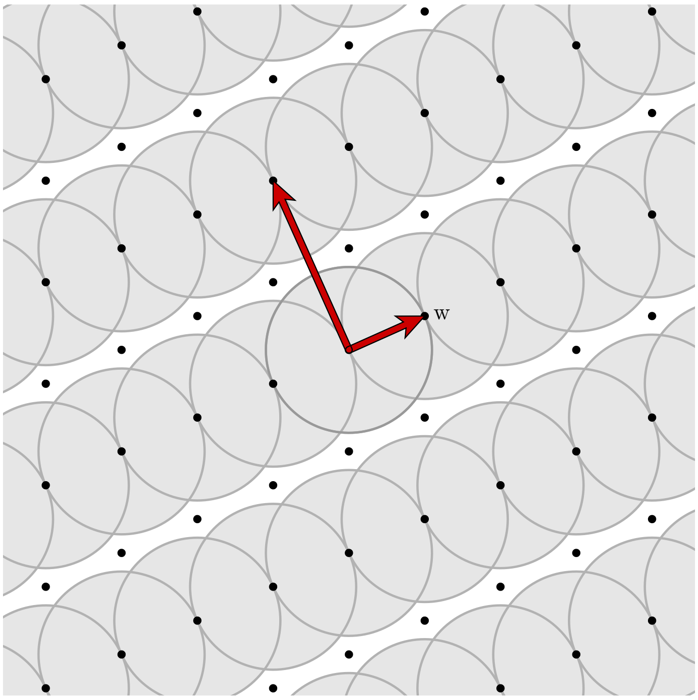
Since w is of least magnitude, there are no elements of I within unit distance of any element of L. If I is not identical with the principal ideal L it must contain a point in the dark area in the following figure:



If it lies at (x, y) there must also be elemnts of I of the form $(x + w, y)$, and by symmetry $-x + w, \sqrt{-5} - y)$. This will contradict the assumption on w unless $x = 0$ or $x = 1/2$, and $y = \sqrt{-5}/2$, as indicated in this picture:

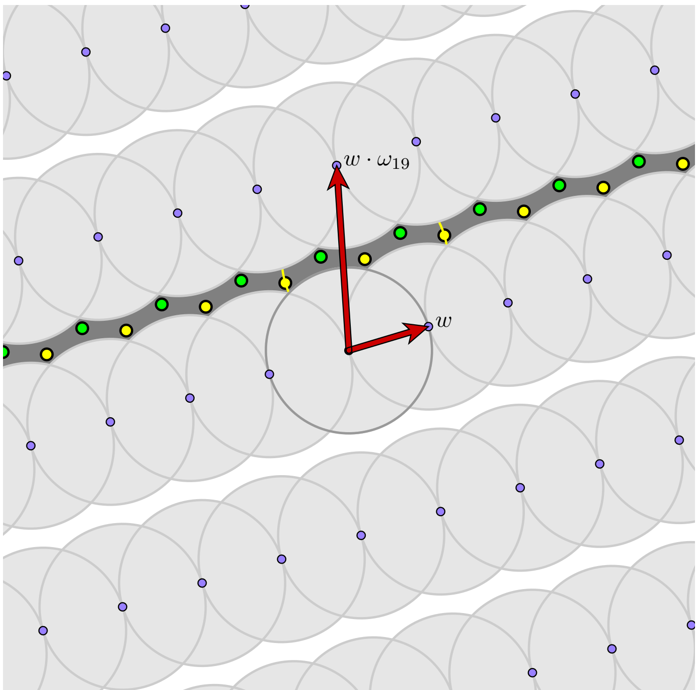


Since $\sqrt{-5}\,\alpha = (5/2)w$, the ideal I cannot contain α. But it can very well contain β, and the points in I then look like this:



The class number of $\mathbb{Z}[\sqrt{-5}]$ is hence 2.

In the case of the ring $\mathbb{Z}[\sqrt{-19}]$. unit circles around its elements do not cover $\mathbb{C}$, but an argument similar to that we have just seen will show that it is nonetheless a principal ideal domain.



The other complex imaginary quadratic fields with class number 1 are $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$. I have not tried looking at those cases. That these have class number one is an elementary application of Gauss' algorithm, but that these are all the ones with this property was only a conjecture of Gauss up until the mid-twentieth century.

6. References

1. Harold Davenport, **The higher arithmetic**, Cambridge University Press, 1992.

2. Peter G. Lejeune-Dirichlet, **Vorlesungen über Zahlentheorie**, Braunschweig, 1863.

3. Carl Friedrich Gauss, **Disquisitiones arithmeticae**, 1801. An English translation from the original Latin by Arthur A. Clarke was published by Yale University Press in 1965.

4. G. H. Hardy and E. M. Wright, **An introduction to the theory of numbers** (fourth edition), Oxford University Press, 1960.