Quadratic Fields

Even when one's primary interest is in integer solutions to equations, it can sometimes be very helpful to consider more general sorts of numbers. For example, when studying the principal quadratic form $x^2 - Dy^2$ of discriminant $4D$ it can be a great aid to understanding to allow ourselves to factor this form as $(x + y\sqrt{D})(x - y\sqrt{D})$. Here we allow D to be negative as well as positive, in which case we would be moving into the realm of complex numbers.

To illustrate this idea, consider the case $D = -1$, so the form is $x^2 + y^2$ which we are factoring as $(x + yi)(x - yi)$. Writing a number n as a sum $a^2 + b^2$ is then equivalent to factoring it as $(a + bi)(a - bi)$. For example $5 = 2^2 + 1^2 = (2 + i)(2 - i)$, and $13 = 3^2 + 2^2 = (3 + 2i)(3 - 2i)$, so 5 and 13 are no longer prime when we allow factorizations using numbers $a + bi$. Sometimes a nonprime number such as 65 can be written as the sum of two squares in more than one way: $65 = 8^2 + 1^2 = 4^2 + 7^2$, so it has factorizations as $(8 + i)(8 - i)$ and $(4 + 7i)(4 - 7i)$. This becomes more understandable if one uses the factorization

$$65 = 5 \cdot 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$$

If we combine these four terms as $(2 - i)(3 + 2i) = 8 + i$ and $(2 + i)(3 - 2i) = 8 - i$ we get the representation $65 = 8^2 + 1^2 = (8 + i)(8 - i)$, whereas if we combine them as $(2 + i)(3 + 2i) = 4 + 7i$ and $(2 - i)(3 - 2i) = 4 - 7i$ we get the other representation $65 = 4^2 + 7^2 = (4 + 7i)(4 - 7i)$.

Thus we will consider the set

$$\mathbb{Z}[\sqrt{D}] = \{\, x + y\sqrt{D} \mid x, y \in \mathbb{Z} \,\}$$

which consists of real numbers if $D > 0$ and complex numbers if $D < 0$. We will always assume D is not a square, so $\mathbb{Z}[\sqrt{D}]$ is not just $\mathbb{Z}$. When $D = -1$ we have $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[i]$, and numbers $a + bi$ in $\mathbb{Z}[i]$ are known as *Gaussian integers*.

Primes and Units

We will be interested in factorizations of numbers in $\mathbb{Z}[\sqrt{D}]$, particularly how they factor into 'primes'. If a prime p in $\mathbb{Z}$ happens to be representable as $p = x^2 - Dy^2$ then this is saying that p is no longer prime in $\mathbb{Z}[\sqrt{D}]$ since it factors as $p = (x + y\sqrt{D})(x - y\sqrt{D})$. Of course, we should say precisely what we mean by a 'prime' in $\mathbb{Z}[\sqrt{D}]$. For an ordinary integer $p > 1$, being prime means that p is divisible only by itself and 1. If we allow negative numbers, we can "factor" a prime p as $(-1)(-p)$, but this should not count as a genuine factorization, otherwise there would be no primes at all in $\mathbb{Z}$. In $\mathbb{Z}[\sqrt{D}]$ things can be a little more complicated because of the existence of *units* in $\mathbb{Z}[\sqrt{D}]$, the nonzero elements $\varepsilon \in \mathbb{Z}[\sqrt{D}]$ whose inverse ε^{-1} also lies in $\mathbb{Z}[\sqrt{D}]$. For example, in the Gaussian integers $\mathbb{Z}[i]$ there are four obvious units, ± 1 and $\pm i$, since $(i)(-i) = 1$. We will see in a little while that these are the only units in $\mathbb{Z}[i]$. Having four units in $\mathbb{Z}[i]$ instead of just ± 1 complicates the factorization issue slightly, but not excessively so.

For positive values of D things are somewhat less tidy because there are always infinitely many units in $\mathbb{Z}[\sqrt{D}]$ when $D > 0$. For example, when $D = 2$ the number $\varepsilon = 3 + 2\sqrt{2}$ is a unit because $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$. All the powers of $3 + 2\sqrt{2}$ are therefore also units, and there are infinitely many of them since $3 + 2\sqrt{2} > 1$ so $(3 + 2\sqrt{2})^n \to \infty$ as $n \to \infty$.

Whenever ε is a unit in $\mathbb{Z}[\sqrt{D}]$ we can factor any other number α in $\mathbb{Z}[\sqrt{D}]$ as $\alpha = (\alpha\varepsilon)(\varepsilon^{-1})$. If we allowed this as a genuine factorization there would be no primes in $\mathbb{Z}[\sqrt{D}]$, so it is best not to consider it as a genuine factorization. This leads us to the following definition:

> An element α of $\mathbb{Z}[\sqrt{D}]$ is said to be *prime* in $\mathbb{Z}[\sqrt{D}]$ if it is neither 0 nor a unit, and if whenever we have a factorization of α as $\alpha = \beta\gamma$ with both β, γ in $\mathbb{Z}[\sqrt{D}]$, then it must be the case that either β or γ is a unit in $\mathbb{Z}[\sqrt{D}]$.

Not allowing units as primes is analogous to the standard practice of not considering 1 to be a prime in $\mathbb{Z}$.

If we replace $\mathbb{Z}[\sqrt{D}]$ by $\mathbb{Z}$ in the definition of primeness above, we get the condition that an integer a in $\mathbb{Z}$ is prime if its only factorizations are the trivial ones $a = (a)(1) = (1)(a)$ and $a = (-a)(-1) = (-1)(-a)$, which is what we would expect. This definition of primeness also means that we are allowing negative primes as the negatives of the positive primes in $\mathbb{Z}$.

A word of caution: An integer p in $\mathbb{Z}$ can be prime in $\mathbb{Z}$ but not prime in $\mathbb{Z}[\sqrt{D}]$. For example, in $\mathbb{Z}[i]$ we have the factorization $5 = (2 + i)(2 - i)$, and as we will be able to verify soon, neither $2 + i$ nor $2 - i$ is a unit in $\mathbb{Z}[i]$. Hence by our definition 5 is not a prime in $\mathbb{Z}[i]$, even though it is prime in $\mathbb{Z}$. Thus one always has to be careful when speaking about primeness to distinguish “prime in $\mathbb{Z}$" from “prime in $\mathbb{Z}[\sqrt{D}]$".

Having defined what we mean by primes in $\mathbb{Z}[\sqrt{D}]$ we can now ask the fundamental questions that will be central to this chapter:

> *Does every element of $\mathbb{Z}[\sqrt{D}]$, apart from 0 and units, have a factorization into primes in $\mathbb{Z}[\sqrt{D}]$? And if it does, is this factorization unique?*

The uniqueness question needs a little explanation. If we have a unit ε in $\mathbb{Z}[\sqrt{D}]$ we can always modify a factorization $\alpha = \beta\gamma$ to give other factorizations $\alpha = (\varepsilon\beta)(\varepsilon^{-1}\gamma)$ and $\alpha = (\varepsilon^{-1}\beta)(\varepsilon\gamma)$. This is analogous to writing $6 = (2)(3) = (-2)(-3)$ in $\mathbb{Z}$. This sort of nonuniqueness is unavoidable, but it is also not too serious a problem. So when we speak of factorization in $\mathbb{Z}[\sqrt{D}]$ being unique, we will always mean unique up to insertion of units (and their inverses).

The Norm

We introduce now a basic tool that is of great use in studying factorizations. For a number $x + y\sqrt{D}$ define its *norm* to be

$$N(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2$$

Thus the norm is a function $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$. The main reason the norm is important is because of the following multiplicativity property:

Proposition. $N(\alpha\beta) = N(\alpha)N(\beta)$ *for all* $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.

Proof: This is simply a calculation. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$. Then $\alpha\beta = (ac + bdD) + (ad + bc)\sqrt{D}$ and hence

$$\begin{aligned} N(\alpha\beta) &= a^2c^2 + 2abcdD + b^2d^2D^2 - (a^2d^2 + b^2c^2 + 2abcd)D \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D \end{aligned}$$

On the other hand we have

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - b^2D)(c^2 - d^2D) \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D \end{aligned}$$

So $N(\alpha\beta) = N(\alpha)N(\beta)$. □

The multiplicative property $N(\alpha\beta) = N(\alpha)N(\beta)$ implies that if two integers m and n are represented by the form $x^2 - Dy^2$, then so is their product mn. In the case of the form $x^2 + y^2$ this fact played a role in our proof of Fermat's theorem in Section 2.3, so now we see how this fits into a more general picture.

Using the multiplicative property of the norm we can derive a simple criterion for recognizing units:

Proposition. *An element* $\varepsilon \in \mathbb{Z}[\sqrt{D}]$ *is a unit if and only if* $N(\varepsilon) = \pm 1$.

Proof: Suppose ε is a unit, so its inverse ε^{-1} also lies in $\mathbb{Z}[\sqrt{D}]$. Then we have $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$. Since both $N(\varepsilon)$ and $N(\varepsilon^{-1})$ are elements of $\mathbb{Z}$, this forces $N(\varepsilon)$ to be ± 1. Conversely, the inverse of an element $\varepsilon = a + b\sqrt{D}$ in

$\mathbb{Z}[\sqrt{D}]$ is $\varepsilon^{-1} = (a - b\sqrt{D})/N(\varepsilon)$ since multiplying this by $a + b\sqrt{D}$ gives 1. Hence if $N(\varepsilon) = \pm 1$ we have $\varepsilon^{-1} = \pm(a - b\sqrt{D})$, an element of $\mathbb{Z}[\sqrt{D}]$, so ε is a unit. □

When D is negative there are very few units in $\mathbb{Z}[\sqrt{D}]$ since in these cases the equation $N(x + y\sqrt{D}) = x^2 - Dy^2 = \pm 1$ has very few integer solutions, namely, if $D = -1$ there are only the four solutions $(x, y) = (\pm 1, 0)$ and $(0, \pm 1)$ while if $D < -1$ there are only the two solutions $(x, y) = (\pm 1, 0)$. Thus the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$, and the only units in $\mathbb{Z}[\sqrt{D}]$ for $D < -1$ are ± 1.

The situation for $\mathbb{Z}[\sqrt{D}]$ with D positive is quite different. Here we are looking for solutions of $x^2 - Dy^2 = \pm 1$ with $D > 0$. This is Pell's equation, and we know from our study of topographs of hyperbolic forms that the equation $x^2 - Dy^2 = 1$ has infinitely many solutions since the value 1 occurs along the periodic separator line in the topograph of $x^2 - Dy^2$ when $(x, y) = (1, 0)$, so it appears infinitely often by periodicity. For some values of D the number -1 also appears along the separator line, and then it too appears infinitely often. Thus $\mathbb{Z}[\sqrt{D}]$ has infinitely many units $\varepsilon = x + y\sqrt{D}$, with arbitrarily large values of x and y. Fortunately the situation turns out to be not so bad as it seems at first glance:

Proposition. *The units in $\mathbb{Z}[\sqrt{D}]$, when $D > 0$, are the elements $\pm\varepsilon^n$ for $n \in \mathbb{Z}$, where $\varepsilon = p + q\sqrt{D}$ and (p, q) is the smallest positive solution of $x^2 - Dy^2 = \pm 1$.*

The unit $p + q\sqrt{D}$ given by this proposition is called the *fundamental unit*.

Proof: We know from Chapter 2 that the translation or glide-reflection symmetry along the separator line for $x^2 - Dy^2$ is given by the transformation

$$\begin{pmatrix} p & Dq \\ q & p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} px + Dqy \\ qx + py \end{pmatrix}$$

On the other hand, we also have

$$(p + q\sqrt{D})(x + y\sqrt{D}) = (px + Dqy) + (qx + py)\sqrt{D}$$

which is really the same transformation of the coefficients x and y. The units in $\mathbb{Z}[\sqrt{D}]$ are exactly the elements $x + y\sqrt{D}$ satisfying $x^2 - Dy^2 = \pm 1$, and we know that the solutions of this equation are exactly the pairs $\binom{x}{y}$ obtainable as products

$$\pm \begin{pmatrix} px + Dqy \\ qx + py \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

as n ranges over $\mathbb{Z}$. Hence the units are exactly the elements $\pm\varepsilon^n$ times 1. □

Another basic application of the norm is the following useful fact:

Proposition. *Let α be an element of $\mathbb{Z}[\sqrt{D}]$. If $N(\alpha)$ is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[\sqrt{D}]$.*

For example, when we factor 5 as $(2+i)(2-i)$ in $\mathbb{Z}[i]$, this proposition implies that both factors are prime since the norm of each one is 5, which is prime in $\mathbb{Z}$.

Proof: Suppose an element $\alpha \in \mathbb{Z}[\sqrt{D}]$ has a factorization $\alpha = \beta\gamma$, hence $N(\alpha) = N(\beta)N(\gamma)$. If $N(\alpha)$ is prime in $\mathbb{Z}$, this forces one of $N(\beta)$ and $N(\gamma)$ to be ± 1, hence one of β and γ is a unit. This means α is a prime since it cannot be 0 or a unit, as its norm is a prime. □

The converse of this proposition is not generally true. For example the number 3 has norm 9, which is not prime in $\mathbb{Z}$, and yet 3 is prime in $\mathbb{Z}[i]$ since if we had a factorization $3 = \alpha\beta$ in $\mathbb{Z}[i]$ with neither α nor β a unit, then the equation $N(\alpha)N(\beta) = N(3) = 9$ would imply that $N(\alpha) = \pm 3 = N(\beta)$, but there are no elements of $\mathbb{Z}[i]$ with norm ± 3 since the equation $x^2 + y^2 = \pm 3$ has no integer solutions.

Prime Factorizations

Now we can prove that prime factorizations always exist:

Proposition. *Every nonzero element of $\mathbb{Z}[\sqrt{D}]$ that is not a unit can be factored as a product of primes in $\mathbb{Z}[\sqrt{D}]$.*

Proof: We argue by induction on $|N(\alpha)|$. Since we are excluding 0 and units, the induction starts with the case $|N(\alpha)| = 2$. In this case α must itself be a prime by the preceding proposition, since 2 is prime in $\mathbb{Z}$. For the induction step, if α is a prime there is nothing to prove. If α is not prime, it factors as $\alpha = \beta\gamma$ with neither β nor γ a unit, so $|N(\beta)| > 1$ and $|N(\gamma)| > 1$. Since $N(\alpha) = N(\beta)N(\gamma)$, it follows that $|N(\beta)| < |N(\alpha)|$ and $|N(\gamma)| < |N(\alpha)|$. By induction, both β and γ are products of primes in $\mathbb{Z}[\sqrt{D}]$, hence their product α is also a product of primes. □

Let us investigate how to compute a prime factorization by looking at the case of $\mathbb{Z}[i]$, the Gaussian integers. Assuming that factorizations of Gaussian integers into primes are unique (up to units), which we will prove later, here is a procedure for finding the prime factorization of a Gaussian integer $\alpha = a + bi$:

(1) Factor the integer $N(\alpha) = a^2 + b^2$ into primes p_k in $\mathbb{Z}$.

(2) Determine how each p_k factors into primes in $\mathbb{Z}[i]$.

(3) By the uniqueness of prime factorizations, the primes found in step (2) will be factors of either $a + bi$ or $a - bi$ since they are factors of $(a+bi)(a-bi)$, so all that remains is to test which of the prime factors of each p_k are factors of $a + bi$.

To illustrate this with a simple example, let us see how $3+i$ factors in $\mathbb{Z}[i]$. We have $N(3+i) = (3+i)(3-i) = 10 = 2 \cdot 5$. These two numbers factor as $2 = (i+i)(1-i)$ and $5 = (2+i)(2-i)$. These are prime factorizations in $\mathbb{Z}[i]$ since $N(1 \pm i) = 2$ and $N(2 \pm i) = 5$, both primes in $\mathbb{Z}$. Now we test whether for example $1+i$ divides $3+i$ by dividing:

$$\frac{3+i}{1+i} = \frac{(3+i)(1-i)}{(1+i)(1-i)} = \frac{4-2i}{2} = 2-i$$

Since the quotient $2-i$ is a Gaussian integer, we conclude that $1+i$ is a divisor of $3+i$ and we have the factorization $3+i = (1+i)(2-i)$. The is the prime factorization of $3+i$ since we have already noted that both $1+i$ and $2-i$ are primes in $\mathbb{Z}[i]$.

For a more complicated example consider $244+158i$. For a start, this factors as $2(122+79i)$. Since 122 and 79 have no common factors in $\mathbb{Z}$ we can't go any farther by factoring out ordinary integers. We know that 2 factors as $(1+i)(1-i)$ and these two factors are prime in $\mathbb{Z}[i]$ since their norm is 2. It remains to factor $122+79i$. This has norm $122^2+79^2 = 21125 = 5^3 \cdot 13^2$. Both 5 and 13 happen to factor in $\mathbb{Z}[i]$, namely $5 = (2+i)(2-i)$ and $13 = (3+2i)(3-2i)$, and these are prime factorizations since the norms of $2 \pm i$ and $3 \pm 2i$ are 5 and 13, primes in $\mathbb{Z}$. Thus we have the prime factorization

$$(122+79i)(122-79i) = 5^3 \cdot 13^2 = (2+i)^3(2-i)^3(3+2i)^2(3-2i)^2$$

Now we look at the factors on the right side of this equation to see which ones are factors of $122+79i$. Suppose for example we test whether $2+i$ divides $122+79i$:

$$\frac{122+79i}{2+i} = \frac{(122+79i)(2-i)}{(2+i)(2-i)} = \frac{323+36i}{5}$$

This is not a Gaussian integer, so $2+i$ does not divide $122+79i$. Let's try $2-i$ instead:

$$\frac{122+79i}{2-i} = \frac{(122+79i)(2+i)}{(2-i)(2+i)} = \frac{165+280i}{5} = 33+56i$$

So $2-i$ does divide $122+79i$. In fact, we can expect that $(2-i)^3$ will divide $122+79i$, and it can be checked that it does. In a similar way one can check whether $3+2i$ or $3-2i$ divides $122+79i$, and one finds that it is $3-2i$ that divides $122+79i$, and in fact $(3-2i)^2$ divides $122+79i$. After these calculations one might expect that $122+79i$ was the product $(2-i)^3(3-2i)^2$, but upon multiplying this product out one finds that it is the negative of $122+79i$, so

$$122+79i = (-1)(2-i)^3(3-2i)^2$$

The factor -1 is a unit, so it could be combined with one of the other factors, for example changing one of the factors $2-i$ to $i-2$. Alternatively, we could replace the factor -1 by i^2 and then multiply each $3-2i$ factor by i to get the prime factorization

$$122+79i=(2-i)^3(2+3i)^2$$

Hence for $244+158i$ we have the prime factorization

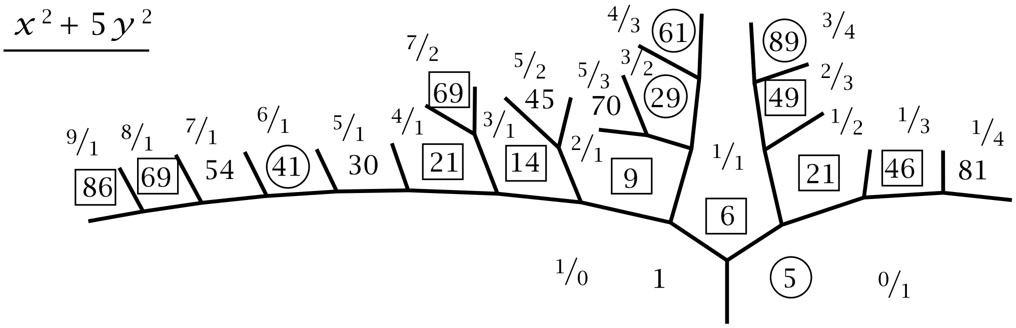
$$244+158i=(1+i)(1-i)(2-i)^3(2+3i)^2$$

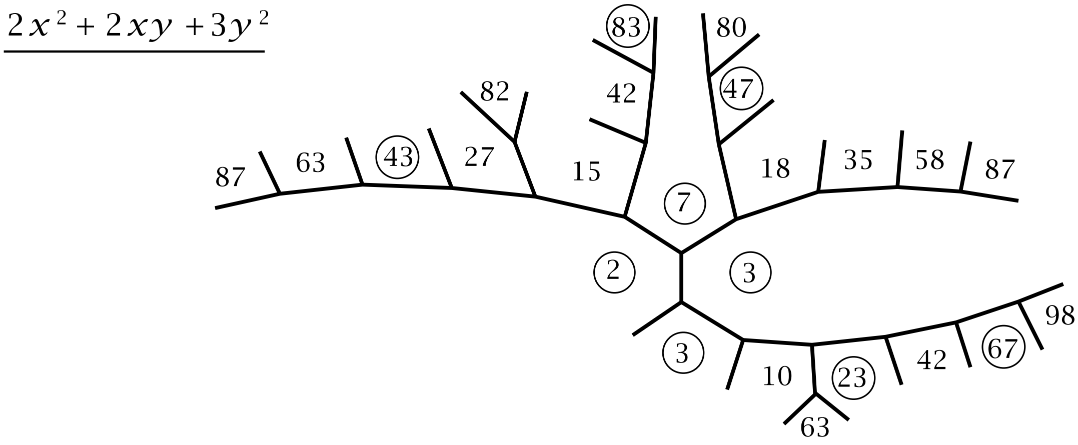
The question of uniqueness of prime decompositions in $\mathbb{Z}[\sqrt{D}]$ is much more subtle. Even if the ambiguity of inserting units is allowed, there are still cases when prime factorizations fail to be unique. One of the simplest instances is in $\mathbb{Z}[\sqrt{-5}]$ where we have the factorizations

$$6=(2)(3)=(1+\sqrt{-5})(1-\sqrt{-5})$$

The only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so these two factorizations do not differ just by units. We can see that 2, 3, and $1\pm\sqrt{-5}$ are prime in $\mathbb{Z}[\sqrt{-5}]$ by looking at norms. The norms of 2, 3, and $1\pm\sqrt{-5}$ are 4, 9, and 6, so if one 2, 3, or $1\pm\sqrt{-5}$ was not a prime, it would have a factor of norm 2 or 3 since these are the only numbers that occur in nontrivial factorizations of 4, 9, and 6. However, the equations $x^2+5y^2=2$ and $x^2+5y^2=3$ have no integer solutions so there are no elements of $\mathbb{Z}[\sqrt{-5}]$ of norm 2 or 3. Thus in $\mathbb{Z}[\sqrt{-5}]$ the number 6 has two prime factorizations that do not differ merely by units.

What is secretly going on in this example is that x^2+5y^2 is not the only quadratic form of discriminant -20, up to equivalence. Another form of the same discriminant is $2x^2+2xy+3y^2$, and this form takes on the values 2 and 3 that the form x^2+5y^2 omits, even though x^2+5y^2 does take on the value $6=2\cdot 3$. Here are the topographs of these two forms, with prime values circled and with boxes around nonprime values that yield nonunique prime factorizations:





In the topograph for $x^2 + 5y^2$ some numbers occur in boxes twice, leading to three different prime factorizations. For example 21 factors into primes in $\mathbb{Z}[\sqrt{-5}]$ as $3 \cdot 7$, as $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ and as $(4 + \sqrt{-5})(4 - \sqrt{-5})$. Another example is $69 = 3 \cdot 23 = (7 + 2\sqrt{-5})(7 - 2\sqrt{-5}) = (8 + \sqrt{-5})(8 - \sqrt{-5})$.

Proposition. *Let p be a prime in $\mathbb{Z}$. Then:*
(a) If either p or $-p$ is represented by the form $x^2 - Dy^2$, so $p = \pm(a^2 - Db^2)$, then $\pm p$ factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \pm(a + b\sqrt{D})(a - b\sqrt{D})$ and both these factors are prime in ZD.
(b) If neither p nor $-p$ is represented by $x^2 - Dy^2$ then p remains prime in $\mathbb{Z}[\sqrt{D}]$.

Proof: For part (a), if $p = \pm(a^2 - Db^2)$, then certainly $\pm p$ factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \pm(a + b\sqrt{D})(a - b\sqrt{D})$. The two factors are prime since their norm is $\pm p$ which is prime in $\mathbb{Z}$ by assumption.

For (b), if p is not a prime in $\mathbb{Z}[\sqrt{D}]$ then it factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \alpha\beta$ with neither α nor β a unit. Then $N(p) = p^2 = N(\alpha)N(\beta)$ with neither $N(\alpha)$ nor $N(\beta)$ equal to ± 1, hence we must have $N(\alpha) = \pm p$ and $N(\beta) = \pm p$. Focusing our attention just on α, this can be written as $a + b\sqrt{D}$, and then we have $\pm p = N(a + b\sqrt{D}) = a^2 - Db^2$, which says that the form $x^2 - Dy^2$ represents $\pm p$. Turning this statement

around, it says that if x^2-Dy^2 does not represent p or $-p$ then p is prime in $\mathbb{Z}[\sqrt{D}]$.
□

Proposition. *If $\mathbb{Z}[\sqrt{D}]$ has unique factorization into primes then the only primes in $\mathbb{Z}[\sqrt{D}]$ are the primes described in (a) or (b) of the preceding proposition (or units times these primes).*

Proof: Let $\alpha = a + b\sqrt{D}$ be an arbitrary prime in $\mathbb{Z}[\sqrt{D}]$. The norm $n = N(\alpha) = (a+b\sqrt{D})(a-b\sqrt{D})$ is an integer in $\mathbb{Z}$ so it can be factored as a product $n = p_1 \cdots p_k$ of primes in $\mathbb{Z}$. Each p_i either stays prime in $\mathbb{Z}[\sqrt{D}]$ or factors as a product $(a_i + b_i\sqrt{D})(a_i - b_i\sqrt{D})$ of primes in $\mathbb{Z}[\sqrt{D}]$. This gives a factorization of n into primes in $\mathbb{Z}[\sqrt{D}]$. A second factorization of n into primes in $\mathbb{Z}[\sqrt{D}]$ can be obtained from the formula $n = (a + b\sqrt{D})(a - b\sqrt{D})$ by factoring the second factor into primes, since the first factor $a + b\sqrt{D}$ is already prime by assumption. (In fact if $a + b\sqrt{D}$ is prime then $a - b\sqrt{D}$ will also be a prime, but we don't need to know this.) If we have unique factorization in $\mathbb{Z}[\sqrt{D}]$ then the prime factor $a + b\sqrt{D}$ of n will have to be one of the prime factors in the first prime factorization of n, or a unit times one of these primes. Thus $a + b\sqrt{D}$ will be a unit times a prime of one of the two types described in the previous proposition. □

Unique Factorization via the Euclidean Algorithm

Our goal now is to show that unique factorization holds for the Gaussian integers $\mathbb{Z}[i]$, and in a few other cases as well. The plan will be to see that Gaussian integers have a Euclidean algorithm much like the Euclidean algorithm in $\mathbb{Z}$, then deduce unique factorization from this Euclidean algorithem.

In order to prove that prime factorizations are unique we will use the following special property that holds in $\mathbb{Z}$ and in some other rings $\mathbb{Z}[\sqrt{D}]$ as well:

$(*)$ *If a prime p divides a product ab then p must divide either a or b.*

One way to prove this for $\mathbb{Z}$ would be to consider the prime factorization of ab, which can be obtained by factoring each of a and b into primes separately. Then if the prime p divides ab, it would have to occur in the prime factorization of ab, hence it would occur in the prime factorization of either a or b, which would say that p divides a or b.

This argument assumed implicitly that the prime factorization of ab was unique. Thus the property $(*)$ is a consequence of unique factorization into primes. But the property $(*)$ also implies that prime factorizations are unique. To see why, consider two prime factorizations of a number n:

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_l$$

We can assume $k \le l$ by interchanging the p_i's and q_i's if necessary. We want to argue that if $(*)$ holds for each p_i, then the q_i's are just a permutation of the p_i's and in particular $k = l$. The argument to prove this goes as follows. Consider first the prime p_1. This divides the product $q_1(q_2 \cdots q_l)$ so by property $(*)$ it divides either q_1 or $q_2q_3 \cdots q_l$. In the latter case, another application of $(*)$ shows that p_1 divides either q_2 or $q_3q_4 \cdots q_l$. Repeating this argument as often as necessary, we conclude that p_1 must divide at least one q_i. After permuting the q_i's we can assume that p_1 divides q_1. If we are assuming all the p_i's and q_i's are positive integers, the fact that the primep_1 divides the prime q_1 implies that p_1 equals q_1, so we can cancel p_1 and q_1 from the equation $p_1p_2 \cdots p_k = q_1q_2 \cdots q_l$ to get $p_2 \cdots p_k = q_2 \cdots q_l$. Now repeat the argument to show that p_2 equals some remaining q_i which we can assume is q_2 after a permutation. After further repetitions we eventually reach the point that the final p_k is a product of the remaining q_i's. But then since p_k is prime there could only be one remaining q_i, so we would have $k = l$ and $p_k = q_k$, finishing the argument.

If we knew the analog of property $(*)$ held for primes in $\mathbb{Z}[\sqrt{D}]$ we could make essentially the same argument to show that unique factorization holds in $\mathbb{Z}[\sqrt{D}]$. The only difference in the argument would be that we would have to take units into account. The argument would be exactly the same up to the point where we concluded that p_1 divides q_1. Then the fact that q_1 is prime would not say that p_1 and q_1 were equal, but only that q_1 is a unit times p_1, so we would have an equation $q_1 = ep_1$ with e a unit. Then we would have $p_1p_2 \cdots p_k = ep_1q_2 \cdots q_l$. Canceling p_1 would then yield $p_2p_3 \cdots p_k = eq_2q_3 \cdots q_l$. The product eq_2 is prime if q_2 is prime, so if we let $q_2' = eq_2$ we would have $p_2p_3 \cdots p_k = q_2'q_3 \cdots q_l$. The argument could then be repeated to show eventually that the q_i's are the same as the p_i's up to permutation and multiplication by units, which is what unique factorization means.

Since the property $(*)$ implies unique factorization, it will not hold in $\mathbb{Z}[\sqrt{D}]$ when $\mathbb{Z}[\sqrt{D}]$ does not have unique factorization. For a concrete example consider $\mathbb{Z}[\sqrt{-5}]$. Here we had nonunique prime factorizations $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. The prime 2 thus divides the product $(1+\sqrt{-5})(1-\sqrt{-5})$ but it does not divide either factor $1 \pm \sqrt{-5}$ since $(1 \pm \sqrt{-5})/2$ is not an element of $\mathbb{Z}[\sqrt{-5}]$.

For $\mathbb{Z}$ we know from Chapter 1 that an equation $ax+by = 1$ always has solutions in $\mathbb{Z}$ whenever a and b have no common factors. This fact can be used to deduce that property $(*)$ holds in $\mathbb{Z}$. To see this, suppose that a prime p divides a product ab. It will suffice to show that if p does not divide a then it must divide b. If p does not divide a, then since p is prime, p and a have no common factors. This implies that the equation $px + ay = 1$ is solvable with integers x and y. Now multiply this equation by b to get an equation $b = pbx + aby$. The number p divides the right side of this equation since it obviously divides pbx and it divides ab by assumption. Hence p divides b, which is what we wanted to show. Thus we have (finally!) proved that $\mathbb{Z}$ has unique factorization.

How did we know that equations $ax + by = 1$ in $\mathbb{Z}$ are solvable when a and b have no common factors? We deduced this from properties of continued fractions and the Farey diagram, but these ultimately came from the Euclidean algorithm. In fact it is not hard to deduce solvability of $ax + by = 1$ directly from the Euclidean algorithm.

What the Euclidean algorithm gives us, in the case of $\mathbb{Z}$, is a method for starting with two positive integers α_0 and α_1 and constructing a sequence of positive numbers α_i and β_i satisfying equations

$$\begin{aligned}
\alpha_0 &= \beta_1\alpha_1 + \alpha_2 \\
\alpha_1 &= \beta_2\alpha_2 + \alpha_3 \\
&\vdots \\
\alpha_{n-2} &= \beta_{n-1}\alpha_{n-1} + \alpha_n \\
\alpha_{n-1} &= \beta_n\alpha_n + \alpha_{n+1} \\
\alpha_n &= \beta_{n+1}\alpha_{n+1}
\end{aligned}$$

From these equations we can deduce two consequences:

(1) α_{n+1} divides α_0 and α_1.

(2) The equation $\alpha_{n+1} = \alpha_0 x + \alpha_1 y$ is solvable in $\mathbb{Z}$.

To see why (1) is true, note that the last equation implies that α_{n+1} divides α_n. Then the next-to-last equation implies that α_{n+1} divides α_{n-1}, and the equation before this then implies that α_{n+1} divides α_{n-2}, and so on until one deduces that α_{n+1} divides all the α_i's and in particular α_0 and α_1.

To see why (2) is true, observe that each equation before the last one allows an α_i to be expressed as a linear combination of α_{i-1} and α_{i-2}, so by repeatedly substituting in, one can express each α_i in terms of α_0 and α_1 as a linear combination

$x\alpha_0+y\alpha_1$ with integer coefficients x and y, so in particular α_{n+1} can be represented in this way, which says that the equation $\alpha_{n+1}=\alpha_0x+\alpha_1y$ is solvable in $\mathbb{Z}$.

Now if we assume that α_0 and α_1 have no common divisors except 1, then α_{n+1} must by 1 by statement (1), and by statement (2) we get integers x and y such that $\alpha_0x+\alpha_1y=1$, as we wanted. In this way we see that the Euclidean algorithm in $\mathbb{Z}$ implies unique factorization.

A very similar argument works in $\mathbb{Z}[\sqrt{D}]$ provided that one has a Euclidean algorithm to produce the sequence of equations above starting with any nonzero pair of elements α_0 and α_1 in $\mathbb{Z}[\sqrt{D}]$. The only difference in the more general case is that α_{n+1} might not be 1, but only a unit in $\mathbb{Z}[\sqrt{D}]$. Thus one would apply statements (1) and (2) to a pair α_0, α_1 whose only common divisors were units, hence α_{n+1} would be a unit, and then the equation $\alpha_{n+1}=\alpha_0x+\alpha_1y$ could be modified by multiplying through by α_{n+1}^{-1} to get an equation $1=\alpha_0x+\alpha_1y$ with solutions x,y in $\mathbb{Z}[\sqrt{D}]$. As we have seen earlier, this would imply unique factorization in $\mathbb{Z}[\sqrt{D}]$.

Let us show now that there is a Euclidean algorithm in the Gaussian integers $\mathbb{Z}[i]$. The key step is to be able to find, for each pair of nonzero Gaussian integers α_0 and α_1, two more Gaussian integers β_1 and α_2 such that $\alpha_0=\beta_1\alpha_1+\alpha_2$ and $N(\alpha_2)<N(\alpha_1)$. If we can always do this, then by repeating the same step over and over we construct a sequence of α_i's and β_i's where the successive α_i's have smaller and smaller norms. Since these norms are positive integers, they cannot keep decreasing infinitely often, so eventually the process will reach an α_i of norm 0, so this α_i must be 0 and the Euclidean algorithm will end in a finite number of steps, as it should.

The equation $\alpha_0=\beta_1\alpha_1+\alpha_2$ is saying that when we divide α_1 into α_0, we obtain a quotient β_1 and a remainder α_2. What we want is for the remainder to be 'smaller' than the divisor α_1, in the sense of having a smaller norm. To get an idea how we can do this it may be helpful to look at the equivalent equation

$$\frac{\alpha_0}{\alpha_1}=\beta_1+\frac{\alpha_2}{\alpha_1}$$

If we were working with ordinary integers, the quotient β_1 would be the integer part of the rational number α_0/α_1 and α_2/α_1 would be the remaining fractional part. For Gaussian integers we do something similar, but instead of taking β_1 to be the 'integer part' of α_0/α_1 we take it to be the *closest* Gaussian integer to α_0/α_1.

Here is an example, where we choose α_0 to be $12+15i$ and α_1 to be $5+2i$. Then:

$$\frac{\alpha_0}{\alpha_1}=\frac{12+15i}{5+2i}=\frac{(12+15i)(5-2i)}{(5+2i)(5-2i)}=\frac{90+51i}{29}=(3+2i)+\frac{3-7i}{29}$$

Here in the last step we chose $3 + 2i$ as β_1 because 3 is the closest integer to $90/29$ and 2 is the closest integer to $51/29$. Having found a likely candidate for β_1, we can use the equation $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ to find α_2. This equation is

$$12 + 15i = (3 + 2i)(5 + 2i) + \alpha_2 = (11 + 16i) + \alpha_2 \qquad \text{hence} \qquad \alpha_2 = 1 - i$$

Notice that $N(1 - i) = 2 < N(5 + 2i) = 29$ so we have $N(\alpha_2) < N(\alpha_1)$ as we wanted.

Will the process of choosing β_1 as the nearest Gaussian integer to the 'Gaussian rational' α_0/α_1 always lead to an α_2 with $N(\alpha_2) < N(\alpha_1)$? The answer is yes because if we write the quotient α_2/α_1 in the form $x + yi$ for rational numbers x and y (in the example above we have $x + yi = \frac{3}{29} + \frac{-7}{29}i$) then having β_1 the closest Gaussian integer to α_0/α_1 says that $|x| \le \frac{1}{2}$ and $|y| \le \frac{1}{2}$, so

$$N\Big(\frac{\alpha_2}{\alpha_1}\Big) = x^2 + y^2 \le \frac{1}{4} + \frac{1}{4} < 1$$

and hence

$$N(\alpha_2) = N\Big(\frac{\alpha_2}{\alpha_1}\cdot\alpha_1\Big) = N\Big(\frac{\alpha_2}{\alpha_1}\Big)N(\alpha_1) < N(\alpha_1)$$

This shows that there is a general Euclidean algorithm in $\mathbb{Z}[i]$, hence $\mathbb{Z}[i]$ has unique factorization.

Let us finish carrying out the Euclidean algorithm for $\alpha_0 = 12 + 15i$ and $\alpha_1 = 5 + 2i$. The next step is to divide $\alpha_2 = 1 - i$ into $\alpha_1 = 5 + 2i$:

$$\frac{5 + 2i}{1 - i} = \frac{(5 + 2i)(1 + i)}{(1 - i)(1 + i)} = \frac{3 + 7i}{2} = (1 + 3i) + \frac{1 + i}{2}$$

Notice that the fractions $3/2$ and $7/2$ are exactly halfway between two consecutive integers, so instead of choosing $1 + 3i$ for the closest integer to $(3 + 7i)/2$ we could equally well have chosen $2 + 3i$, $1 + 4i$, or $2 + 4i$. If we stick with the choice $1 + 3i$ then we use this to calculate the next α_i:

$$5 + 2i = (1 + 3i)(1 - i) + \alpha_3 = (4 + 2i) + \alpha_3 \qquad \text{hence} \qquad \alpha_3 = 1$$

The final step would be simply to write $1 - i = (1 - i)1 + 0$. Thus the full Euclidean algorithm is:

$$\begin{aligned} 12 + 15i &= (3 + 2i)(5 + 2i) + (1 - i) \\ 5 + 2i &= (1 + 3i)(1 - i) + 1 \\ 1 - i &= (1 - i)1 + 0 \end{aligned}$$

In particular, since the last nonzero remainder is 1, a unit in $\mathbb{Z}[i]$, we deduce that this is the greatest common divisor of $12 + 15i$ and $5 + 2i$, where 'greatest' means 'of greatest norm'. In other words $12 + 15i$ and $5 + 2i$ have no common divisors other than units.

As in the case of ordinary integers, the equations that display the results of carrying out the Euclidean algorithm can be used to express the last nonzero remainder in terms of the original two numbers:

$$\begin{aligned} 1 &= (5 + 2i) - (1 + 3i)(1 - i) \\ &= (5 + 2i) - (1 + 3i)[(12 + 15i) - (3 + 2i)(5 + 2i)] \\ &= -(1 + 3i)(12 + 15i) + (-2 + 11i)(5 + 2i) \end{aligned}$$

If it had happened that the last nonzero remainder was a unit other than 1, we could have expressed this unit in terms of the original two Gaussian integers, and then multiplied the equation by the inverse of the unit to get an expression for 1 in terms of the original two Gaussian integers.

Other Instances of Unique Factorization

Elements of $\mathbb{Z}[\sqrt{-2}]$ factor uniquely into primes because there is a Euclidean algorithm in $\mathbb{Z}[\sqrt{-2}]$. The crucial point we used in the verification that $\mathbb{Z}[i]$ had a Euclidean algorithm was that each complex number is within a distance less than 1 from some Gaussian integer. The same thing is true for $\mathbb{Z}[\sqrt{-2}]$ since the numbers in $\mathbb{Z}[\sqrt{-2}]$ form a rectangular lattice in the plane, where the rectangles have width 1 and height $\sqrt{2}$. Every point in such a rectangle is at distance less than 1 from one of the four vertices since the worst case is the center point of the rectangle, which is at distance $\sqrt{3}/2$ from the vertices.

This argument does not work in $\mathbb{Z}[\sqrt{-3}]$ since in a rectangle of width 1 and height $\sqrt{3}$ the center point is at distance exactly 1 from the vertices, and one needs distance strictly less than 1 for the Euclidean algorithm. In fact unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$, and in many other cases too:

Proposition. *Unique factorization fails in $\mathbb{Z}[\sqrt{D}]$ whenever $D < -2$, and it also fails when $D > 0$ and $D \equiv 1$ modulo 4. (In the latter case we assume as always that D is not a square).*

Proof: The number $D^2 - D$ factors in $\mathbb{Z}[\sqrt{D}]$ as $(D + \sqrt{D})(D - \sqrt{D})$, and it also factors as $D(D-1)$. The number 2 divides either D or $D - 1$ since one of these two consecutive integers must be even. However, 2 does not divide either $D + \sqrt{D}$ or $D - \sqrt{D}$ in $\mathbb{Z}[\sqrt{D}]$ since $(D \pm \sqrt{D})/2$ is not an element of $\mathbb{Z}[\sqrt{D}]$ as the coefficient of $\sqrt{D}$ in this quotient is not an integer. If we knew that 2 was prime in $\mathbb{Z}[\sqrt{D}]$ we would then have two distinct factorizations of $D^2 - D$ into primes in $\mathbb{Z}[\sqrt{D}]$: One obtained by combining prime factorizations of D and $D - 1$, and the other obtained by combining prime factorizations of $D + \sqrt{D}$ and $D - \sqrt{D}$. The first factorization would contain the prime 2 and the second would not.

It remains to check that 2 is a prime in $\mathbb{Z}[\sqrt{D}]$ in the cases listed. If it is not a prime, then it factors as $2 = \alpha\beta$ with neither α nor β a unit, so we would have $N(\alpha) = N(\beta) = \pm 2$. Thus the equation $x^2 - Dy^2 = \pm 2$ would have an integer solution (x, y). This is clearly impossible if $D = -3$ or any negative integer less than -3. If $D > 0$ and $D \equiv 1$ modulo 4 then if we look at the equation $x^2 - Dy^2 = \pm 2$ modulo 4 it becomes $x^2 - y^2 \equiv 2$, but this is impossible since x^2 and y^2 are congruent to 0 or 1 modulo 4, so $x^2 - y^2$ is congruent to 0, 1, or -1. □

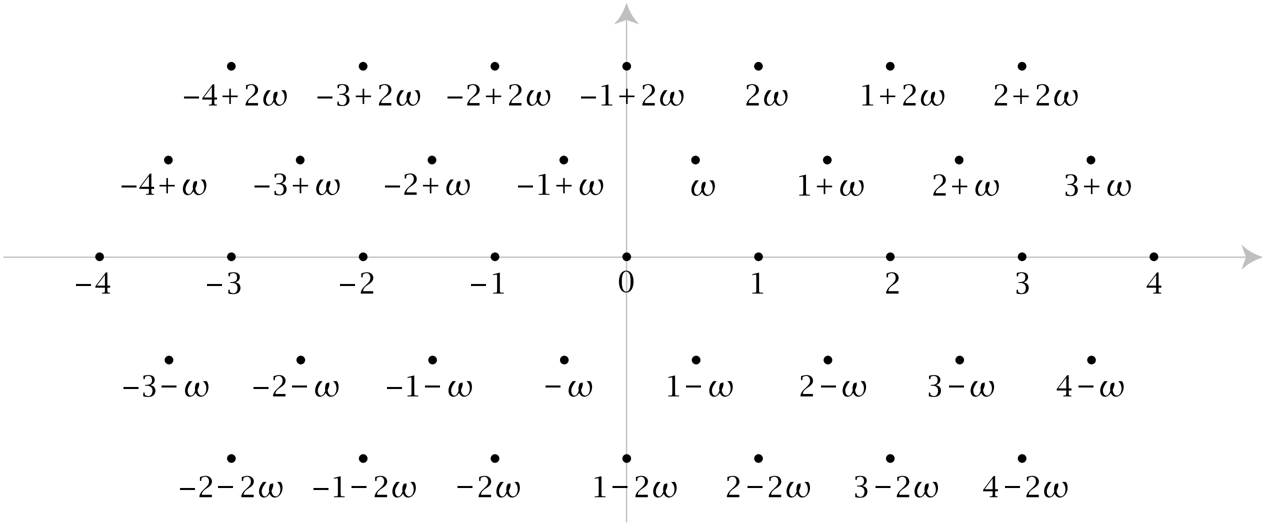
In the cases $D \equiv 1$ modulo 4 there is a way to enlarge $\mathbb{Z}[\sqrt{D}]$ to a slightly larger ring $\mathbb{Z}[\omega]$ which sometimes has unique factorization when $\mathbb{Z}[\sqrt{D}]$ does not. The construction also fills a gap by providing a norm form whose discriminant is congruent to 1 modulo 4, complementing the norm form $x^2 - Dy^2$ of discriminant $4D \equiv 0$ modulo 4. The new norm form will be $x^2 + xy - dy^2$, of discriminant $1 + 4d$.

The number $\omega = (1+\sqrt{1+4d})/2$ satisfies the quadratic equation $\omega^2 - \omega - d = 0$, whose other root is $\overline{\omega} = (1 - \sqrt{1+4d})/2$. From the quadratic equation we obtain the relation $\omega^2 = \omega + d$, and this implies that the set $\mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\}$ is closed under multiplication and hence forms a ring, like $\mathbb{Z}[\sqrt{D}]$. The norm in $\mathbb{Z}[\omega]$ is defined by

$$\begin{aligned} N(x+y\omega) = (x+y\omega)(x+y\overline{\omega}) &= x^2 + xy(\omega+\overline{\omega}) + y^2\omega\overline{\omega} \\ &= x^2 + xy - dy^2 \end{aligned}$$

since $\omega + \overline{\omega} = 1$ and $\omega\overline{\omega} = -d$. This norm function still satisfies the key property $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[\omega]$ since it is in fact just the restriction of the earlier norm to the subring $\mathbb{Z}[\omega]$ of $\mathbb{Q}(\sqrt{1+4d})$.

For example, when $d = -1$ we have $\omega = (1+\sqrt{-3})/2$ and the elements of $\mathbb{Z}[\omega]$ form a lattice of equilateral triangles in the xy-plane:



When $\omega = (1+\sqrt{-3})/2$ there is a Euclidean algorithm in $\mathbb{Z}[\omega]$ since every complex number is within distance less than 1 of some element of $\mathbb{Z}[\omega]$. Hence unique factorization holds in $\mathbb{Z}[\omega]$. There are six units, the six lattice points of distance 1 from the origin, which are the numbers ± 1, $\pm\omega$, and $\pm(\omega - 1)$. Equivalently, these are the powers ω^n for $n = 0, 1, 2, 3, 4, 5$, with $\omega^6 = 1$. The norm in $\mathbb{Z}[\omega]$ is given by the formula $N(x+y\omega) = x^2 + xy + y^2$. The primes p in $\mathbb{Z}$ that factor in $\mathbb{Z}[\omega]$ are those that can be written in the form $p = x^2 + xy + y^2 = N(x+y\omega)$. The analog of Fermat's theorem in this context is the fact that the primes p that can be written as $x^2 + xy + y^2$ are $p = 3$ and the primes $p = 3k+1$. For example $3 = N(1+\omega)$,

$7 = N(2+\omega)$, $13 = N(3+\omega)$, and $17 = N(3+2\omega)$. The factorization in each of these cases is given by the formula $p = N(x+y\omega) = (x+y\omega)(x+y\overline{\omega})$.

For larger negative values of d the picture of $\mathbb{Z}[\omega]$ in the complex plane is similar but stretched in the vertical direction. It is not hard to do the measurements to show that $\mathbb{Z}[\omega]$ is Euclidean only in the three cases $d = -1, -2, -3$ when the discriminant $\Delta = 1 + 4d$ is $-3, -7, -11$. There are four other negative values of the discriminant when $\mathbb{Z}[\omega]$ has unique factorization even though it does not have a Euclidean algorithm, the discriminants $\Delta = -19, -43, -67, -163$. Together with $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ this brings the total number of negative discriminants for which $\mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}[\omega]$ has unique factorization to nine, the discriminants

$$\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

These are exactly the nine negative discriminants for which all quadratic forms of that discriminant are equivalent. (This is not an accident.)

At first glance the choice of ω as $(1+\sqrt{1+4d})/2$ might seem somewhat arbitrary, and one might wonder whether similar constructions using other denominators besides 2 would also be possible. In order to do multiplication within the set $\mathbb{Z}[\omega]$ of complex numbers $x + y\omega$ with x and y integers one must be able to express ω^2 in this form as $m\omega + n$, so ω must satisfy a quadratic equation $\omega^2 - m\omega - n = 0$. This has roots $(m \pm \sqrt{m^2+4n})/2$, so we see that larger denominators than 2 will not work. If m is even, say $m = 2k$, then ω becomes $k \pm \sqrt{k^2+n}$, with no denominators at all. If m is odd, $m = 2k+1$, then ω is $(2k+1 \pm \sqrt{4k^2+4k+1+4n})/2$, which can be written as $k + (1+\sqrt{1+4d})/2$ so we are actually in the situation already considered.

We have seen that enlarging the ring $\mathbb{Z}[\sqrt{D}]$ to $\mathbb{Z}[\omega]$ in the cases $D = 1 + 4d$ can sometimes restore unique factorization. Another sort of enlargement comes from the fact that $\mathbb{Z}[\sqrt{n^2 D}]$ is contained in $\mathbb{Z}[\sqrt{D}]$. For example $\mathbb{Z}[\sqrt{-8}]$, which does not have unique factorization, is contained in $\mathbb{Z}[\sqrt{-2}]$ which does. For this reason it is often best to restrict attention to integers D having no square factors, and in this case we unify the notation by letting R_D denote the ring $\mathbb{Z}[\sqrt{D}]$ if $D \neq 1 + 4d$ and $\mathbb{Z}[\omega]$ if $D = 1 + 4d$. The discriminant of R_D is then D when $D = 1 + 4d$ and $4D$ when $D \neq 1 + 4d$.

When the discriminant is positive, R_D is a subring of the real numbers, so it is somewhat paradoxical that these cases tend to be more complex than in the case of negative discriminant, when R_D contains complex numbers. One reason for the added complication is that the norm form $x^2 - Dy^2$ or $x^2 + xy - dy^2$ is a hyperbolic form rather than elliptic. In particular, this means that norms can be negative as well as positive, and the norm doesn't have the nice geometric meaning of the square of the distance to the origin that it has in the imaginary case. Since the norm can be negative, the definition of a Euclidean algorithm is modified so that in the equations $\alpha_{i-1} = \beta_i \alpha_i + \alpha_{i+1}$ it is required that $|N(\alpha_{i+1})| < |N(\alpha_i)|$. It is known that there are exactly 16 positive values of D for which there is a Euclidean algorithm in R_D:

$$2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

In these cases one has unique factorization, but there are 22 other values of $D < 100$ where unique factorization holds even though there is no Euclidean algorithm:

$$14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97$$

It is still not known whether there are infinitely many values of D where there is unique factorization, although it is known that there are infinitely many values of D for which unique factorization fails.